CYBER CRIME DIGITAL FORENSIC READINESS SECURED BYOD ENVIRONMENT

A Thesis

Submitted in partial fulfillment of the requirements for the

award of the degree of

DOCTOR OF PHILOSOPHY
in

(Computer Applications)

By

Md Iman Ali

Registration Number 41800264

Supervised By

Dr. Sukhkirandeep Kaur

LOVELY PROFESSIONAL UNIVERSITY
PUNJAB
2022

Declaration

I declare that this thesis titled “Cyber Crime Digital Forensic Readiness Secured BYOD Environment” has been prepared by me under the guidance of Dr. Sukhkirandeep Kaur, Assistant Professor, Computer science and Engineering in Lovely Professional University. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Md Iman Ali
School of Computer Applications,
Lovely Professional University,
Punjab
Date: 5th July’2022

Certificate

I certify that Md Iman Ali has prepared his thesis entitled “Cyber Crime Digital Forensic Readiness Secured BYOD Environment” for the award of Ph.D. Degree of Lovely Professional University under my guidance. He has carried out the work at the Department of Computer Applications, Lovely Professional University.

Supervisor

Sukhkirandeep

Dr. Sukhkirandeep Kaur

Date:5th July’22

ABSTRACT

Bring your Own Device (BYOD) service offers internet access to employees' own devices. It is a provision to provide internet access to employees' smartphones, tablets, and personal devices to improve employee work efficiency in today's digital era. Intel was the first organization to adopt this technology in the year 2009[1], later in 2012 slowly and gradually majority of the organization has started adopting BYOD services. The Enterprises are investing more in BYOD infrastructure because organizations are benefiting by providing lesser devices to their Employees. BYOD becomes a rule rather than an exception, BYOD is the alternate way of working method in the corporate. As per Gartner, BYOD users will be increased to 75% by 2022[2] from 35% in 2018. By 2021[3] maximum organizations are expected to use IoT; approximately, 94% of the organization will adopt IoT as per Microsoft report. Enhanced employee satisfaction, increased business productivity, collaboration, and mobility are key reasons for adopting BYOD in the enterprise.

BYOD also brought the associated risks because of exponential growth in the number of cybersecurity incidents due to which business eco-system gets disrupted and fragmented. Although several methods and mechanisms have been developed as well as adopted to mitigate the risk associated with BYOD. They still portray a challenge as the corporate network gets exposed to inherent threats caused by the BYOD threat landscape.

The first part of the research explains the onboarding of the BYOD users on the corporate trusted network, authentication mechanism has a significant role in reducing attacks. A secured BYOD Design architecture and implementation process were analyzed. A practical approach is conducted in this research in securing BYOD infrastructure. Post successful simulation of BYOD onboarding technique using certificate-based authentication model, this is concluded that new approach is secured and reducing risk in BYOD.

The second part of this research contributes to a new method of detecting and protecting malicious activities which can't be otherwise detected and protected by traditional security technology like IPS, IDS, Anti Bot, or Antivirus. The proposed technique compared to the existing methods led to a significant contribution in identifying the threat before an attack takes

place. During the detection process, various options are explored to detect the malicious traffic so that categorization of the malicious attack/ traffic can be achieved. More attention was paid to the detection process and finally “Detection” model was developed to detect malicious traffic in this research. Post detection of malicious traffic simulation extended to protect the critical infrastructure by developing the “Protect” algorithm to build an efficient secured BYOD environment. Lastly, this phase of research outcome contributes to building a Cyber-defense BYOD environment and cyber forensic BYOD ecosystem to defend the critical infrastructure of the organization.

The existing solution in BYOD cyber forensic model has limitations in doing end-to-end forensic investigation post an incident. Threat hunting mechanism is another limitation in existing solutions. Our third objective overcomes the limitations by implementing the Next Generation Digital Forensic (NG-DFR) Readiness Model. The third phase of this research contributes to defining a new approach of the Next Generation Digital Forensic (NG-DFR) Readiness Model to build a cyber forensic ecosystem so that a cyber secured BYOD environment can be enabled safely. The final outline is proposed as the next-generation digital forensic readiness (NG-DFR) model. A detailed progressive process is described to complete the cyber forensic ecosystem. This includes policies, processes, technologies, humans, and integration. Integration of process and technology with human interaction area covered to build cyber forensic BYOD environment.

Acknowledgment

My sincere and lovely gratitude would be expressed to my supervisor Dr. Sukhkirandeep Kaur for her patience, support, guidance, and encouragement from the start to the completion of my Ph.D. studies and thesis writing. May the good Lord bless you abundantly and increase you from grace to grace.

To all the panel members of SOTA, End Term Seminars and Research Degree cell, I say thank you for providing critical and constructive suggestions during the progress reports and presentations. Without you, my research would not have been kept on track.

Contents

List of Tables

List of Figures

List of Algorithms

List of Pseudocode

Chapter 1: Introduction

1.1 BYOD (Bring Your Own Device)

Bring your Own Device (BYOD) term used to refer in providing secured internet access to employees' personal devices like smartphones, tablets and guest users in the corporate environment. BYOD aims to improve employee productivity and satisfaction, increase business revenues, enhance collaboration, mobility and address changing working preferences. Intel was the first organization to adopt BYOD practice in the year 2009[1], then later in 2012 most of the organizations started adopting the same.

During the initial stage, most of the organizations decide not to give network access through the corporate network due to security risk involved in BYOD infrastructure. However, in later stages, organization started understanding the benefits of BYOD and began moving towards positive direction. BYOD is becoming a rule rather than an exception as it offers the alternate way of working model in corporates. One of the major purpose for the enterprise to move in BYOD infrastructure is minimizing investments by offering lesser devices to employees.

Study indicate BYOD users will get increase by 75% by 2022[2] from 35% in 2018. By 2021[3] maximum organizations are expected to use IoT approximately 94% of the organization will adopt IoT as per Microsoft report.

1.1.1 BYOD Evolution

Bring Your Own Device (BYOD) replaced "Use What You are Told" (UWYT). UWYT was the old established term used in the corporate environment for employees. It was the model where employer had full control over the devices to use for work[4] in the corporate environment. UWYT was not having any security issues but in that approach there was no life and work balance. In UWYT organizations had fully tight measured over the devices used. In terms of information security standard endpoint and rules applied to reduce risk, UWYT approach was not able to provide the required synchronization between personal and work life[5].

Then, the subset of consumerization of IT , i.e. BYOD or Bring Your Own Device came into play so that employees can use same device for both personal and business purpose[6].

This shift was triggered by new generation and thoughts of the employees who demanded flexibility and freedom from controlled devices. According to HP survey in 2013 , more than 50% employees were using more than three devices for work and IT department was facing difficulties to trace [7] all the sources . In order to fulfill the current demand and after continuous evolution, BYOD turned into better solution.

1.2 Cyber Crime and Cyber Security

Cyber crime is defined as a crime where computers or mobile devices are used as an object to commit the offense. In this digital age, cybercrime is one of the major threat worldwide which counters integrity, confidentiality, and accessibility of attacked computer data or systems [8]. Cyberattacks are increasing exponentially day by day and hampering confidential data, corporate information, thereby interrupting businesses and posing numerous negative impacts. According to a PWC "Global Crisis Survey[9]" report on Major Crises, organizations with 5,000 or more employees are most likely to experience crises related to cybercrime which is 26% of the overall crisis.

Cyber security is the concept of detecting and protecting the network of computers, confidential information of the organization and individuals from unauthorized access or any security breach. Cyber threat is the Second highest risk for the organization as per KPMG 2018 Global CEO outlook [10].

Digital transformation of the business is a necessity in today's business model as cybercriminals are targeting cyber infrastructure and computer networks. BYOD infrastructure is also becoming the target of cybercriminals. Exploitation of smartphones, data theft, and malicious activities are increasing due to poor security models in BYOD infrastructure. Providing internet access in BYOD is a major cybersecurity risk and can lead to concerns of security, data leakage, loss of control, etc. if proper security practice is not followed[11]. For instance, BYOD is one of the challenges that falls in smart city development as a major cybersecurity risk[12] today. The latest technology trend of the BYOD has escalated the risk of cybersecurity in airports [13] which is a critical infrastructure of security.

1.2.1 Different Types of Cyber Security

Cyber security consists of various computer security aspects of preventing and defending networks, devices and electronic systems from threats. Typical cyber security practice consists of people, processes, and technology that can be broadly classified into following-

1.2.1.1 Network Security

Network security threats are the major concerns for attackers as they can gain access to core infrastructure and lead to major cyber attacks. Network security ensures the reliability and integrity of network that ensures network is secured and reliable to use[14]. Its core components include Ant-Virus, Anti-Spyware, Firewall, IPS, IDS, VPN. The strong Network security model ensures that attacks are detected on time and thereby infrastructure[15] is protected. A zero-day attack is part of network security detection.

Network Security is a very complex and challenging area for the organization's infrastructure. Though, continuous study, research and development of the technology to protect the network is ongoing; but still, network cyberattacks are increasing, not completely resolved and far away from the solution[16]. Researchers are giving high priority to this area and all the original equipment manufacturers (OEM) of the security products are working to secure the network but still volume of network cyberattack is large.

1.2.1.2 Application Security

Application cyber security is the measure of security during the life cycle of development of the application and protection of the application from threats. During application development, deployment flaws in the design result in risks of cyber threats to the application. So, to minimize risks during application access, session management is kept as focused area of application cybersecurity. Input parameters, role-based access authentication and authorization are implied for application cybersecurity where audits, logs, and parameter interchange are major key components[17].

1.2.1.3 Information Security

System’s digital data is the vital property of the organization . Protection of asset[18] that digital data is information security. Access management, authorization, and identification are the area of information security. Cryptography is one of the techniques to address information security[19].

1.3 BYOD Cyber Security

In the BYOD infrastructure, unmanaged external devices using wireless infrastructure and resources of the organization increase the risk of cybersecurity incidents. BYOD networks are used by cybercriminals to perform malicious activities when a proper security mechanism is not implemented within the networks .

In BYOD network, attackers try to get access of internal and cloud networks to perform malicious activities and damage the potential data, causing reputation loss for organization. Installing malware and accessing the internet from BYOD infrastructure can also lead to serious damage. BYOD environment has huge security risk[20], so the devices owned by employees, suppliers, or partners, must be secured to ensure corporate data protection while isolating the personal data. Therefore, data theft, shadow IT, and cyber security are major concerns in BYOD.

Impact evaluation of BYOD security in research study of the Airport Smart System describes that compromised BYOD devices can impact system integrity and availability[21]. Security breaches are more in BYOD network infrastructure where employees, partners, and staff utilize their own devices. Therefore, with BYOD adoption, security should be considered at all the stages.

1.3.1 Cyber Security for On-premise Data Center and Cloud Data Center

Adoption of new technology is always a trend in the organization. Cloud transformation is majorly adopted and by organizations for ease of accessibility and improve flexibility. Accessing cloud services using BYOD is an additional risk for the organization[22] due to potential security risks.

1.3.2 Cyber Security for BYOD with SD-WAN

SD-WAN refers to decoupling of the network hardware for control and data plan to improve security . This technology is driven for digital business transformation[23] and fulfilling growing business demands for on-premesis and cloud-based application deployment. Adoption of SD-WAN trend in 2018 is 40% and expected to be 90% by 2023[23]. BYOD services over SD-WAN to ensure performance, throughput, and prioritization are the major area of concern. BYOD traffic flow and segmentation over SD-

WAN and how this traffic will be encrypted without having any touch point over corporate network has become an area of study.

1.4 BYOD Secure Authentication

BYOD User Authentication Mechanism is an important area of attention to secure the network. To understand how BYOD users get authenticated and provisioned in organization network to provide internet access is a crucial part of BYOD infrastructure design. There are various ways to authenticate users, like an authentication mechanism using BAP [24](Blockchain Authentication) which is one of the secured models of the BYOD onboarding process. Some of the other authentication methods are discussed below.

1.4.1 BYOD User category classification

BYOD users' identification and classification is a crucial part to identify users to whom, accessibility will be offered in BYOD infrastructure.

1.4.2 BYOD authentication using Blockchain technique

BYOD authentication process is the area where the majority of the security concerns are required to be addressed. Out of multiple authentication methods, the Blockchain authentication process was studied to address the weak security models. Blockchain authentication is a record-based authentication process that enhances security and prevents data leakage[24].

1.5 BYOD Cyber Threat

BYOD adoption has become a necessity for the organization with changing work environments and internet dependency. The traditional BYOD model is not effective enough to identify and protect networks against continuously evolving cyber threats. Advanced threat identification and protection mechanism are required in the BYOD technology framework.

1.5.1 BYOD Threat Identification

When organizations do not have any awareness of the security measures to be taken to protect BYOD infrastructure, or devices are lost or stolen, threat landscape increase. Identification of such cases is primarily the goal for threat identification. Apart from this while networks is unsecured this becomes one of the major reason for threats and hunting

those threats in a poor or unsecured network becomes a major reason for threat protection. The malicious pattern of traffic in the network sometimes hints at threat hunting. Also, unsecured data transfer becomes the major reason for the threat landscape increase.

The primary objective of threat identification is to achieve complete visibility of the network traffic to detect and categorize threats. After the classification of a threat, the next action becomes the protection of the critical infrastructure. Threat identification and comprehensive security measures can maximize user efficiency and satisfaction along with protecting critical infrastructure of organizations. Reducing the cost of the infrastructure and increasing business agility is the key approach for threat identification.

1.5.2 BYOD Threat Protection

Different tools and technologies developed and adopted to protect critical infrastructure and even the research in academia and industries have increased in this direction but are not sufficient enough to fight against today's threat landscape.

The research was conducted to detect and protect critical areas of BYOD like the secure onboarding process so that threats can be eliminated at the initial level. This process was formalized in multiple studies. Secure onboarding process was also [25] developed and encryption practice revealed for securing corporate networks [26]. Different tools and techniques were developed to protect the BYOD infrastructure like Scyther Tool combination with dual-factor verification method [27]. Many different processes and methods were developed, tested and multi-directional results were projected. But apart from technology development, many more dimensions are important to protect the BYOD critical infrastructure like process, awareness, BYOD policy framework, cyber law based on country or region, etc.

1.5.3 Cyber threat global risk ranking

Cyber threat ranked in top three major global risk[28]. The increased trend of WFH (Work from home) option and alternate method of the working environment enablement increases the risk portfolio. Cyber-attacks are consistently becoming a global risk factor as per the

study of the Cyberthreat Global Risk Index. Risk position index from 2012 till 2020 is shown in figure below.

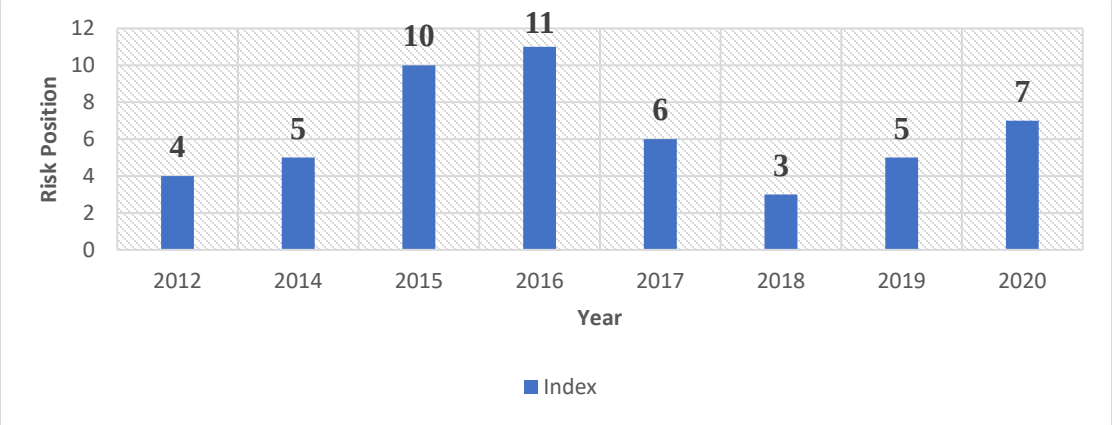

Fig 1. Global risk in terms of likelihood [29]

Multiple government cybersecurity agencies are sharing information which can appreciate more risk of cyberattack and can finally damage the country's economic situation and also increase geopolitical tension. In order to reduce the impact of cyberattack, a collaborative approach of incident response system is required [29]. Also, a trustworthy cyber infrastructure and cybersecure ecosystem is required specially in BYOD where cyber risks are high.

1.6 BYOD Forensic

BYOD cyber security technology and policy has a strong correlation with cyber forensic. BYOD forensic ideally been expected to strengthen BYOD model and cover all the threat-related activities. It includes detection of threats thereafter classification of the threats, attacks and identification is done. Post an incident all activities performed in reverse mechanism and proof generation technique include in BYOD forensic module. BYOD forensic module called after an incident to classify, identify the logs and artifacts which is digital evidence. Threat hunting is a process of collecting digital evidences , analyzing them and find the source of attack post a cyber-attack is a major challenge in building a cyber secured BYOD forensic ecosystem.

1.7 BYOD and Cyber Forensic

Internet users are increasing exponentially by using IoT/BYOD in every organization, public environment, and now in smart city infrastructure. Along with it, cybercrime rates are exponentially growing and this is a challenging area to handle and investigate post-incident. Government and public/private sector need to gear up to fight against this major crisis.

Govt of India has taken an initiative to enhance the infrastructure of the National Cyber Crime Lab (NCFL) and started a new project called "CyPAD"-Cyber Prevention, Awareness & Detection Centre by Union Home Minister on 18th Feb'2019[30]. Union Home Minister has pointed out that cybercrime becomes a big challenge to handle.

1.7.1 BYOD and Digital Forensic

Post an attack there is a need for forensic investigation in BYOD. Major components in digital forensic investigation are[31]

- Computer forensic
- Network Forensic
- Database Forensic
- Mobile forensic

Digital forensic or cyber forensic ideally include [32] (a) human, (b) digital evidence, and (c) process, which act as a reference point. BYOD has all those components to be covered in forensic investigation.

According to Juniper Survey, 80% of BYOD devices will be unprotected in future. There is a need for secure BYOD infrastructure which should include components of digital forensic investigation. A large-scale clustering deployment of BYOD infrastructure needs a digital forensic readiness model for detection and investigation[33].

DFR (Digital Forensic Readiness) in BYOD infrastructure is one of the model which is used to detect the attackers' activities and in-depth behavior analysis using Honeypot deception technology. An extended study has been conducted to mature the approach of DFR and CTI (Cyber Threat Intelligent), digital forensic investigation and to reduce the time and cost. The accuracy level was achieved in analyzing the root cause post-incident

up to 90.73%[34]. This is an extended study on deception technology which improved the maturity level of DFR model.

1.8 Motivation

The whole world is experiencing exponential growth of cyberattacks. Cybercriminal has created a panic situation in the growing internet world. Organizations are experiencing cyber-attacks and challenges to conduct digital forensic investigation of the crime due to the lack of digital forensic evidence which is resulting in loss of organization reputation. Prediction of cybercrime by 2021 is $6 trillion annually as per research done by cybersecurity ventures in 2016[35].

The majority of the organizations are moving towards BYOD which could be the invitation for external attacks or cyber attacks.However, an efficiently secured BYOD Authentication model can reduce the number of attacks. Additionally, Digital forensic readiness of BYOD infrastructure can help in conducting a digital forensic investigation. Thus, the need of secured BYOD infrastructure to minimize cyberattacks motivates further research in the BYOD authentication area.

1.8.1. Need of advance level of cyber infrastructure

Mumbai TAJ terror attacks in 2008 established the fact that India needs to become more equipped with cybersecurity infrastructure to respond to digital intelligence based information. Unlike cyber network of US that saved them from multiple cyber attacks, Mumbai police overlooked the importance of those tools and technologies. The study also articulates this attack could have been avoided[36] if India's Cybersecurity infrastructure would have forward-thinking technology.

Cyberinfrastructure is all about internet users which include BYOD users also. This motivates to explore further and help the nation to reduce cyberattacks by analyzing traffic behavior, patterns and malicious activities. This example shows that advance level of digital forensic system is required to quickly analyze any information.

1.8.2. Need of next level Cybersecurity Policies

22nd March 2018 attackers attacked encrypted files and destroyed valuable data in Atlanta Smart city[37]. This cybercrime was not detected due to lack of immediate investigation, advanced cybersecurity infrastructure and cybersecurity policy strategy[38].

The Identity Management System is the area where detection and protection could have been done. This incident triggered for further study to reduce attacks at the initial stage of authentication, and detection to prevent malicious attacks.

1.8.3 Need for Digital Forensics

Post-incident, root cause analysis is a critical requirement for fact-finding which is nothing but digital forensic evidence analysis. A hospital in California was shut down for a week time post a cyber attack[39] but it took longer time to identify the root cause.

Above mentioned attacks proves that cybercrimes are growing exponentially and to overcome current cyber attack nature, organizations need an advanced layer of defense model.

In increased Cyber threat landscape, Network Cyber Incident and Cloud Cyber incident has a very strong relationship with BYOD infrastructure. The impact of cybersecurity risk [40]on business due to BYOD adoption along with mitigation strategies is an area to study further. According to the analysis done on Security of the Mobile Device [41]which was prepared by the Department of Homeland Security (DHS) in discussion with the "National Institute of Standards and Technology (NIST)" several communication routes remain unprotected and leave the general ecosystem weak to vulnerable attacks which calls for further research.

Mobile devices are the weakest link to Cybersecurity threats and data leakage of the organization. Similarly, BYOD have insider concerns of data breach and security risk. Thus, BYOD solutions should be efficiently secured to address cybersecurity threats otherwise BYOD infrastructure can create panic for lots of organizations.moreover digital forensic ecosystem is required in any BYOD solution.

1.8.1 Network Snipping

Network attacker can connect their rogue access points and get access of the corporate network for carrying out snipping and phishing activities[40].

1.8.2 Network congestion

By getting access to the corporate network, congestion can be created by generating a huge volume of traffic by the BYOD devices in the network. As a result, the entire network can

go down and impact the business. Generally, this type of attack is triggered by attackers using a DDoS mechanism.

1.8.3 DDoS Attack

Shutting down a system or network infrastructure and making it inaccessible is the Denial-of-Service Attack. In this case, more traffic is sent by the attacker which can't be handled by the system. As a result business ecosystem gets fragmented. A single device is sometimes used to attack from a single location and in case of a DDoS attack, multiple locations are attacked. DDoS attacks are deployed faster and the speed of attack is also faster so it becomes more difficult to track. DDoS attacks normally use multiple remote machines or bots to send higher traffic to crash down the system. Tracing the source of the attack is much more difficult in a DDoS attack[42]. Various forms of DDoS attacks are mentioned below[42].

1.8.3.1 Teardrop DoS attack

A DoS attack sends countless IP fragments to the network infrastructure and creates anomalies.

1.8.3.2 Volumetric DDos attack

This category of attack is ideally targeted to over-utilized bandwidth. A large amount of ICMP messages are sent so that high bandwidth is utilized to make the network inaccessible due to overutilization.

1.8.3.3 Flooding attack

This type of attack happens when multiple connection requests send to the destination but the transaction never completes.

1.8.3.4 Protocol attack

Normally such attacks happen in Layer 3 and Layer 4 of the OSI model. Like exploiting TCP connections, used spoofed IP addresses that send connection requests

1.8.3.5 IP Fragmentation attack

In this pattern of attack altered network packet is sent so that the destination side cant reassemble. All resources are used and due to bulk packet network turn into bogged down situation.

1.8.3.6 Attack on Application-based

This category of DDoS attack normally happens in Layer 7 of the OSI model. This type of attack is very critical to detect as it sends partial packets.

1.8.3.7 Other attacks in this category

Various types of DDoS attacks also include Zero-day attacks, HTTP flood, NTP amplification, ping of death, etc.

1.8.4 Cloud Services

Due to the exponential growth of mobile device usage in work environments organizations are moving to cloud services for flexibility of work. For instance, Microsoft Office 365. Cloud services including shared services and shared security models are also increasing the number of cyber incidents [43] and compounding cybersecurity challenges. Security solutions is a key area in BYOD. Moving to the cloud and increasing the use of BYOD[44] has increased cyber security risk and has a positive correlation. More devices leads to more risks as BYOD devices are used to download malicious apps and cloud connectivity create more cyber risk. Cloud security is one of the areas to develop security model analysis and secure the cloud to reduce cybercrime activities.

1.8.5 Digital Forensic

Post-incident analysis of the root cause, finding facts, accessing the logs, securing and getting data from such disparate sources is a very challenging[45] task from the BYOD environment. Building the secured infrastructure in BYOD can give the right direction of creating forensic ecosystem.

Along with it, BYOD security policies are required for robust computer forensic investigation process post-incident. Due to the inherent risk for allowing untrusted devices in the network[46], BYOD security policies need to be strict. Digital forensic also includes digital evidence recovery which is one of the challenges in BYOD infrastructure that needs to addressed.

1.8.6 Open Issues and Challenges

There are multiple open issues in the existing BYOD authentication model and BYOD digital forensic infrastructure where further study can be conducted.

1.8.6.1 Authentication

Authentication is the starting point of the backdoor for an attacker, auditing and accounting of the malicious activities need to be defended in the entry point itself. Conventional techniques of authentication are prone to attack[24]. So secured model of BYOD authentication implementation is required.

1.8.6.2 Security

Advance Security is a must to have a requirement in a BYOD environment. More the secured network is, less is the risk, so improvement in the BYOD security model is required. Since cybercriminals are using advanced tools and technology to conduct criminal activities, so advancement of the security model is required in BYOD infrastructure.

1.8.6.3 Digital Forensic Investigation

One of the biggest challenges in the forensic investigation post-attack or any malicious activities is the lack of a proper detection model. Attackers can move and exit after an attack and break the chain of custody. Threat hunting, source of attack and chain of custody are the major challenges in digital forensic investigation. Further study needs to be performed for in detail forensic investigation to collect the data, preserve, analyze and present the digital evidence as required by the court of law.

1.8.6.4 Guest traffic over MPLS or Corporate Leased Internet link

Either authentication traffic or actual data traffic flow over MPLS is a risky environment. Also using corporate IP addresses by BYOD users can be a disaster situation due to the blacklisting of IP by a third party. So a secured model of traffic flow mechanism is required to implement.

1.8.6.5 BYOD over SD-WAN

Segmentation of the guest user traffic over MPLS is a major area of study where all corporate data traffic destined to be in on-prem data center or cloud is merged in a single SD-WAN device. Security features of SD-WAN are a major concern today because most of the SD-WAN OEMs are not even integrated with Palo Alto or Checkpoint Security VNF to protect in the first layer of Defense. Also, there is a challenge of secured authentication

of BYOD over SD-WAN with centralized authentication and forensic investigation framework.

1.8.6.6 BYOD over Cloud

Organizations are moving towards cloud service adoption in shared infrastructure. BYOD users accessing cloud services and traffic exit with organization's registered IP address becomes a challenge and open path for accessing cloud services using corporate register IP address range. There is a need to study in detail for BYOD traffic going towards cloud and also cloud security architecture. BYOD and cloud security architecture are major area for threat hunting and source of the attack.

1.9 Objectives of this Research

This section describes the objective of the Research.

1.9.1 Secure Authentication

Design a novel approach for a secured onboarding process during authentication of BYOD users to make the network free from cybersecurity risk.

1.9.2 Threat Detection and Protection

Analysis, detection and protection of BYOD malicious activities for digital forensic investigation.

1.9.3 Next-Generation Digital Forensic

Post cyber attack in BYOD infrastructure finding the evidence of the crime is a critical task, the objective is to find the source of the attack, analyze and preserve the evidence, and then present that as per the requirement of the court of law. Next Generation level of advanced Digital forensic readiness model on BYOD infrastructure is a demand in industry to complete the digital forensic investigation, therefore designing Next Generation Digital Forensic Readiness model in BYOD infrastructure post cyber attack is an important objective in this research.

1.10 Contribution

In this research work, we proposed a secured and scalable solution to the BYOD environment. Proposed methods and techniques are simple and efficient to implement in the BYOD environment to protect the organization from the threat landscape.

This work consists of major 3 parts. The first part of the research work focused on the secure onboarding process of the BYOD environment so that major risks can be minimize at entry level only. The second part of the work is focused on the detection of malicious activities in the BYOD environment. The third part contributes to protecting the organization's critical infrastructure from detected threats. In the fourth phase of this research we have projected a unique method of building end to end Cyber forensic ecosystem called the Next-Generation Digital Forensic Readiness model or NG-DFR model. Finally, our research aimed to build a cyber-secure BYOD ecosystem.

1.10.1 Certificate-based Secured Authentication model

Onboarding of BYOD is one of the major areas of study. Various methods and techniques are developed to onboard BYOD. However various incidents proved that even after so many methods, the BYOD onboarding process is not secured or security issues are not addressed as a result threats are increasing. Various techniques are used in different organizations but every method has its loophole and attackers get the chance to attack. Out of all the available authentication models, the certificate-based authentication method is considered as best secured mode of authentication.

Below are the major components used in creating a secured onboarding process

- AAA: Authentication, Authorization, and Accounting used for authentication purposes. All requests are redirected to AAA for connecting internal user database to validate the user
- Internal user Database (AD): Active directory used to validate the BYOD user with activate/deactivate status. All valid users of the BYOD are existing in this database.
- PKI certificate: Public Key Infrastructure is used for secured certificate-based authentication

- Wireless Controllers: Wireless controllers are used for relaying traffic for authentication.

In this work, we have used a certificate-based authentication model which is considered the most secured model of authentication. Also correlation and integration between authentication server, user database, user certificate and user ID and password is established. A strong method to validate secured authentication method is created to demonstrate the work. We have designed a new architecture for the secured onboarding process to make the network risk-free.

For onboarding BYOD users, several techniques and mechanisms are being used however, the certificate-based authentication technique is considered to be the most secure and reliable. While continuing BYOD research and studies a loophole is identified in secured certificate-based authentication. After thorough investigation and studies, a protection mechanism is developed to mitigate the loopholes.

1.10.2 BYOD Cyber Threat Detection and Protection Model

With growing numbers of internet users and dependency on internet connectivity even for basic tasks, it has become necessary to provide internet connectivity to employees, contractors and guests visiting offices while keeping the attention on all security aspects of corporate infrastructure as well as users data confidentiality to reduce the risk of emerging cyber threats. Securing corporate networks and advancing the detection method for suspected malicious activities is an ongoing research area where continuous advancement is required. This study encourages secured BYOD environment adaptation and cyber secured ecosystem in the corporate infrastructure.

1.10.3 Next Generation BYOD Forensic ecosystem

Cyber attacks on critical corporate infrastructure are getting increased, hampering business operation and reputation as there is no mechanism developed to defend against cyberattacks in BYOD environment. This alarming situation urges us to develop a BYOD infrastructure and mechanism which is secure and ready to defend against cyberattacks in

the organizations from next level cyber threats. In this study, a cyber forensic structure is proposed considering the cyber secure BYOD model.

In the first phase of research, threat detection technology is discussed considering various tools and techniques for further research and analysis.

In the second phase of the research, after addressing the loophole in the system a novel approach is proposed which is threat identification and cyber defense mechanism for zero-day attacks which are not identified by the conventional technologies such as IPS, IDS, antibots and antivirus. After compiling the study and research results, an advanced cyber forensic environment is developed which contributes to cyber secure BYOD enabled corporate infrastructure.

After a cyber-attack collecting digital evidence, artifacts and threat identification is required in a cyber forensic investigation which is described in the research using various methods and technologies such as Sandblasting and Cortex.

At the final stage of the research, The Cyber secure and Cyber Forensic readiness BYOD outline is achieved. In order to address the requirement of digital forensic investigation and to create reliable, cyber-secure BYOD infrastructure, a Next-Generation Digital Forensic (NG-DFR) framework is developed.

1.10.4 Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment

Cyber security risks and threats in existing BYOD model encourage to develop an efficient cyber-secure BYOD framework with the readiness of cyber forensic ecosystem. Thus, Identification of risks and threats inside BYOD infrastructure is the important objective of the research.

Adopting and enabling BYOD is an important requirement of organizations but it is not safe to allow untrusted insecure devices to use corporate network services. Thus, there is a requirement to develop a detection mechanism and a cyber secure BYOD ecosystem for

securing the corporate network from untrusted BYOD users along with detecting and eliminating malicious traffic. With help of this research, a method is developed to investigate malicious traffic and offer reliable framework to enable BYOD infrastructure using various control methods like Checkpoint and Palo Alto.

1.11 The organization of this thesis

The remaining part of the thesis is organized as-

After the current introduction chapter, we have provided a detailed literature review mentioning the existing study in the area of BYOD authentication along with evolution of security tools and technology. Further in chapter 3 to 6, the contribution of this research work is mentioned. In chapter 3 we proposed a novel approach of the secured authentication model to protect the organization's critical infrastructure from unauthorized access. In Chapter 4 we have proposed the detection and protection model for secured BYOD environment. In chapter 5 we have analyzed BYOD cyber forensic ecosystem. This includes end-to-end digital forensic ecosystem in the BYOD environment. In Chapter 6 which is the last section of the contribution, we proposed the Next Generation Digital Forensic Readiness Model. Finally, chapter 7 described the conclusion and future work.

Chapter 2: Review of Literature

Most of the research conducted in this area are mentioned in Golden age of Digital Forensic (1997-2007). However, there is still a need for a standard, modular[47]approach to digital forensic. Though new technologies are adopted, the deployment approach has been changed but there is no single mitigation technique[48] evolved due to changing nature of cyber attacks. Thus, continuous evolvement in forensic technology is required as stated in a study by Deloitte[45] as well.

2.1 BYOD Network Architecture

We have discussed in detail different BYOD key areas, technology framework evolution and different methods of services. Various components of BYOD services are discussed in the next subsequent sections.

2.1.1 BYOD Technology framework

Bring Your Own Technology (BYOT) delivers the basis for changing the organization into a new system of the working environment. Since 2009, BYOD adopted by the organization [1] and incremental development was observed on various processes, tools and techniques. Security concerns, awareness of the users while giving access to BYOD and policy frameworks in protecting the critical infrastructure of the organization are their fundamental needs.

To enable the BYOD services securely, so many techniques, products and technologies have been established by researchers and OEMs. The major focus in this area is observed as data security, authentication, cybersecurity, forensic ecosystem procedures and policies. Apart from this layered security is also proposed in BYOD environment to protect critical infrastructure[49]. However, most of the research contributed and framed the abstract in terms of theoretical and practical approaches for enabling the services and developing the framework. The outcome of this development has shown tools and techniques in data security, cybersecurity, secured authentication, honeypot technology to detect attacks, protect, and then forensic investigation.

2.1.1.1 BYOD Design Architecture

Shadow IT and data theft in the BYOD infrastructure are considered to be the biggest concerns. Another major concern is to revoke internet access while the employee is no more in the system or left the organization. Connecting malware while BYOD devices are part of the internet leads to major damage and cyberattacks to critical infrastructure.

Poor BYOD design significantly leads to organizational cybersecurity risk. This major concerns need to be addressed for better designing of BYOD infrastructure. Data protection and privacy concerns are two key aspects that need to be taken care of while designing BYOD environment. Both the concerns can be addressed by providing security policy guidelines for safer access to the BYOD infrastructure. Data leakage is another concern in BYOD, which carries the potential risks for organization. Incident identification, detection, protection, and at last forensic model development has become the fundamental need of designing BYOD infrastructure.

2.1.1.2 BYOD Onboarding tactics

Enabling internet access to external devices using BYOD in corporate network has multiple challenges which increase significant security risk. Major concerns such as data theft, damage of critical infrastructure, damage of organization reputation, business disruption etc can rise in the organizations if onboarding techniques are not secured. This indicate the need of secure BYOD model. Secured prototype of BYOD implementation helps organizations to lay down BYOD security policy in securing the network. Onboarding techniques are ideally expected to cover all the parameters of security concerns in BYOD. Onboarding technique should also contribute in BYOD malicious traffic detection, suspicious traffic detection mechanisms. Primarily onboarding technique is more focused in authentication related parameter. Authentication techniques and threat modeling are the key dimensions for designing onboarding tactics of BYOD infrastructure. Additionally, onboarding technique should also contribute in the required parameters of BYOD forensic.

2.1.2 BYOD Security Technology Evolution

Bring your Own Device (BYOD) is the strategy followed by most organizations [25] for providing internet access to the employee's personal devices using corporate IT infrastructure. At first, Intel adopted this technology in 2009 [1], and post 2012 other organizations adopted and slowly this has become a fundamental need for the enterprises. This strategy increased employee satisfaction and improved business efficiency, collaboration, and accessibility. The characterization and classification of Bring Your Own Device (BYOD) matured over time. Creating an alternate method of the working environment using BYOD becomes a fundamental need for the organization but this strategy also called serious threats for any organization. Thus, the cyber threats has become a business survival issue and not only a technical challenge.

Global PWC Survey "Global Crisis Survey[9]" says, the digital business risk for today is cybersecurity risk. Subsequently, 'cyber threat' is considered as 2nd highest digital business risk in "Global CEO Outlook" [10] conducted by KPMG. Also, cyber threat has become the fastest global jeopardy as per the study of World Economic Forum(WEF). WEF introduced the Global Centre for Cyber Security in 2018[50] to combat with cybersecurity threats.

Adoption of BYOD services in the corporate environment was expected to grow from 35% to 75% by 2022[2] as indicated in 2018 but Covid-19 increased this demand even more. Since the adoption of BYOD increased and the BYOD is less secured, cyberthreats are becoming a worldwide business disruption risk factor [29]. Being unmanaged devices they contain malicious content[51] and are more vulnerable.

2.1.2.1 BYOD Certificate-based Authentication

Authentication mechanisms were developed and enabled secure onboarding [25] of BYOD user devices. One of the methods is a multi-factor authentication method which is a hybrid certificate-based authentication uses a three-tier captcha. It turned out to be successful and secured authentication method for BYOD infrastructure [52]. Other method was the dual-factor authentication method which is explored using the tool named Scyther for automatic verification of IoT based BYOD devices [27] . Additionally, 802.1x authentication and

security control [53] method were also explored to secure LAN connectivity of BYOD devices.

Considering some additional security measures multifactor authentication model as blockchain model was also explored in the past [54]. Lastly, to protect infrastructure from unauthorized access, data leakage and data breach, a security model based on the self-registration portal method was studied [24]. In the BYOD environment, the certificate-based authetication[25] model is considered to be the most secure model for onboarding of BYOD users. For end-to-end security, encryption techniques are considered to secure the BYOD infrastructure of corporate networks [26].

2.1.2.2 Deception Technology

In the various past research, work has been done for threat detection in BYOD infrastructure. A deception technology called Honeypot was introduced in the year 2016[33]. Fundamental research was done to integrate Honeypot technology with the cyber risk management process of FEMA mission [55] (Federal emergency management agency). Further advancement in the research was conducted in the year 2019- “A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology" [33]. A study was conducted in the direction of intelligent threat platform to identify threats and accuracy of the detection mechanism [34]. To improve accuracy of threat and malicious activity identification, audit logs were collected from intelligent threat sources, as a result, accuracy is analyzed as 90.73%, 96.16%, and 93.71% [34].

2.1.3 Cryptographic Blockchain Method of Forensic

For secure onboarding and authentication of BYOD users, blockchain based Public-Key Cryptography (PKC) authentication method was explored where authentication logs were recorded for BYOD users and a record-keeping ledger was maintained. These authentication logs provides evidence and artifact for cyber forensic investigation and malicious traffic sources [54]. The multi-factor authentication process was also tested with this record-keeping blockchain authentication method[54]. It was explored that after cyber forensic investigation, this record-keeping method can provide critical evidence against

threats and malicious activities, such as image haze removal technique[56] and reverse mechanism in dual-tree complex wavelet transform (DTCWT)[57]. In the IoT environment intrusion detection technique was used with distributed ledger technology to identify source of threats and nature of cyber-attack by collecting digital evidences. This technique helped in cyber forensic investigation and creates a cyber defense ecosystem for corporates[58].

2.1.4 Stride based Threat Model

Stride [59]based BYOD Threat model is proposed and analyzed threat interaction in BYOD. BYOD internal and external threat interaction to the corporate network is analyzed so that security and forensic threats in BYOD can be understood. Also, the forensic analysis mechanism was analyzed for internal and external traffic threats [60]. Reverse adoption of encryption using the Group Encrypted Transport VPN (GETVPN) method of BYOD traffic was a novel approach to detect malicious activities and to reduce the threat.

2.1.5 Threat Interaction Model

The Threat Interaction Model was proposed for analyzing different threats in Stride based model[59] where internal and external threat interaction was studied, which further helped in forensics analysis. However, adoption of GetVPN[61] in BYOD, where corporate and BYOD traffic was segregated, became another part of novel study. Encryption with GetVPN[61] to isolate corporate traffic from untrusted traffic turned out to be reverse adoption for diversification of external and internal traffic[60].

2.1.6 Blockchain-based Authentication for BYOD users

The most successful authentication and onboarding method of BYOD users is a blockchain-based multi-factor authentication model with added security [54] and defense features in the BYOD infrastructure. To reduce the risk of data breach and protect critical infrastructure from unauthorized access a successful self-service portal-based authentication model is also explored in the research[24].

2.1.7 Secure BYOD with Encryption Model

To secure corporates from data leakage and integrity, the encryption-based BYOD model is an efficacious model [26]. Cryptographic end-to-end traffic encryption is a secure method for network security that was studied in recent research of 2019 [62]. Remote site authentication traffic forwarding considering remote access services is a severe issue as traffic congestion can be caused by Distributed-Denial-of-Service Attack (DDoS) [63] which is studied and mitigated in the research using IPS/IDS technologies.

2.2 Cyber Security in BYOD SD-WAN

Cyber security is considered as the fastest increasing global risk by World Economic Forum. To tackle with cybersecurity threat WEF launched the "Global Center for Cyber Security" in 2018[50]. In one of the other report, World Economic Forum concluded cybersecurity has become 3rd major risk worldwide. As per the study of PWC "Global Crisis Survey[9]" cybersecurity risk is a major digital business risk today. Cyber security threat is the second highest risk for the organization as per KPMG 2018 Global CEO Outlook [10]. Cybersecurity is no more a technology issue, this becomes a business survival issue.

In every stage of BYOD infrastructure, security should be always in place for protecting networks, data, and applications. BYOD system becomes a huge security risk[20] as the devices owned by an employee, supplier, partner is not secured. Unmanaged devices might not be following the standard security practice or the line of defense against malicious content[51]. Corporate data protection while isolating personal data in BYOD always needs to be addressed.

Securing SD-WAN is harder and complex[64]. Integrated use of BYOD over SD-WAN becomes a challenging area that required serious attenuation to address. Failure and ignorance of security measures with explosive growth of SD-WAN can cause major security breaches and cybersecurity threats to BYOD untrusted infrastructure. BYOD/IoT with SD-WAN has become flexible routing strategy and a complex area to address cyber threats. The benefit of SD-WAN technology is always explored but the reverse impact of SD-WAN on cybersecurity is a major concern.

When traffic exit from branch location to Internet or interbranch communication over SD-WAN, security become a major concern. Attacks are more likely to take place. Cyber-attacks are exponentially growing where systems are more vulnerable to internal attacks than external attacks. In SD-WAN, the control or the brain is withdrawn from the CE devices and organization data security becomes challenging to address. Cyber forensic investigation is another aspect of BYOD over SD-WAN. Post-incident cyber forensic investigation, cyber security and risk compliance are significant challenges to address.

Any traffic going towards MPLS or the internet should get routed through the firewall first on the basis of the best path parameter. For finding out the evidence after a cyber-attack for digital forensic investigation, an important requirement is to find the source of the attack. Major components in digital forensic investigation are[31] Computer forensic, Network forensic, Mobile forensic, and Database forensic. The digital forensic or cyber forensic component also includes [32] (a) Human, (b) digital evidence, and (c) Process. In SD-WAN technology all these are required to be addressed. Post-inciden finding the source of attack[13] in SD-WAN has become an important requirement.

When traffic was routed through MPLS in a trusted network, this was ignored ideally by the organization, but in SD-WAN this becomes a fundamental need to address. In this study, cyber forensic investigation and threat hunting mechanisms are also addressed using a high-level perimeter firewall.

2.3 Malicious traffic detection

2.3.1 BYOD Threat detection mechanism

Detection of malicious activities was studied in multiple research in the past. Honeypot technology is one of the important key studies done in the past, where detection of malicious activities performed [33] and combination of deception to combat cyber risk management process of FEMA (Federal emergency management agency) mission with five preparedness [55] was explored. A subsequent incremental study was also conducted to improve in another study "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology" [33]. Enhancement of the research was also conducted with Smart Threat Stage to detect the incident and amplify the accuracy level [34]. Using the audit trail mechanism, the accuracy level was increased in finding the source of the attack, and

was investigated as 93.71% then 90.73%, and 96.16% [34]. Another novel approach is defined in evaluating malware infection risk using the machine learning approach[65].
After all, these studies toward detection of BYOD malicious activities have a significant contribution but since the threat landscape increasing every day, more focused explicit novel approach abstraction is required in this area, especially the detection of malicious activities and protection mechanisms.

2.4 Scope

Further research of BYOD secured authentication model and BYOD digital cyber forensic/ computer forensic investigation environment are important for the following reasons -

2.4.1 BYOD Security

The major concern on BYOD is the cybersecurity risk during onboarding and post-provisioning. A secured model of the authentication process will reduce the security risk and will help the organization to run BYOD services risk-free.

2.4.2 Malicious Traffic Detection

One of the biggest concerns of the BYOD users accounting mechanism for auditing and cybersecurity incident analysis is post-incident root cause analysis which starts from the authentication and provisioning period of BYOD users. So, authentication mechanism, secured threat detection, and prevention mechanism is quite important to study.

2.4.3 Digital Forensic Next-Generation Model

Digital forensic investigation model needs to be implemented in a BYOD environment as it would help in forensic investigation by searching digital evidence post incident which is important to present in court of law for finding the criminal activities.

2.5 Existing study and summary of findings

The literature review is an ongoing process during the entire research but the landscape of the existing literature review is given below.

Table 1: Landscape of the existing literature review

Sl No	**Paper Title & Date/version**	**Author and affiliation**	**Volume/issue number/ Year**	**Abstract**	**Finding**

1	Bring your own device in organizations : Extending the reversed IT adoption logic to security paradoxes for CEOs and end users[66]	Paméla Baillette, Yves Barlette, , Aurélie Leclercq-Vandelannoitt.	Volume 43, December 2018	This research focus on BYOD adoption and security risk with BYOD and reverse IT adoption logic	Conceptually this paper has studied the security risk of BYOD. Data security concerns is been addressed with this study. The adoption of tools for BYOD security is been addressed.
2	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology	Victor R. KEBANDE1, Nickson M. KARIE2, H. S. VENTER3	78-1-905824-55-7, 2016	This study is conducted on Digital Forensic readiness using honeypot, a deception technology. This study analyzed and showed an approach on how to conduct digital forensic analysis after an incident and detection mechanism. A new method is proposed for the Security model.	This study has concluded a DFI (Digital Forensic Investigation model using honeypot in BYOD deployment. DFR model has been proposed.

3.	Improving Forensic Triage E_ciency through Cyber Threat Intelligence	Nikolaos Serketzis, Vasilios Katos Christos Ilioudis , Dimitrios Baltatzis and Georgios Pangalos	2019, 11, 0162	A study conducted on the extended approach of DFR (Digital Forensic readiness) in BYOD infrastructure to mature the DRF and reduce time and cost in the investigation after an incident	In this study accuracy of the DFI is conducted, to minimize the cost and time for investigation. Maturity level is increased by collecting patterns of malicious activities from different Threat Intelligent platform
4.	BYOD Authenticatio n Process (BAP) Using Blockchain Technology[24]	Fara Jamal,	Vol. 10, No. 11, 2018	This research concluded a model of BYOD authentication technique using Blockchain, which is considered as a secured model.	The research concluded with BYOD blockchain technique authentication with a self-service portal. This covered the data leakage threat due to unauthorized access. The use of blockchain in the authentication process helps to reduce data leakage and secure the core network from attack.

5	A Novel Approach on Mobile User Authentication for the Internet of Things.[67]	Telu Alekhya , M.K.S. Prasad	Volume 3 , Issue 5,ISSN 2456-3307,2018	User authentication validation technique studied, Two-factor authentication method is the area of the paper	The dual-factor authentication method has been analyzed for secure communication. using Scyther Tool, a computerized dual-factor authentication mechanism is tested as an automatic verification tool with a secured approach.
6	Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology[54]	Fara Jamal , Mohd. Taufik Abdullah , Azizol Abdullah, Zurina Mohd. Hanapi	7 (4.31) (2018) 74-79, 2018	The Blockchain Model of BYOD authentication is the area of research. Record keeping model of authentication is the approach	The multi-factor blockchain secured model is studied. A secured model of blockchain cryptographic authentication model is suggested.
7	A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT[68]	Seong-Kyu Kim , Ung-Mo Kim , and Jun-Ho Huh	Energies, 12, 402, 2019	Blockchain an improved model using spectrum chain is studied.	A base blockchain algorithm is proposed to reduce the security challenges which is weakest in the IoT environment. PKI environment is used.

	Multiplatform Security				
8	Certificate-based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment [52]	Upasana Raj, Monica Catherine S	Vol. 13, No. 12, December 2015	Certificated-based verification mechanism proposed in the hybrid model. During authentication, a potential attack can strike and can create a cyber attack.	This research provided the authentication model using certificates. A Certificate-based authentication method is proposed in general. Attribute-based certificate signing is proposed.
9	Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information[59]	Denys A. Flores , Farrukh Qazi, Arshad Jhumka	2324-9013/16, 2016	In this research, Stride based BYOD threat model is proposed, analyzing threat interaction in BYOD.	BYOD internal and external threat interaction to the corporate network is analyzed so that security and forensic threats in BYOD can be understood.

10	Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang[69]	Astari Retnowardhani, Raziv Herman Diputra,Yaya Sudarya Triana	TELKOMNIKA, Vol.17, No.2,2018	Studied cybersecurity aspect of the BYOD environment to improve security system with a risk analysis of internal data	This research concluded with a framework of BYOD with ISO27002:2013. This paper conducted a study on the BYOD security framework on cybersecurity activities to protect the data with Identity, protect, detect, respond and recover.
11	Diverging deep learning cognitive computing techniques into cyber forensics[70]	Nickson M. Karie, Victor R. Kebande, H.S. Venter	1 (2019) 61e67, 2019	Research is based on Deep learning using machine learning techniques for forensic investigation after the crime.	Deep learning technique, cognitive computing technology for the forensic investigation. A deep learning Cyber forensic framework has been proposed.

12	An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD[22]	Vasileios Samaras1, Semir Daskapan1, Rizwan Ahmad, Sayan Kumar Ray	978-1-4799-5044-7, 2014	This study concept is the security concern on the cloud where BYOD infrastructure is used with an enterprise-level security architecture while accessing SaaS applications through BYOD	This study studied the "Sharewood Applied Business Security Architecture". This paper has concluded the information security architecture of BYOD while accessing SaaS applications on the cloud.
13	Implement Network Security Control Solutions in BYOD Environment [53]	Khoula AlHarthy, Wael Shawkat	978-1-4799-1508-8/13, 2013	This paper studied the BYOD user's authentication process. monitoring and performance parameters of BYOD is focused.	In this study, the authentication process is well framed with 802.1x model. In this study, 2 VLANs have been created to segregate the traffic. In this study storage capacity was also highlighted for logging.

14	BYOD IMPLEMENTATION IN UNIVERSITY: BALANCING ACCESSIBILITY AND SECURITY	Halimaton Sa'adiah Ariffin Zul Hilmi Abdullah2 Shaharudin Ismail Mohd Zalisham Jali	: 978-967-14841-7-3, 2018	The paper focused more on the approach of BYOD security guidelines. Study on university campus environment BYOD internet access	This study proposed a clear solution to be in place for BYOD infrastructure. This study needs extended research on BYOD secured infrastructure to build with proper security policies.
15	Cybersecurity Threats Analysis for Airports[13]	George Suciu Andrei Scheianu1, Ioana Petre, Loredana Chiva, and Cristina Sabina Boso	978-3-030-16184-2_25, 2019	This study is related to Cybersecurity on BYOD in Airport security systems. New-gen E-enabled airport Cyber Security studied	Potential Cyberattack in Airport and aircraft system has been studied. Security approach is required to incorporate in BYOD model. Airport critical infrastructure cyberattack risk is highlighted.

16	SMARTPHONE TRIGGERED SECURITY CHALLENGES - ISSUES, CASE STUDIES AND PREVENTION[71]	Saurabh Ranjan Srivastava, Sachin Dube1, Gulshan Shrivastava, Kavita Sharma	(187–262, 2019	Mobile security challenges have been studied. Preventive measurement to improve mobile security is explored	Mobile-related crimes are explored. Cybersecurity risk is addressed with a set of policies that need to be implemented.
17	Future challenges for smart cities: Cyber-security and digital forensics[72]	Zubair A. Baig*, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew Peacock	1742-2876, 2017	The smart city components are part of IoT. All devices, humans are connected. A network of networks where all components are part of the network. Digital fraud and Cybercrime happened. Forensic analysis and finding out the root cause analysis is the important view	This study especially gives the idea of data security on the cloud. Stored data in the cloud does not have enough control, and location of the data. Since cloud data is not an enterprise control data center, so data accessed by an unauthorized entity is a risk. Data integrity is an important parameter for forensic analysis post-incident

				that has been highlighted. Intelligent artificial is also one of the major points which is been pointed here in this study. Identification of the security threats.	
18	The Future of BYOD in organizations and higher Institution of Learning[1]	Onyechere Ugochukwu Franklin, Mr. Mohamed Ismail Z.	Vol. 3 (No.1), April 2015	This paper study the use of BYOD for learning purpose, benefit, and flexibility.	This paper demonstrated how BYOD is helping the higher education system. This helps in the learning process as explored in this study.

2.6 Gap Identification

This section presents the gap analysis between the existing architecture of BYOD and secured model of BYOD authentication using different authentication mechanisms. BYOD forensic investigation after an incident is the evidence finding technique using multiple technologies. But if the onboarding process can be addressed during the onboarding of the BYOD users, most of the incidents can be avoided. Moreover, after an attack investigation of digital forensic should be conducted and BYOD infrastructure needs to be designed in such a way that digital evidence is available. However malicious activity prevention technology analysis is a major area for further study to protect organization vital data, damage of infra and organization reputation, to reduce cyber attack and post an attack digital investigation readiness infra is required. Different BYOD solution proposed

different solution and below mentioned table explained the work done so far and the identified gap.

Table 2: Gap analysis between different BYOD Solution

Sl No	Author	Year	Work Done	Methodology	Gap Analysis
1	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology[33]	2016	This study is conducted on Digital Forensic readiness using honeypot, a deception technology. This study analyzed and showed an approach on how to conduct digital forensic analysis after an incident and detection mechanism. The security model in DFR has been proposed in this study	Deception technology, honeypot has been used to detect a threat in BYOD infrastructure. This gives the way of doing root cause analysis post-incident	An authentication mechanism can also be considered for BYOD forensic activities. During onboarding of the BYOD users, 1st level of readiness can be performed. A secured way of onboarding can be considered.
2.	Improving Forensic Triage E_ciency through Cyber Threat Intelligence	2019	This is an improved extended study of "A Generic Digital Forensic Readiness Model for BYOD using Honeypot	Using audit logs of malicious activities collected from Intelligent Threat collector,	This study can be extended to the detection and protection mechanism as well. Threat prevention can be the next approach before an incident in endpoint, network, core

			Technology[33]". In this study, the Intelligent Threat Platform is used and detected the incident and accuracy has been analyzed.	accuracy has been analyzed and found 90.73%, 96.16, and 93.71%	infrastructure. Digital forensic investigation and automatic prevention mechanisms can be considered. For further study in BYOD infrastructure.
3	BYOD Authentication Process (BAP) Using Blockchain Technology[24]	2018	Blockchain authentication process has been proposed in this study	Blockchain authentication process has been proposed in this study, Authentication has been done with Blockchain model	Authentication mechanism can be further studied with certificate-based authentication to automate BAP while keeping the same security level to protect the BYOD infrastructure
4	Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology[54]	2018	The cryptographic blockchain authentication process has been studied. Record keeping system has been used for secured authentication of BYOD users. Evidence collection for forensic investigations are	The digital method of the record-keeping system has been used for the multi-factor authentication process	Instead of user interaction more, this can be reduced with certificate-based cryptographic authentication using the key, and authentication parameters.

			also been covered using records.		
5	Cybersecurity Threats Analysis for Airports[13]	2019	Cyberattack and risk are studied in this paper. Airport Security which is a major risk of the country is studied in this paper	The airport Security system in Aircraft and BYOD threat cases has been studied.	An extended study is required in threat hunting modeling in BYOD.

2.6.1 Limitations of existing measures in BYOD environment

BYOD malicious activity detection mechanism consisting of different tools, methods and technologies are already exist and developed over the time. But digital forensic ecosystem needs more advanced level of detection mechanism. Unfortunately, due to the current trend of threat advancement, this is an impending area for building a reliable forensic ecosystem due to threat heterogeneous landscape and complexity. This required considerable dedicated consistent attention towards the inclusion of new abstracts so that digital forensic evidence with end-to-end back-trace capability can be developed with more accurate potential threat detection mechanism. Strongly suspected quite possible to stumble potential evidence related to forensic due to lack of correlation of logs from different components used in the BYOD infrastructure. Due to the back trace of logs and identity, sometimes investigation does not get successful. Also because of huge amount of data and traffic logs from various components, investigations becomes challenging due to the lake of integration between different components.

Existing study in deception technology which is a reactive mechanism been explored to address today's threat landscape[33]. Also, next level of protection approach, cyber threat intelligence and efficiency were explored[34]. Automatic prevention is required post

detection to protect network critical resources from damage which is not present in existing measures.

In another study self-service portal based authentication is developed in order to reduce risk of data breach [24]. However, certificate based authentication did not addressed risk from un-authorized access and onboarding. Also, another certificate-based next level of authentication process of 3 tier model was proposed [52], but again BYOD authentication risk mitigation is missed which elevated security incident even after post-authentication where BYOD user has valid certificate but user id was no longer valid or end date is over. In another study safe provisioning and authentication of BYOD users through Public-Key Cryptography (PKC) blockchain-based authentication process also explored and authentication logs are recorded in a record-keeping ledger. These logs provide indicator and artifacts for cyber forensic investigation and malicious traffic sources [54] where user interaction is more which can be reduced in extended study. Post incident threat hunting modeling is also required to build BYOD cyber secured ecosystem which need tracing back to the source of the attack[13] post incident. More over further detailed gap analysis is presented in section 4.7 in chapter 4.

2.7 Comparison of gap analysis of existing approach in BYOD

This section explained about the BYOD gap analysis of existing approach. Specifically 3 different areas are focused in this section as BYOD authentication gap, BYOD malicious traffic detection and protection mechanism. Apart from this BYOD digital forensic area is also covered to identify the gap. Below table shows the detailed gap analysis and also section 4.7 explained extended further details.

Table 3: Comparative gap analysis of existing study in BYOD mechanism.

BYOD required solution	**How this is addressed**	**Gap in existing studies**

Unauthorized access-Data Leakage	Authentication of BYOD user on trust model basis **[52]** and also 3 tier architecture developed	Post authentication malicious category traffic is not identifiable if validation is expired and on top of this forensic technique is required post incident.
Authorized access-Data leakage	Record storing blockchain process **[24]**. Record keeping ledger developed to detect the BYOD user details	This required detection and Protection mechanism integrated to protect the BYOD enabled environment.
Evidence for BYOD data leakage	Evidence collection using Blockchain based method **[54]** where user interaction is more which is not seemeless enablement of BYOD services	Next Gen catetgory of Digital forensic model required for complete forensic investigation in BYOD environment.
Detection of malicious traffic through deception Technology	BYOD Honeypot technology **[33]** was explored in 2016 (2002C,.1989d), and in 2019 again further developed "Threat intel platform introduced" for detection and FEMA framework in 2019.	In today's increased threat landscape zero-day attack prevention is required as industry need this to enable byod services while protecting organization's internal network

2.8 Conclusion

To enable the BYOD environment in the corporate infrastructure most of the organizations are adopting certificate-based authentication methods, but like all the technologies certificate-based authentication methods also have some limitations and challenges, such as unauthorized user access creating a loophole. However, a cyber forensic digital investigation ecosystem to provide digital evidence and support cyber forensic

investigation after a cyber attack was developed to resolve challenges. As a result of this research, a detection technique for BYOD infrastructure is developed . The enablement and adoption of BYOD technology in the corporates cyber defense and cyber forensic BYOD ecosystem is developed as per the result of this research. A functional and efficient approach is proposed to detect malicious activities in the BYOD environment to secure critical corporate infrastructure. To collect the results and evidence of the research multilevel simulation and testing were conducted.

In the corporate infrastructure still, adoption of BYOD infrastructure is not considered to be secure and safe due to structural loopholes and threats. Two important objectives this research has explored are the Identification and Protection of BYOD infrastructure from modern-day cybersecurity threats and challenges that can't be achieved by traditional technologies and method. However the cybersecurity technologies have developed and proved to be effective to develop a key strategy to integrate defense technologies as a framework to provide identification and protection from BYOD threats and risks at the stage of enumeration before a cyber attack. The other part of the research is to develop a Cyber forensic investigation model which is reliable and efficient to provide digital evidence and artifacts against cybercrime and identify the source of the attacks to conduct the investigation further.

As a conclusion of the research two deliberate prospectives are delivered. To secure corporates from inherent BYOD environment risk and threats an efficient identification and protection mechanism is developed as traditional cybersecurity technologies and tools such as IPS, IDS, AntiBot, or Antivirus are not delivering due to lack of defense mechanism as proposed in this research. The second aspect of the research developed the Next Generation Digital Forensic (NG-DFR) Readiness Model that contributes to the Cyber Forensic ecosystem, enabling Cyber Secure BYOD environment adoption in the corporate infrastructure with cyber confidence.

Chapter 3: Secured Authentication Model

BYOD is rapidly growing phenomena which provide internet access to devices like mobile, tablets, etc. of corporate users and visitors and allow them to work from the devices of their choice and convenient. Also the demand is seamless internet access within the organization boundary irrespective of the location/branch the employee is working. This approach has become a primary requirement but this became challenging for the organization's IT department. Enabling internet access to employees' personal devices can lead to a potential security risk, data leakage and loss of control if a proper security mechanism is not considered while designing a BYOD environment[11]. For instance, using mobile devices for personal and professional work simultaneously can lead to critical security risks as mobile devices are not managed by the organization and third-party tools are also installed on these devices [73]. It is important to understand the criticality of BYOD design to mitigate the risk included with the service. ignorance of proper BYOD design can lead into such security risk.

Then how the BYOD environment should be designed? In an organization, there can be 2 different sets of BYOD users- organization employees who are part of active directory and guest users who are not active directory users. Need is both category of users should be segregated and create secure solution of BYOD.

Data privacy and data protection mechanism are also crucial which must be mitigated while designing and implementing a BYOD solution. Organizations need to leverage the advantages of technology for eliminating and reducing potential risks [74].

Employee satisfaction of an organization is assured with the quality of work culture, flexibility and facility given to the employee. As the internet has become one of the fundamental components for the employees nowadays, every employee of an organization has minimum of 2 to 3 devices with them, official and personal. Carrying multiple devices is hard to manage and also includes the cost. But every employee expects to have internet services enabled on their personal devices for flexibility and ease of work. Considering the internet access dependency in day-to-day life, BYOD market is expected to reach $367 billion by 2022, up from just $30 billion in 2014 (Source: BetaNews). With an official

laptop, employees get internet services and security policies in place at the perimeter firewall and all the web gateways. Providing internet access to personal devices using the same wireless access point and the controller, traffic segregation normally done with SSID, layer 3 authentications, etc.

Primary focus of this study is to develop secure design architecture and complete analysis based on the security parameters and create two different security standard using the same wireless infrastructure. Finally, after performing test and analysis, this study proposed a framework for secure model of BYOD architecture for corporate..

3.1 The Motivation of the Design

In order to address changing working preferences in today's digital transformation age, enterprises are benefiting by providing lesser devices to their employees, and being prepared for emerging technology such as BYOD, IoT, etc. Slowly BYOD will become a necessity rather than a choice. However, connecting untrusted external devices in a corporate network increases the cybersecurity risk and data leakage incidents. Using BYOD services users can perform illegitimate malicious activities, try to gain unauthorized access to the internal network for cyber attack which can lead to a major security breach and that can crumple the organization's integrity, business operation and reputation. Because of unsecured design architecture of BYOD, addressing and defending significant security risks, data theft, and shadow IT became more challanging. Installing malware using BYOD services and establishing an insecure connection over the internet can also lead to serious damage and major security risk.

3.2 Proposed Architecture Implementation

The proposed design and working mechanism of three different segments of architecture using a single wireless infrastructure that is the same wireless access point and wireless controller along with AAA server and user database are shown in 3 different figures.

In the first scenario, the BYOD user is an employee of the organization and the user ID is retrieved from an active directory domain controller. The user authentication method is based on the availability of the user ID and other parameters in the active directory employee database.

Block diagram shows architecture for BYOD-trusted-employee devices having userbase in organization with active directory from which user authentication information is retrieved.

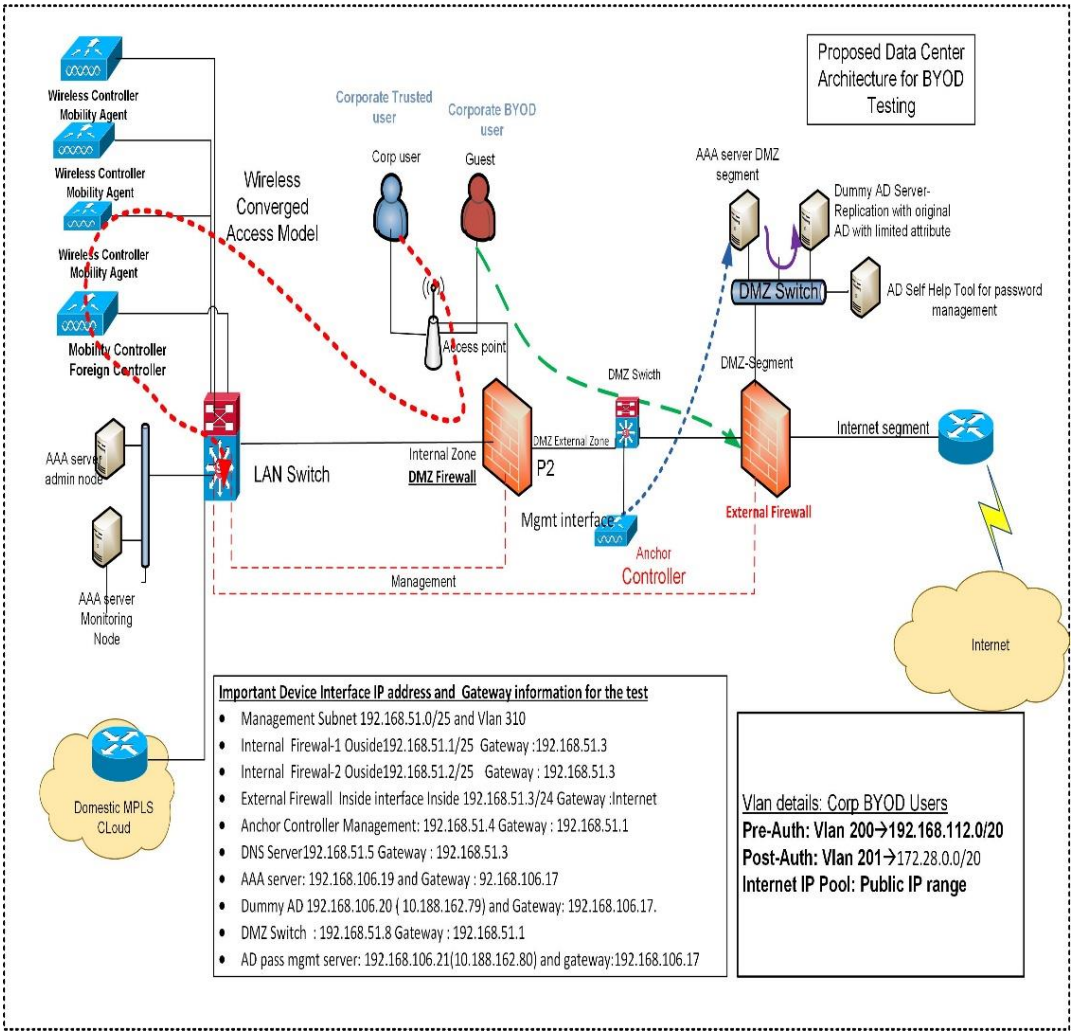

Fig 2. Proposed BYOD model architecture block diagram explaining the working mechanism for the user who is active users in the active directory.

3.3 Testing components used for the Implementation

For the testing below mentioned components of products with their model are used.

Table 4: Products, components and devices used during the test.

Seq#	Technology/Service	Product used for test
1	AAA server	Cisco Identity Service Engine
2.	Internal Firewall	Cisco Firewall
3.	External Firewall	Checkpoint Firewall
4.	Anchor Controller	Cisco WLC 5508

4.	Foreign controller/Mobility controller	Cisco WLC
5.	Mobility Agent	Cisco 3850
6.	Active directory	Microsoft AD
7.	Router	Cisco Router
8.	BYOD devices	Android/iPhone
9	Corporate Device	Laptop

3.4 Secured Authentication model

There is an inclination in the workplace for BYOD which results in the diversity of business difficulties that can be solved in numerous ways. This diversity includes accessing guest wireless networks to provide BYOD device authentication, secured identification and onboarding. The main goal is to deliver a common secured work environment, irrespective of the category of the device being used by the employees or external guests. For delivering the same, secured authentication model is explored more. Secured authentication model has different parts which include security policy framework, authentication access policy restriction and allowed critical access area, layers of network security defense system and enforcing policies. Keeping all these in place this research simulated various aspects of the authentication model.

3.5 Simulation

3.4.1 Traffic flow during the Simulation

The architecture of authentication flow as mentioned below

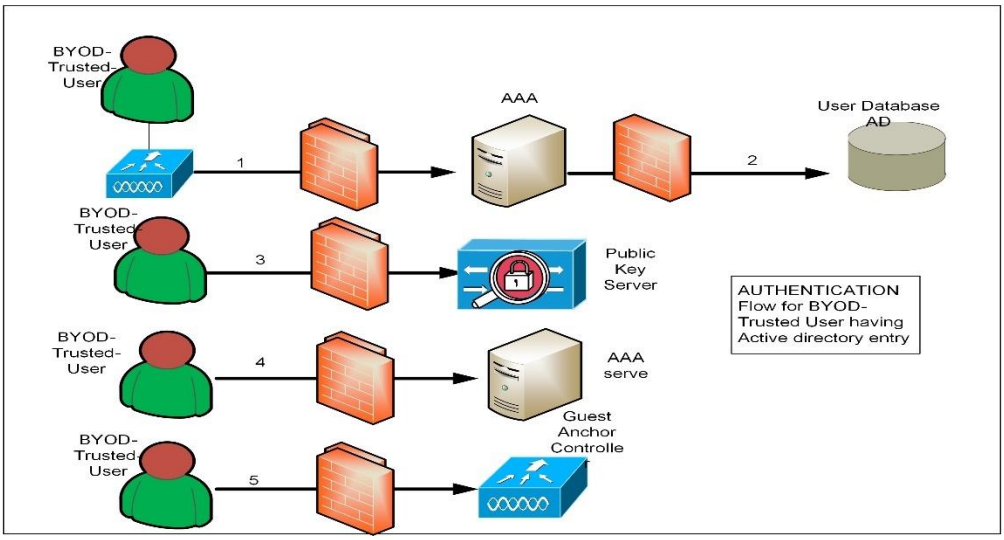

Fig 3. Step by step Traffic flow demonstration

As shown in Fig 3. when BYOD user requests for authentication with a proxy of wireless LAN controller, the request is forwarded to AAA server (1) and then AAA server request to the user database (2) to authenticate the valid and active user, AD responds to AAA with a response as “Valid”, it redirects for certificate. Here 802.1x authentication mechanism is used to secure network[75] . In this phase, the BYOD device gets the certificate (5). Then AAA server response back to the anchor controller to change the VLAN, which is known as Post auth VLAN (Internet access IP).The post-auth network segment will have secured access to the internet. Security policy on external firewall is given below

Table 5: Perimeter Firewall policy for internet access

Seq	Source	Destination	Port	Natting
1	Post-Auth Vlan	Any	Any	Yes

In this next stage, BYOD-trusted employee will get secure internet access without any IP routing of network communication in the corporate internal network. The major security concern of connecting personal devices [76] in the corporate network is addressed in separate BYOD segments. Further, user validation issue is addressed with certificate-based secured authentication. In this case, security posture[77] is maintained and associated security risk with the traditional BYOD model is addressed and mitigated as vulnerable devices can be major security threats. In this test, BYOD traffic is completely segregated from the corporate network.

3.4.2 Traffic flow for BYOD Architecture

Traffic flow of the BYOD-Trusted-User having user entry in Active Directory is mentioned below.

Table 6: Traffic flow with port numbers.

Seq#	Source	Destination	TCT/UDP Port
1	Foreign Controller	AAA server	1812
2.	BYOD user	DNS	53
3.	BYOD user	AAA server	8443
4.	BYOD	AAA server	8905

3.4.3 Simulation parameters

Simulation was conducted in a real lab by using OEM products. There are different OEM products used in this simulation as mentioned in table 4 above . As the objective of this simulation is towards BYOD authentication, so relevant parameters are considered[78] as per the standard design guide related to authentication. The simulation parameters are mentioned in table below.

Table 7: Simulation parameters

Sl No	**Parameter**	**Protocol/ components**
1	Authentication between controller to AAA server (Identity Service Engine)	Radius
2.	Authentication between BYOD user to AAA server (ISE)	https
3.	Address resolution	DNS
4.	Between controller and ISE	EAP-TLS
5	Between AP and controller	CAPWAP tunnel
6	Authentication framework	802.1x
7.	Root Certificate	PKI certificate
8.	User database	Active directory

3.5 Comparison

A comparison of this simulation is done on the basis of the existing study outcome. Existing problems are addressed in the past in various ways. For instance, unauthorized access of the data which is related to the authentication problem is addressed by the user trust authentication model. In this approach integration of certificate-based model and user ID and password-based is introduced and in later stage integration with detection and protection module was also simulated. While data leakage issue is addressed by a record-keeping system which was a blockchain-based model but in this study, we have introduced detection and protection concept with integration of log management system.

3.6 Monitoring and Audit Compliance

Monitoring activities using public IP to avoid any malicious activities and cybercrime,[79] it is mandate for service providers to manage and keep the logs as per the log retention policy for any dispute and situation where an investigation is required. Service provider will directly identify the IP assigned to the organization. In this case, user identification will be the responsibility of the enterprise while ISP will only identify the enterprise where public IP was released. User acceptance policy also needs to be agreed upon and signed by the BYOD user as per organization security policy framework measurement and regulation.[80] Monitoring of the BYOD user activity is a major concern, so a proper log management model to capture logs and identification of the users, storing such a large amount of logs, records should be easily available to the concerned organization body.

In this study, Cisco Identity Service[81] solution is used in connection with Microsoft Active Directory as an additional user database, while the Aruba CPPM Clearpass Policy manager[82] solution is also one of the solutions to manage logs is used in this research. ARUBA CPPM solution is used for the IoT, mobile devices and access management, which works in a role-based access model. Maintaining the enterprise security policy and audit requirement is the responsibility of the organization. In this study, we have addressed security compliance requirements while enabling the BYOD services for the organizations.

3.7 Result and Analysis

Test result and analysis of the BYOD-Trusted-Users with EAP-TLS secured certificate-based authentication method is mentioned in this section.

In the result and analysis phase, logs are collected from the AAA server. In the test, a BYOD device with MAC address: 94:65:2D:E8:A4:88 was used. Steps included during authentication is as mentioned below

Table 8: The sequential events during the authentication process.

Event #	Event Details
11001	Received RADIUS Access-Request

11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with the challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12502	Extracted EAP-Response containing EAP-TLS challenge accepting EAP-TLS as negotiated
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12809	Prepared TLS CertificateRequest message
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session

12504	Extracted EAP-Response containing EAP-TLS challenge
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session

12504	Extracted EAP-Response containing EAP-TLS challenge
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge
12568	Lookup user certificate status in OCSP cache – certificate Services Endpoint Sub CA – AAA1
12570	Lookup user certificate status in OCSP cache success Certificate Services Endpoint Sub CA – AAA1
12554	OCSP status of user certificate is good - certificate for Endpoint Sub CA - AAA1
12568	Lookup user certificate status in OCSP cache - certificate Services Node CA - AAA01
12570	Lookup user certificate status in OCSP cache success Certificate Services Node CA - AAA01
12554	OCSP status of user certificate is good - certificate for Node CA -AAA01
12835	An expired certificate was accepted from the client
12811	Extracted TLS Certificate message containing client c
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12802	Prepared TLS Finished message

12816	TLS handshake succeeded
12509	EAP-TLS full handshake finished successfully
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge
61025	Open secure connection with TLS peer
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
22072	Selected identity source sequence - BYOD_Sequence
22070	Identity name is taken from certificate attribute
22037	Authentication Passed
12506	EAP-TLS authentication succeeded
24423	ISE has not been able to confirm previous successful
15036	Evaluating Authorization Policy
15048	Queried PIP - Cisco.cisco-av-pair
15048	Queried PIP - Network Access.NetworkDeviceName
15048	Queried PIP - Radius.NAS-Port-Type
15048	Queried PIP - EndPoints.LogicalProfile

15048	Queried PIP - EndPoints.BYODRegistration
15048	Queried PIP - Network Access.EapAuthentication
15048	Queried PIP - Network Access.UseCase
15048	Queried PIP - CERTIFICATE.Subject Alternative Nam
15048	Queried PIP - Radius.Calling-Station-ID
15016	Selected Authorization Profile – Change Vlan
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

In this state, the BYOD trusted user is accepted after completion of the authentication and the device COA(Change of Authorization) got triggered. Post COA the device will get a Post-auth IP address from an isolated network, which will directly go to the internet through an external firewall.

Security risk is included even after segmentation of BYOD network and internal network if the same internet exit path of the enterprise is used. If the enterprise has an APNIC IP address registered then any malicious activity done by the BYOD user will be the responsibility of the enterprise as their IP address and infrastructure was used. This study highlight and strongly suggest using a different internet exit path apart from corporate internet path.

Another risk that can occur is with cloud services, if corporate IP is used for BYOD users. The ideal case of any enterprise cloud services is creating NSG in the cloud for accepting traffic from the enterprise public IP segment. If we are using the same IP segment for BYOD users then they will get access to the enterprise trusted infrastructure hosted in the cloud. So

this study explains the risk to the cloud services and suggests using different public IP/separate isolated public networks to build a secure infrastructure.

3.7.1 Attack model for BYOD authentication

The attack model is considered in this simulation with a test BYOD user. The test user connected a smartphone device in the BYOD infrastructure . The access is granted to BYOD through Active directory user authentication and certificate based authentication.

The attack is focused on getting access to organization BYOD network even after the user id is deactivated from Active directory which means user is no more trusted user of the organization. When this untrusted user gets access to corporate network through BYOD, various resources are accessed which means an attack to BYOD network. This lead to damage of critical infrastructure, confidential data theft, information leakage and other malicious activities.

In order to evaluate the attack scenario, initially access was provided in BYOD infrastructure and deactivated the user id from Active directory. In this phase internet access revocation from BYOD devices is the requirement of secured BYOD environment. But post simulation it is been observed that user got the access as shown in section 4.4 using the same device. The detailed investigation logs captured in table 11 for the evidence to simulate the attack. Also malicious traffic is detected from this user in corporate infrastructure perimeter firewall as shown in figure 9. Internal BYOD users of the organization are normally considered as trusted users and no risk to organization. Authentication is processed using Active directory user validation. Even one layer ahead of security, certificate based authentication also performed. But this shows that internal trusted users are even more vulnerable and threat to the organization. Attack performed by internal user to critical infrastructure. Based on this, criteria , attack model is defined in the simulation.

3.8 Discussion

This research and design framework has a major advantage for the BYOD-trusted-employees (internal employees) as they can travel across any other branch office of the organization and have seamless secured access to BYOD internet services as certificate-

based authentication is used for seamless onboarding process. This will provide a hassle-free seamless internet access experience enhancing the productivity of the employee. SSID has to be the same and the same AAA is used. A central method of authentication is available even this can be in a distributed architecture.

3.9 Contribution

A major requirement of secured BYOD design architecture in a corporate environment to enable services through personal device is secured onboarding of BYOD. One important area in secure onboarding process is authentication method of BYOD. This section addresses corporate secured BYOD authentication model which is a serious challenge in terms of security.

This study also focused towards standard design process of BYOD environment. The requirement of traffic routing from BYOD user device to the AAA server up to the internet exit gateway also creates risk to the environment. BYOD architecture should be designed to avoid the risk and ensure the security of the organization.

This study demonstrated a very secured model of routing BYOD traffic. Before even getting the pre-authentication IP address, traffic is encrypted with an EOIP tunnel and landed directly outside corporate LAN bypassing the internal corporate network. In this scenario, it is analyzed that BYOD (Both types of SSID) VLAN does not even require to be created in the corporate core LAN infrastructure. Routing of BYOD IP segments inside LAN is also not required with this model. With this secure model, internet access is provided to BYOD users without compromising the security of corporate LAN infrastructure. Below figure shows the final approach of secure onboarding technique of the BYOD to protect critical infrastructure while providing internet access.

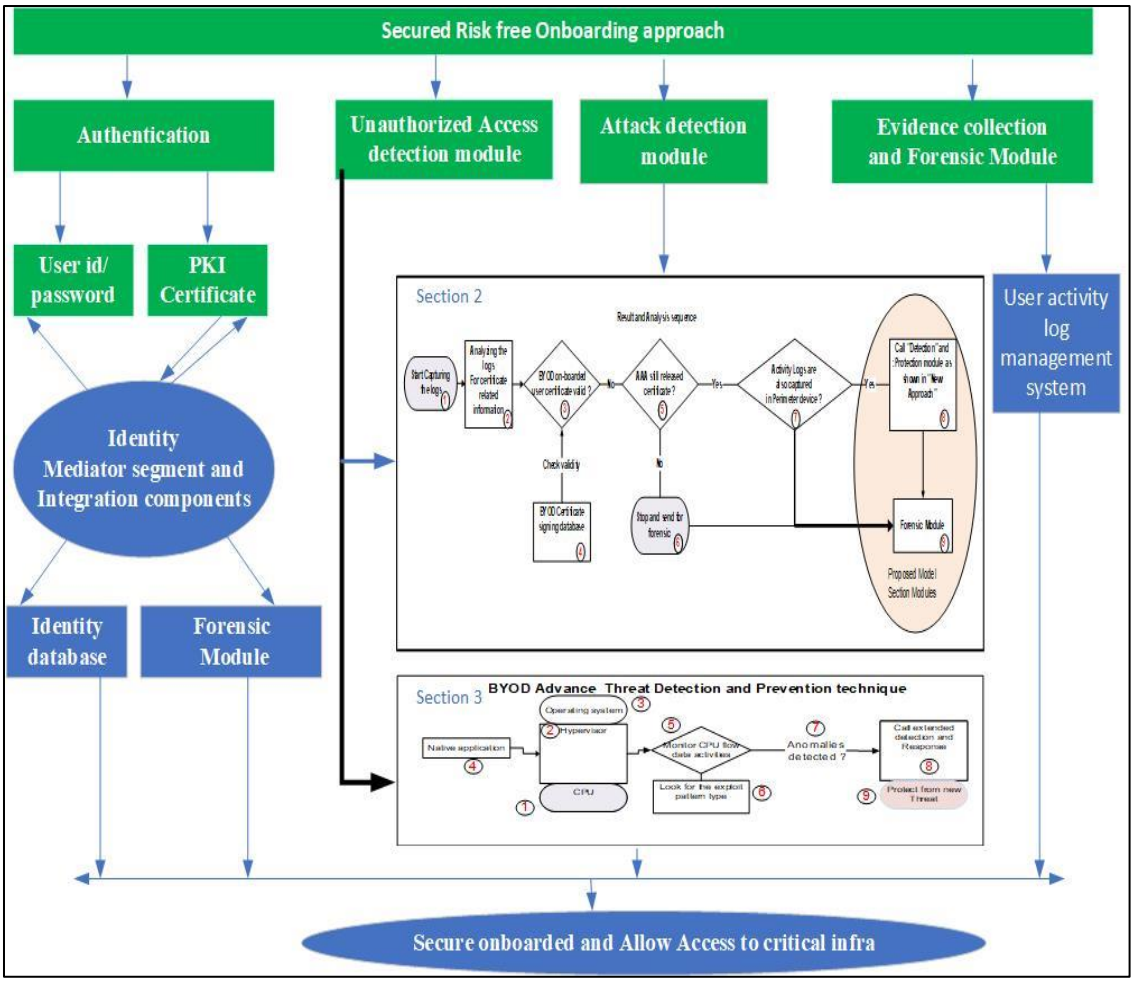

Fig. 4. BYOD Secure onboarding and detection module

This research also contributes a secured framework of the BYOD implementation in a centralized and distributed model. Finally, a novel approach of secure BYOD service is developed while following all organizations' security policy and practices.

3.10 Summary

Organizations must address the security risk while giving internet access to employees on their personal devices from corporate wireless infrastructure. As, it is not possible to segregate wireless access point and wireless LAN controller for corporate intranet wireless and BYOD wireless in the same physical area due to crosstalk between radio signal transmission so co-channel interference (CCI) and adjacent channel interference lead to

major interruption of services in RF media. During the test, the same wireless access point and controller are used for BYOD services as used for the internal network. For giving the internet access using the same wireless controller and access point, the BYOD infrastructure must be designed and implemented in such a way so that end-to-end traffic segregation is maintained and security remains intact. We have broadcasted multiple Service Set Identifiers (SSID) to enable BYOD services and internal network connection.

In this study, it is demonstrated that BYOD service to be divided into two different profiles. Firstly for BYOD corporate user profile which is a trusted user profile, where certificate-based authentication can be recommended as a secured model. Secondly, for guest access which is untrusted profile, a layer of three open authentication is recommended and considered in the proposed security model.

In either of the case, it is recommended to have the gateway of the BYOD devices separate from the corporate LAN infrastructure, which is considered to be the most secure way of managing BYOD infrastructure as per the study. Even if the personal devices are connected to the same wireless access point, the gateway of the BYOD devices should be outside the DMZ Firewall as mentioned in Fig. 2 which segregates LAN and external network profile to maintain a secured way of internet access minimizing the security risk.

In organizations where the number of users are high, BYOD access enablement and revoking of internet access as an exit management process could be very extensive and resource-consuming which can be automated with the proposed BYOD model that protects the organization from security risk and provides system driven automated process rather than manual intervention.

This study also analyses one important area of designing the BYOD infrastructure with cloud security architecture and helps to mitigate security risk towards rapidly growing cloud services in the corporates.

Chapter 4: Detection and Protection of Malicious traffic

4.1 The Motivation of BYOD Cyberthreat Detection and Protection background

Honeypot technology is one of the important areas on which studies have been done in the past, in which detection of malicious activities **[33]** and combination of deception to combat cyber risk management process of FEMA (Federal emergency management agency) mission with five preparedness **[55]** was explored. A subsequent study, "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology" was also conducted, succeeding previous studies in this field **[33]**. Enhancement of the research was also conducted following the study of Smart Threat Stage to detect the incident and amplified accuracy level **[34]**. Using the audit trail mechanism, the accuracy level of finding the source of the attack was increased in the research, and the accuracy level was improved to be 93.71% then 90.73% to 96.16% **[34]**. A novel approach is also developed to evaluate malware infection risk using the machine learning approach**[65]**.

4.2 Design implementation

Real time traffic detection of BYOD user is a complex task. Detection and correlation of logs for evidence is the major requirement. In order to produce different types of traffic for detecting malicious traffic in BYOD environment, network architecture was designed. While designing the network, maximum security measures were taken to secure the network to avoid open loophole for malicious traffic. The lab was designed with all required components like BYOD devices, wireless controllers, access points, external and internal firewall. As traffic was routed through MPLS network, encryption key server was used. The network was designed in such a way so that traffic can be detected in all the levels to identify malicious traffic and correlation of logs can be done to trace the source of attack for further forensic analysis.

4.2.1 Simulation

This research experiment was performed in a lab environment. The designed architecture was applied and traffic was routed from different locations. Untrusted traffic of BYOD users

was routed through spoke and branch locations. An encryption technique was used during the routing of untrusted traffic in the MPLS network.

Architecture and design were built as mentioned below in below figure.

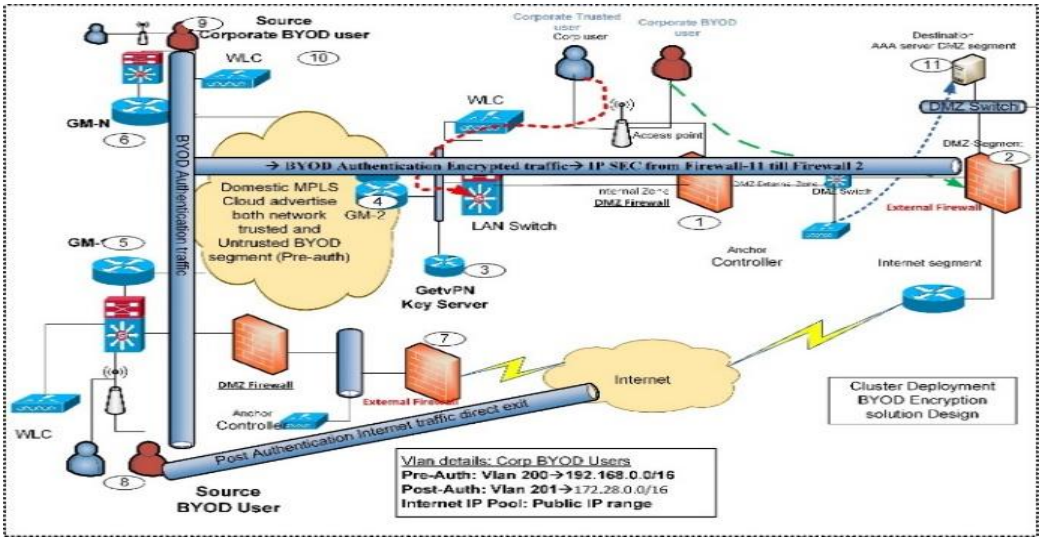

Fig. 5. Research simulation Lab architecture

4.2.2 Components used for the simulation

Components used in the architecture mentioned in Table below.

Table 9: Components used during the research as per Fig. 5.

Index	Components	Used for
3	Key Server (Getvpn)	Encryption management
4,5,6	Group Member	Encryption for secure traffic routing
1	Firewall	Inside Firewall for traffic segregation between of DMZ (cisco)
2,7	Firewall,7	Internet-facing Firewall for malicious traffic detection
8,9	BYOD user	BYOD users
10.	BYOD Guest controller	Anchoring controller
11	Authentication server	AAA server and CA signing authority

To reduce attacks from authentication, the first layer of defense is used by applying traffic encryption **[83]** and mitigate cyber threat risk **[84]**. Untrusted traffic is routed through a secured MPLS network where trusted traffic is transmitted using GETVPN encryption to

protect internal critical infrastructure **[61]** and BYOD untrusted traffic bypassed from encryption to reduce cyber threat **[85]**.

This study was conducted in 2 phases, the first phase was to detect the malicious traffic, the second phase was to develop protection mechanism and to capture traffic from different locations along with central locations as well.

4.2.3 Dataset to validate simulation

In order to validate the simulation, all the parameters are captured so that reverse validation can be done. Simulation was done in real lab environment as per design. Traffic routed from different locations over MPLS and key technique of the traffic encryption was GetVPN **[61]** to reduce security risk as first layer of defense. Traffic generation source of BYOD user and detection of the traffic to validate the test mentioned in the table below.

Table 10: Dataset for the simulation

Sl No	**Reference**	**Traffic Origination**	**Traffic Detection**
1	Fig.5	BYOD user detail, mac address, timestamp mentioned below Testuser 04:c8:07:2d:ce:24 4779a22d524b4d2f94ca6769d351c977 8/4/2020 11/3/2020 CN=Certificate Services Endpoint Sub CA - Reserach CA C=US, ST=State, L=City, O=Company name, OU=Example unit, CN=Testuser Expired EAP_Authentication_Certificate_Template	data source as per design architecture table 7, component#11 AAA server - ISE
2	Fig.5	Authentication parameters Authentication Details Source Timestamp 2020-11-13 19:51:55.659 Received Timestamp 2020-11-13 19:51:26.494 Policy Server Research CA Event 5200 Authentication succeeded Username Testuser	data source as per design architecture table 7, component#11 AAA server - ISE

		Endpoint Id 04:C8:07:2D:CE:24 Calling Station Id 04-c8-07-2d-ce-24 Endpoint Profile Unknown Audit Session Id 829ABC0A00001DEEC1DD53C7 Authentication Method dot1x Authentication Protocol EAP-TLS Service Type Framed Network DeviceWLC01 Device Type All Device Types Location All Locations NAS IPv4 Address 10.1.1.130 NAS Port Id capwap_9000000c NAS Port Type Wireless – IEEE 802.11 Authorization Profile Change Vlan Response Time 27 milliseconds	
3	Attribute	Other Attributes ConfigVersionId 353 DestinationPort 1812 Protocol Radius NAS-Port 1617 Framed-MTU 1485	data source as per design architecture table 7, component#11 AAA server - ISE
4	Provision	Post provisioning details Time 51:32.3 Status Session Identity Testuser Endpoint ID 04:C8:07:2D:CE:24 Authorization Profiles ChangeVlan Authorization Policy Default >> Employee_EAP-TLS_temp_troubleshooting IP Address 172.28.40.244	data source as per design architecture table 7, component#11 AAA server - ISE

4.3 Organization structure of the result of the experiment

Primarily results have been captured to control the unauthorized access as per security policy. We have captured the results from the AAA server initially from where the certificate was issued to the user with the valid issue date and the expiry date.

The Result and Analysis section contains lots of logs and artifacts collected from the testing during the research. A block diagram with the flow represented in below figure for the understanding of the result.

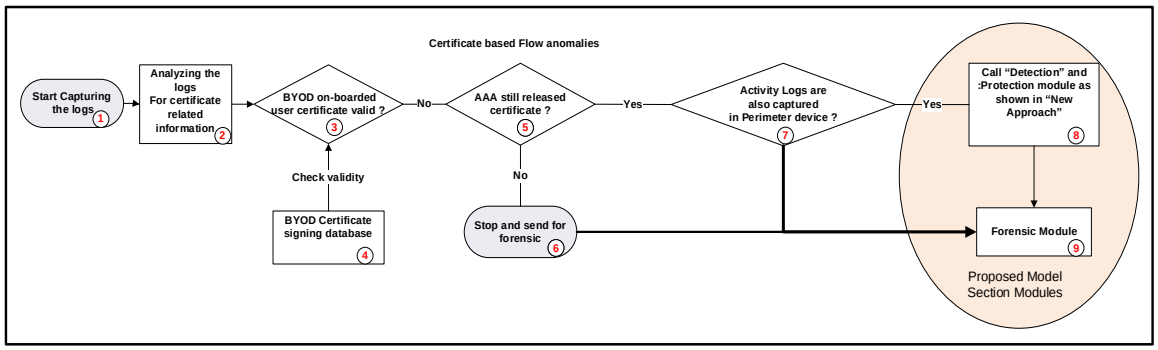

Fig. 6. Organization of the Result and Analysis in this section.

The organization of the result is as per pseudocode1 mentioned below.

Pseudocode 1: Organization of Result and Analysis Section

Begin

Certificate checked and picked up a BYOD user whose certificate is expired

//Then Tried the same BYOD user to get access to critical infrastructure by onboarding in BYOD infrastructure

If BYOD user authentication successful

then

check logs in certificate server

Checked the logs from the controller

Checked the logs from the Perimeter firewall

If results are accepted logs showing

Then

A new approach of detection and Protection model called in next section

```
            End If
 End If
Stop
```

4.4 Result and analysis

To identify the loophole in the secured access model below steps have been followed.

Step 1: At first Secure certificate by PKI authority was issued with a defined start and end date.

Step 2: Once the certificate is expired without re-issue of the certificate, logs were verified related to the certificate.

Step 3: Post the expiry of the certificate, the BYOD user tried to access the resources and logs captured.

Step 4: After authentication, logs were collected from the perimeter firewall and traffic access logs were also captured.

Detail investigation logs are captured and collected as mentioned in the subsequent section below

Step 1: BYOD user was provided with access to the network as the certificate was issued which was valid from 4th Aug'20 to 3rd Nov'20 for 90 days service validity defined by the security policy of the organization as mentioned in figure below.

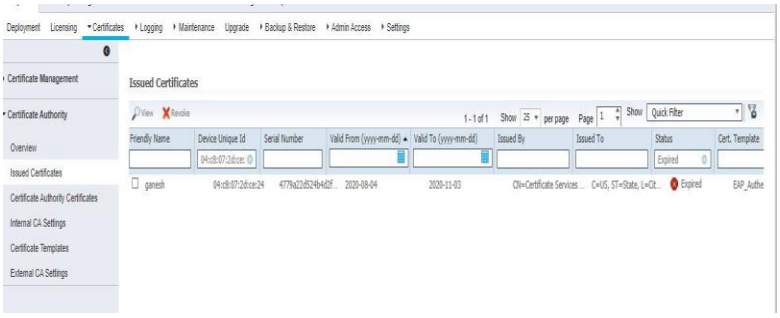

Fig. 7. Certificate issue and expiry date

(data source as per design architecture table 7, component#11 AAA server -ISE)

In Step 2: We have checked logs on the AAA server for the same user and confirmed that the certificate got expired as mentioned in Fig.8 below

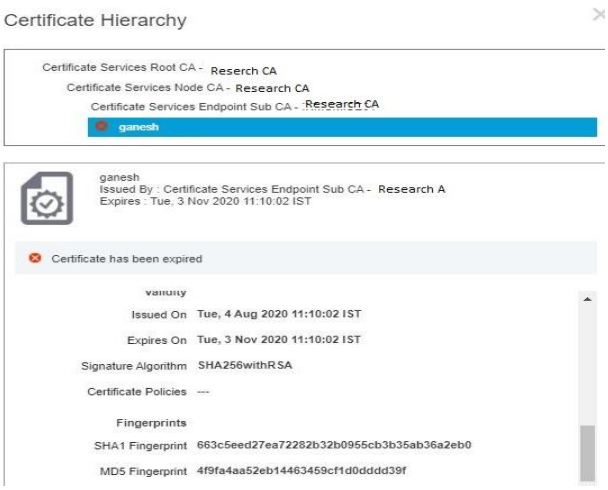

Fig. 8. BYOD Certificate expiry information

(data source as per design architecture table 7, component#11 AAA server -ISE)

The certificate was expired on 3rd Nov'20 along with fingerprints as mentioned in Fig. 8. Consequent information was also available in the logs as shown in Table 11 below.

Table 11: Certificate validity logs captured

(data source as per design architecture table 7, component#11 AAA server -ISE)

Testuser 04:c8:07:2d:ce:24 4779a22d524b4d2f94ca6769d351c977 8/4/2020 11/3/2020 CN=Certificate Services Endpoint Sub CA - Reserach CA C=US, ST=State, L=City, O=Company name, OU=Example unit, CN=Testuser Expired EAP_Authentication_Certificate_Template

Step 3: In this step, we analyzed the logs for the BYOD user's authentication.

The detailed investigation of the logs gives us evidence that the user was able to authenticate successfully on 13th November'20 while the user certificate validity expired on 3rd Nov '20. Below logs shows the step-by-step authentication details, event 5200 defines that authentication was completed for the MAC address of the endpoint 04-C8-07-2D-CE-24 and the duration was 27 ms as mentioned in Table 12.

Table 12: Authentication Log Details

(data source as per design architecture table 9, component#11 AAA server -ISE)

Authentication Details	
Source Timestamp	2020-11-13 19:51:55.659
Received Timestamp	2020-11-13 19:51:26.494
Policy Server	Research CA
Event	5200 Authentication succeeded
Username	Testuser
Endpoint Id	04:C8:07:2D:CE:24
Calling Station Id	04-c8-07-2d-ce-24
Endpoint Profile	Unknown
Audit Session Id	829ABC0A00001DEEC1DD53C7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC01
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.1.1.130
NAS Port Id	capwap_9000000c
NAS Port Type	Wireless – IEEE 802.11
Authorization Profile	Change Vlan
Response Time	27 milliseconds

While checking the attributes, we have found the BYOD user crossed all the parameter checks and passed all attribute changes as a normal user. The certificate attribute was observed as normal as a valid user. The user can be seen to get connected on TESTNET SSID without even certificate validity as mentioned in Table 13.

Table 13: The attributes of BYOD user connection

(data source as per design architecture table 9, component#11 AAA server -ISE)

Other Attributes
ConfigVersionId 353
DestinationPort 1812
Protocol Radius
NAS-Port 1617
Framed-MTU 1485
State
37CPMSessionID=829ABC0A00001DEEC1DD53C7;37SessionID=INMUMISE01/3
78044182/819801;
NetworkDeviceProfileId 11263857-0059-4960-96b5-fcbdd151ff79
IsThirdPartyDeviceFlow false
AcsSessionID Research CA/378044182/819801
SelectedAuthenticationIdentityStores Preloaded_Certificate_Profile
AuthenticationStatus AuthenticationPassed
IdentityPolicyMatchedRule Default
AuthorizationPolicyMatchedRule Employee_EAP-TLS_temp_troubleshooting
Serial Number 47 79 A2 2D 52 4B 4D 2F 94 CA 67 69 D3 51 C9 77
Subject – Common Name Testuser
Subject Alternative Name 04-C8-07-2D-CE-24
Subject – Organization Company name
Subject – Organization Unit Example unit
Subject – Location City
Subject - Country US
Subject - State or Province State
CPMSessionID 829ABC0A00001DEEC1DD53C7
EndPointMACAddress 04-C8-07-2D-CE-24
ISEPolicySetName Default
IdentitySelectionMatchedRule Default
TLSCipher ECDHE-RSA-AES256-GCM-SHA384
TLSVersion TLSv1.2
DTLSSupport Unknown
Subject C=US,S=State,L=City,O=Company name,OU=Example unit,CN=Testuser
Subject Alternative Name - EMail 04-C8-07-2D-CE-24
Issuer CN=Certificate Services Endpoint Sub CA – Research CA
Issuer - Common Name Certificate Services Endpoint Sub CA - Research CA
Key Usage 0
Key Usage 1
Key Usage 2
Extended Key Usage - Name 130
Extended Key Usage - OID 1.3.6.1.5.5.7.3.2
Template Name EAP_Authentication_Certificate_Template
Days to Expiry 0
AKI 80:38:e0:63:a5:d2:54:dc:3b:82:6e:91:a7:10:38:01:da:70:c0:ac
Location Location#All Locations

Device Type Device Type#All Device Types Network Device Profile Cisco BYODRegistration UnKnown RADIUS Username Testuser NAS-Identifier TEST-WLC Device IP Address 10.188.154.130 Called-Station-ID a4-b2-39-7e-e0-a0:TESTNET CiscoAVPair service-type=Framed, audit-session-id=829ABC0A00001DEEC1DD53C7, method=dot1x, client-iif-id=285218009, vlan-id=16, cisco-wlan-ssid=TESTNET service-type=Framed, audit-session-id=829ABC0A00001DEEC1DD53C7, method=dot1x, client-iif-id=285218009, vlan-id=16, cisco-wlan-ssid=TESTNET

Finally, the certificate was also consumed. The base license was assigned to the BYOD user. The base license was consumed as shown in Table 14.

Table 14: License allocation result

(data source as per design architecture table 9, component#11 AAA server -ISE)

Result State ReauthSession:829ABC0A00001DEEC1DD53C7 Class CACS:829ABC0A00001DEEC1DD53C7:Research CA/378044182/819801 Tunnel-Type (tag=1) VLAN Tunnel-Medium-Type (tag=1) 802 Tunnel-Private-Group-ID (tag=1) 201 EAP-Key-Name 0d:24:fa:9d:74:37:35:ec:a9:8c:80:c5:7f:77:1b:57:18:b2:b4:66:8e:9b:ad:5e:53:2a:f5:ea: 24:28:72:f1:f8:27:f4:df:4d:9f:a5:f5:72:1a:ee:58:76:84:af:ee:88:e4:22:51:42:90:88:19:91:bd:fb: 1e:7d:d4:71:de:e0 MS-MPPE-Send-Key **** MS-MPPE-Recv-Key **** LicenseTypes Base license consumed

After successful authentication, the BYOD user endpoint having MAC address 04-C8-07-2D-CE-24 got an IP address of 172.28.40.244 as mentioned in Table 15.

Table 15: IP address allocation of BYOD user

(data source as per design architecture table 9, component#11 AAA server -ISE)

Time	51:32.3
Status	Session
Identity	Testuser
Endpoint ID	04:C8:07:2D:CE:24
Authorization Profiles	ChangeVlan
Authorization Policy	Default >> Employee_EAP-TLS_temp_troubleshooting
IP Address	172.28.40.244
Network Device	

At last, logs were collected from the external firewall where traffic was detected for the same BYOD user. External firewall logs show that even after the certificate was expired, BYOD users were able to access all required resources. The below figure shows that the user's allocated IP address was 172.28.40.244 and the user was able to access the infrastructure as mentioned in Fig. 9 below.

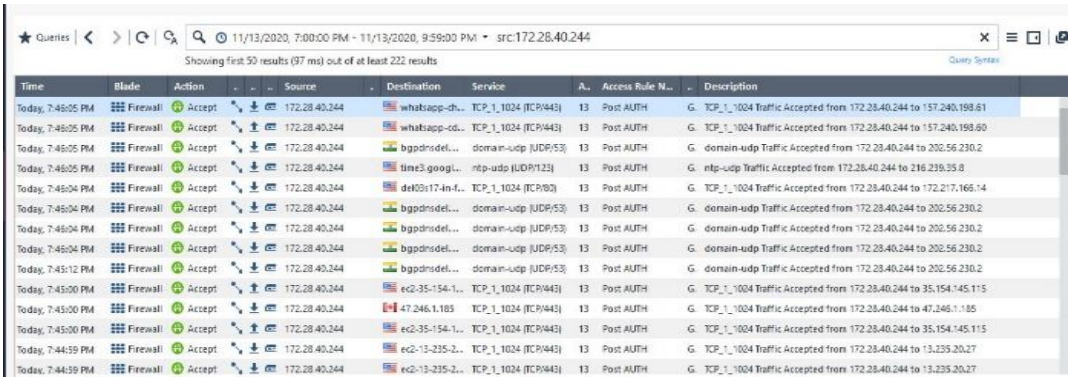

Fig. 9. Un-authorized traffic permitted logs

(data source as per design architecture table 9, component#2,7 External Firewall)

After analysis of the results, it is concluded that even after the certificate gets expired, user was able to successfully authenticate and able to access the critical infrastructure of the organization. As per the test result, it is has been concluded that the secure certificate-based access model has a loophole. Based on this analysis, a detection model was developed to mitigate the loophole and to detect unauthorized access. A secure architectural model and algorithm were developed to detect this.

4.5 Detection Model

Detection of cyberattack in the BYOD environment is the most critical task. A subsequent study revealed BYOD might become "Bring Your Own Danger"**[86]** if control of cybersecurity is not instigated and forensic investigation after an attack is not organised.

4.5.1 Motivation

In this research phase, detection of unauthorized access has been the primary approach. To enable secure internet access for BYOD users a certificate-based model was considered the most secured model in the BYOD environment. But in this study, a loophole was identified in the certificate-based model which leads to major cybersecurity risk. A detailed technique to detect the unauthorized access of BYOD traffic is presented in an algorithm followed by the architectural approach of this model.

4.5.2 Detection algorithm

Post analysis of the simulation of the research, a novel tactic is established in the BYOD environment to build a cyber defense ecosystem. The proposed established model has a dual approach. The initial phase is proposed to detect and identify the suspicious category of BYOD traffic. The second phase is proposed to protect the critical infrastructure from suspicious activity.

The increased amount of cyber-attack is challenging the corporate business ecosystem and cybersecurity has also become a business survival reason. The available security framework and techniques of BYOD operation mechanism are not enough to match the pace of security threat protection at which cyber threats are rising. The malicious category of traffic in the BYOD environment needs an advanced level of detection mechanism for cyber forensic investigation.

4.5.3 Protocol and mechanism to detect loophole of certificate-based mechanism

During the test we have found even after the secured 3 tier mechanism, there is a serious loophole, which act as a source of attack as mentioned below

Certificate issue date=dd1/mm1/yy1 (X)

Certificate expiry date = dd2/mm2/yy2 (Y)

User id deletion/deactivate date=dd3/mm3/yy3 (Z)

in this case, Z is before the Y and after X, then BYOD user having a secure certificate will have access to critical infrastructure during the days between dd3/mm3/yy3 and dd2/mm2/yy2

Unauthorized access duration A(days)=Y(date)-X(date).

so critical infrastructure will be accessible to BYOD untrusted user even after user id deletion or deactivation as shown in below Fig. 10 below.

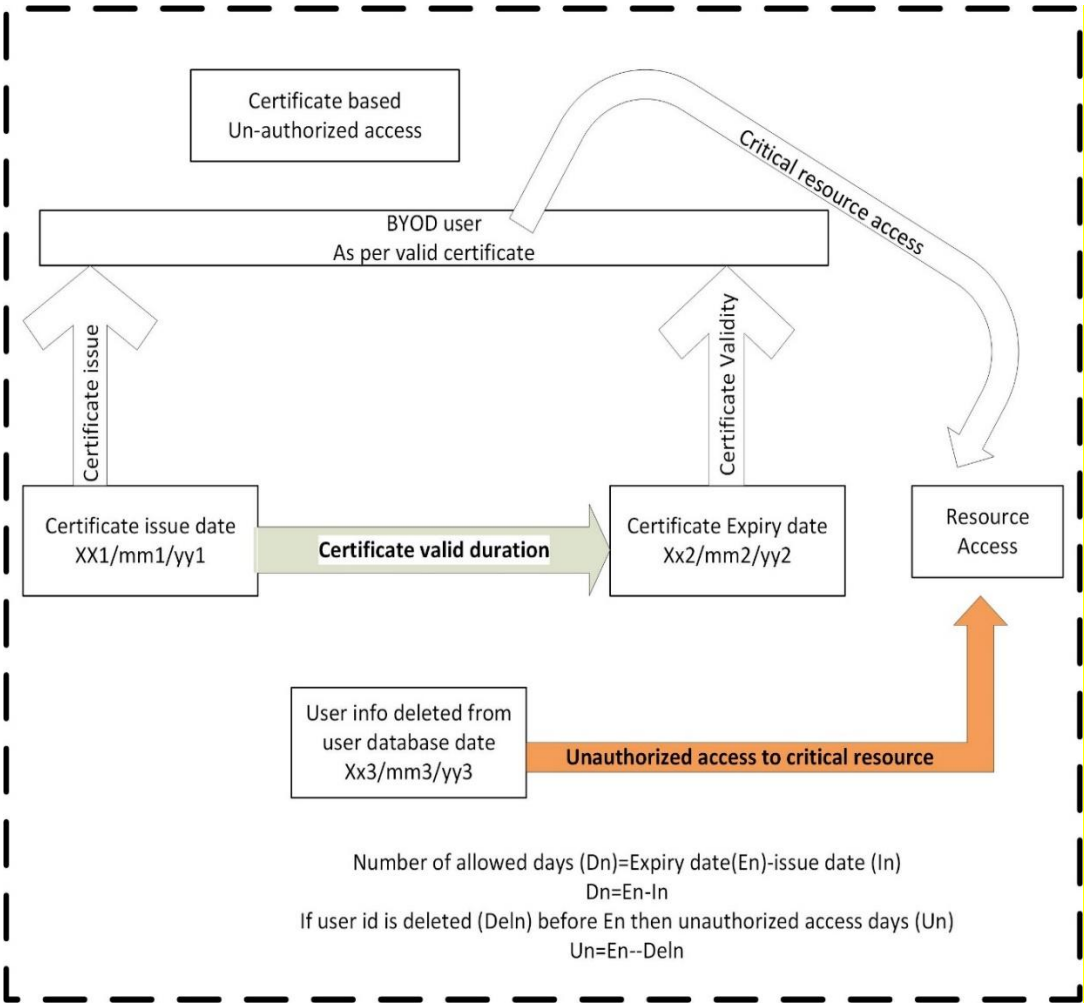

Fig. 10. Unauthorized access architecture block diagram

The important objective of our study is to develop a "PROTECT" mechanism to protect the critical infrastructure which is explained in the following section.

4.5.4 Developed Detection Algorithm

Below mentioned Thesis shows the algorithm of detect-mechanism.

Algorithm 1: Algorithm to detect Malicious BYOD traffic

```
Step 1: Start
Step 2: Input  variables D1, D2 and D3
Step 3: Integrate User database(UD) with
External Firewall Identity Awareness (IM)
Step 4: Read Date from UD on run time basis
Step 5: Assign values
                D1=Secure PKI certificate issue date
                 D2=Secure PKI certificate expiry date
                  D3=Date of BYOD user ID deactivation from User database
       N1 = D2 - D3
step 6: Compare values
      IF
              (D3=Null && D2<D3)
         Then
                Allow access and Sandboxing for forensic
          Else
                 Goto Step 7 for Identity check
      Endif
Step 7:
      IF
              D2>D3

          Then
                Detect and alert as "Malicious"
                  Goto Module "PROTECT"
           else
                        Alert to  AAA
      Endif
Step 8: STOP
```

Algorithm details:

The algorithm which is developed in this research to derive the detection technique is explained in step by step process below.

Variables taken in this algorithm was D1, D2, and D3 as

D1 is the date that the Secure BYOD PKI certificate was issued.

D2 is the date that the issued certificate get expired.

D3 is the date of deactivation of the User from the user database.

In the first case if D3 does not have any date which means the ID is active and normally permits user to access the organization's critical infrastructure and forensic sandboxing of logs triggered.

In the 2nd case, if the value of D2 is greater than D3 that means, the certificate is not expired but the user ID is deactivated from the user database. If the result of the 2nd case is true then this is considered unauthorized user access and access needs to be denied. This is a situation where the BYOD user is not a valid authorized user anymore but the same BYOD user can access the critical infrastructure as shown in Fig. 9. as an artifact.

This has been proved that the secured BYOD certificate-based model is having a loophole that is a critical vulnerability and cybersecurity risk. It gives access to attackers and creates a threat path. From this point, control was transferred to the proposed "PROTECT" Module which is subsequently developed to protect the infrastructure in this study. Before this step, we also captured activity logs and performed forensic analysis.

Also, the exact duration of unauthorized and malicious access has been calculated as below. The number of days of unauthorized access can be calculated as

$$N = D2 - D3 \qquad (1)$$

So, N is the number of days of unauthorized access considered as malicious access and security risk.

Based on the algorithm a flow chart is also designed to present the detection model and technique as mentioned in Fig. 11 below

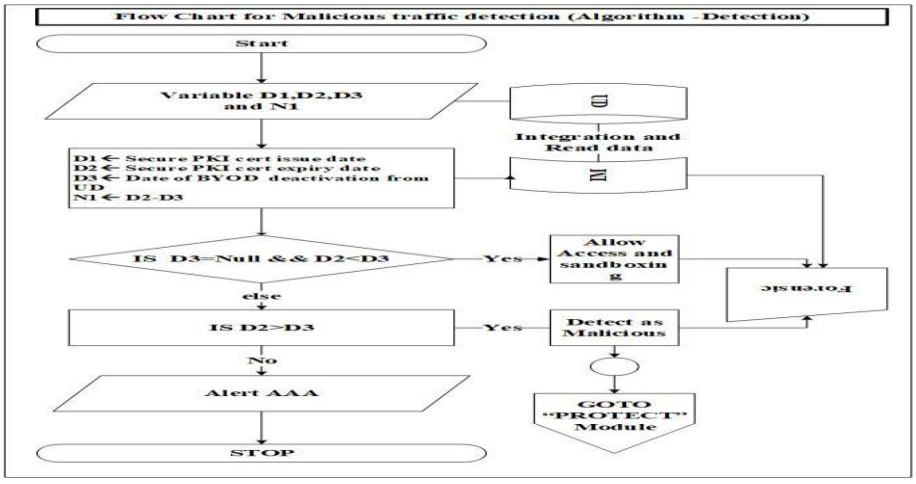

Fig. 11. Detection model of BYOD malicious traffic.

In the flow chart, we can see step by step process of the algorithm presented so that the detection process becomes easy and forensic ecosystem can be developed to secure the organization with BYOD adoption.

The flow chart also transfers the control to the "PROTECT" Module, which does further processing to restrict the undesired access to the organization's critical infrastructure. This mechanism secured the infrastructure of the organization by eliminating loopholes we have found with traditional BYOD technology.

4.6 Protection Algorithm

4.6.1 Motivation

Digital transformation of the business demands to adopt different new services and technology. The growing trend of working from home option has accelerated the adoption of BYOD even more faster to offer more flexibility to employees. Since 2009 BYOD started growing exponentially and different methods and techniques were developed to implement the technology using existing infrastructure.

However, the security aspect of the BYOD infrastructure needs to be considered cautiously while adopting and implementing the same due to increasing cybersecurity risks. It has been found that attackers are finding new ways to attack, and 62% of attacks are caused by insider threats **[87]**. As per "Global Crisis Survey**[9]**" by PWC, 26% of the major cybercrime crisis were caused by internal users. The result section depicts one of the reasons for increasing insider attackers.

In this research, a secured certificate-based model is proposed with the design of BYOD architecture. Additionally, model from detection to the protection of the critical infrastructure from cybersecurity risk is developed in the study.

4.6.2 Protection Algorithm Analysis

4.6.2.1 "PROTECT" Model for Malicious users traffic protection

To mitigate the security risk and restrict malicious traffic, we come out with a solution called "PROTECT". The architecture of the "PROTECT" mechanism depicts how to mitigate this risk as shown in below Fig. 12.

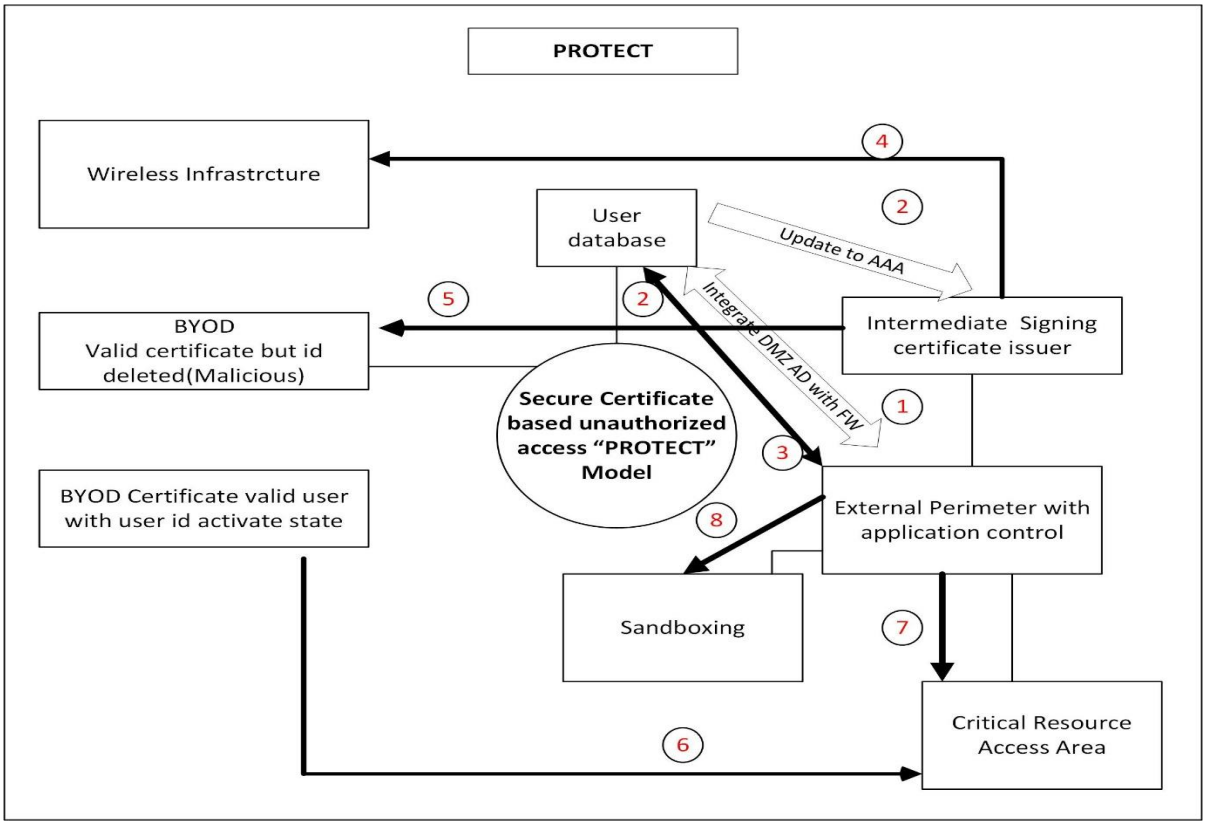

Fig. 12. The architecture of the "PROTECT" mechanism

A secure defense mechanism "PROTECT" based on secure certificate-based authentication, perimeter external access, and forensic sandboxing is developed to detect malicious user access and restrict malicious user traffic.

This proposed "PROTECT" mechanism continuously monitors the ecosystem dynamically to inspect any malicious activity and access, it can detect unauthorized user access and triggers the system for access restriction and isolation of unauthorized devices. PROTECT mechanism also perform a verification process to check if there are any additional devices of the malicious user in the system, if any such device is found then all other related certificates will be dropped. Then it will generate a certificate revocation alarm to AAA and forensic sandboxing.

In this scenario external perimeter firewall (integrated with DMZ AD) will detect the status of identity and DMAAD and AAA will be triggered for certificate revocation.

“PROTECT” architecture successfully protects the critical infrastructure from malicious user access which is having a security certificate but posing risk to the infrastructure. It is an extended study of practical approach of malicious activity in various phases of BYOD which is relied on certificate-based authentication model for achieving cyber defense ecosystem.**[88]**.

4.6.2.2 Analysis of the Algorithm

A novel approach of protection mechanism is developed in this phase of the research to protect the critical infrastructure from cybersecurity risk and threats found with the traditional BYOD model. To mitigate the loophole in the secure access model of the traditional BYOD mechanism, a new approach is required to be implemented in the BYOD infrastructure which is effective and eliminate the risk created by the existing loophole in the system.

This phase of the research shows the development of protection mechanisms and cyber defense ecosystems. An algorithm is developed to defend and drop unauthorized user access and malicious activity with the integration of an external firewall with a AAA server and user database.

An algorithm was developed to mitigate the cyber threats and loopholes detected in the previous models. The algorithm was invoked with a detection module discussed earlier in this study. Apart from this, a forensic module was also used for sandboxing. Once the malicious activity is detected in the system , activity logs were recorded and used for forensic analysis to finally develop a cyber forensic ecosystem.

Based on the finding of the gap in the detection mechanism, step by step algorithm of the protect module is developed and mentioned in Algorithm 2.

Algorithm 2: “PROTECT” algorithm for Drop traffic

```
Step 1: Start
Step 2: Input  variables D1, D2 and D3
Step 3: Integrate User database(UD) with External Firewall Identity Awareness (IM) and AAA
Step 4: Read Data
        D2<-- Secure PKI certificate expiry date from AAA
        D3<--Date of BYOD user ID deactivation from UD
        Ux<--BYOD user from UD
        N<--Number of devices issued
Step 5: Read Data
Step 6: If
          D2>D3 then
                Alert IM to drop and sandboxing for forensic
                   Goto step 7 //for N
                While
                    (N!=0)
                         do
                      revoke certificate from AAA
                N=N-1
                 done
                  else
                    Goto step 8
step 7:
        Input Value= Ux,
                check if  User name=Ux
              then
                count number of devices
                N=Count
               Else
                   N=1
Step 8: STOP
```

A detailed discussion on the algorithm concerning the protection mechanism is mentioned below

Initially, this module was called from the detect module as a control transfer.

Variable D1, D2, and D3 were taken and values were assigned as below:

D2=The date of the expiry date of the certificate

D3=Date of deactivation of the user from the User database

Ux=Test BYOD random user

N=Number of devices issued to BYOD user Ux

2nd part of step 6 of the algorithm was to identify the number of devices where this license was issued or used so that it can be logged for forensic and revocation of the certificate can be triggered.

This identifies the number of devices and revokes the certificate till N=0 and then the process gets stopped.

This process drops the traffic and captures all logs for forensic investigation.

The subsequent Flow of this algorithm is also developed as mentioned in Fig. 13 below.

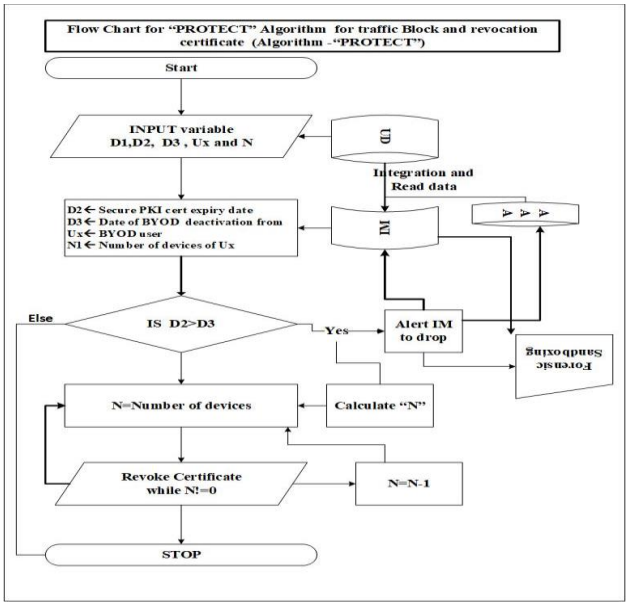

Fig. 13. Flowchart for "PROTECT" algorithm

The step-by-step process for protecting the critical infrastructure is shown in the flowchart.

Certificate-based secured authentication model inline with PROTECT architecture was proposed so that cyber defense ecosystem[88] can be built.

4.7 Comparison

A series of studies conducted in various segments since the inception of Bring Your Own device (BYOD). The exponential growth of the adoption of BYOD technology increased the demand for research. As a result, academic researchers created a good amount of abstracts with new techniques and methods which ultimately offered a systematic study of existing techniques and development of the BYOD cybersecurity ecosystem. The primary goal of this systematic review is to identify the existing research specifically BYOD cyber forensic ecosystem, group the techniques developed in various areas and summarize the findings. Out of 8519 articles in the BYOD segment present in various publication databases, we identified the 18 potential research which contributes to enhance the cybersecurity forensic ecosystem. Limitations of existing research are also identified which organizations need to mitigate to build a cyber secured forensic BYOD environment.
The outcome of the research from existing research is documented below in table 16.

Table 16: Analysis of finding from existing research

Sl No	**Paper Title**	**Findings/problems addressed**
N1	Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users[66]	This research focuses on BYOD adoption and security risk with BYOD and reverses IT adoption logic. Conceptually this paper has studied the security risk of BYOD. Data security concerns is been addressed in this study. The adoption of a tool for BYOD security is been addressed.
N2	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology	This study is conducted on Digital Forensic readiness using honeypot, a deception technology. This study analyzed and showed an approach on how to conduct digital forensic analysis after an incident and detection mechanism. A security model in DFR has been proposed in this study. This study has concluded a DFI (Digital Forensic Investigation model using honeypot in BYOD deployment. DFR model has been proposed.

N3.	Improving Forensic Triage Efficiency through Cyber Threat Intelligence	A study was conducted on the extended approach of DFR (Digital Forensic readiness) in BYOD infrastructure to mature the DRF and reduce time and cost in the investigation after an incident. In this study accuracy of the DFI is conducted, to minimize the cost and time for investigation. The maturity level is increased by collecting patterns of malicious activities from different Threat Intelligent platform
N4.	BYOD Authentication Process (BAP) Using Blockchain Technology[24]	This paper studied a model of BYOD authentication technique using Blockchain, which is considered as a secured model. The paper concluded with BYOD blockchain technique authentication with a self-service portal. This covered the data leakage threat due to unauthorized access. The use of blockchain in the authentication process helps to reduce data leakage and secure the core network from attack.
N5	A Novel Approach on Mobile User Authentication for the Internet of Things.[67]	The user authentication validation technique studied, the Two-factor authentication method is the area of the paper. The dual-factor authentication method has been analyzed for secure communication. Using the Scyther Tool, the computerized dual-factor authentication mechanism is tested as an automatic verification tool with a secured approach.
N6	Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology[54]	The blockchain model of BYOD authentication is the area of research. Record keeping model of authentication is the approach. The multi-factor blockchain secured model is studied. A secured model of blockchain cryptographic authentication model is suggested.
N7	A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT[68] Multiplatform Security	Blockchain an improved model using spectrum chain is studied. A radix of blockchain core algorithm is proposed, to reduce the security challenges which is weakest in the IoT environment. PKI environment is used.

N8	Certificate-based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment[52]	Certificated-based authentication is proposed in the hybrid model. During authentication, a potential attack can strike and can create a cyber-attack. This paper studied the authentication model using a certificate. Certificate-based authentication method proposed in general. Attribute-based certificate signing is proposed.
N9	Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information[59].	In this paper, the Stride-based BYOD threat model is proposed, analyzed threat interaction in BYOD. BYOD internal and external threat interaction to the corporate network is analyzed so that security and forensic threats in BYOD can be understood.
N10	Security risk analysis of bringing your own device (BYOD) system in a manufacturing company at Tangerang[69]	This paper studied the cybersecurity aspect of the BYOD environment to improve security systems with a risk analysis of internal data. This paper concluded with a framework of BYOD with ISO27002:2013. This paper conducted a study on the BYOD security framework on cybersecurity activities to protect the data with Identity, protect, detect, respond, and recover.
N11	Diverging deep learning cognitive computing techniques into cyber forensics[70]	The Paper is based on Deep learning using a machine learning technique for forensic investigation after the crime. Deep learning technique, cognitive computing technology for the forensic investigation. A deep learning Cyber forensic framework has been proposed.
N12	An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD[22]	This paper's concept is the security concern on the cloud with BYOD infrastructure. An enterprise security architecture while accessing SaaS through BYOD. This paper studied the “Sharewood Applied Business Security Architecture”. This paper has concluded the information security architecture of BYOD while accessing SaaS applications on the cloud.

N13	Implement Network Security Control Solutions in BYOD Environment[53]	This paper studied the BYOD users' authentication process. Monitoring and performance parameter of BYOD is focused. In this paper, the authentication process is well framed with the 802.1x model. In this study, 2 VLANs have been created to segregate the traffic. In this study storage capacity was also highlighted for logging.
N14	BYOD IMPLEMENTATION IN UNIVERSITY: BALANCING ACCESSIBILITY AND SECURITY	The paper focused more on the approach of BYOD security guidelines. Study on university campus environment BYOD internet access. This study proposed a clear solution to be in place for BYOD infrastructure. This study needs extended research on BYOD secured infrastructure to build with proper security policies.
N15	Cybersecurity Threats Analysis for Airports[13]	This study is related to Cybersecurity on BYOD in Airport security systems. New-gen E-enabled airport Cyber Security studied. Potential Cyberattack in Airport and aircraft system has been studied. Security approach is required to incorporate in BYOD model. Airport critical infrastructure cyberattack risk is highlighted.
N16	SMARTPHONE TRIGGERED SECURITY CHALLENGES - ISSUES, CASE STUDIES AND PREVENTION[71]	Mobile security challenges have been studied. Preventive measurement to improve mobile security is explored. Mobile-related crimes are explored. The cybersecurity risk is addressed with a set of policies that need to implement.
N17	Future challenges for smart cities: Cyber-security and digital forensics[72]	The smart city components are part of IoT. All devices, humans are connected. A network of the networks where all components are part of the network. Digital fraud and Cybercrime happened. Forensic analysis and finding out the root cause analysis is the important view that has been highlighted. Intelligent artificial is also one of the major points which is been pointed here in this study. Identification of the security threats. This study especially gives the idea of data security on the cloud. Stored data in the cloud does not have enough control, and location of the data. Since cloud data is not an

		enterprise control data center, so data accessed by an unauthorized entity is a risk. Data integrity is an important parameter for forensic analysis post-incident
N18	The Future of BYOD in organizations and higher Institution of Learning[1]	This paper study the use of BYOD for learning purpose, benefit, and flexibility. This paper demonstrated how BYOD is helping the higher education system. This helps in the learning process as explored in this study.

In the next step, all relevant articles are evaluated in detail and documented the major focused area. Different research addressed the different areas of the BYOD ecosystem. Various techniques and methods are proposed to mitigate the identified gap. The below table shows the key area of BYOD major gap mitigation using different techniques.

Table 17: Various research outcomes from potential research

Paper ID	Security risk	Data Security	Deception technology	Detection mechanism	Protection mechanism	Forensic model	data leakage framework	Secure authentication	threat modeling
N1	Yes	yes	No	No	No	No	No	No	No
N2	No	No	Yes	Yes	No	Yes	No	No	No
N3	No	No	Yes	No	No	Yes	No	No	No
N4	No	No	No	No	No	No	Yes	Yes	No
N5	Yes	No	No	No	No	No	No	Yes	No
N6	Yes	No	No	No	No	No	No	Yes	No
N7	Yes	No	No	No	No	No	No	Yes	No
N8	Yes	No	No	No	No	No	No	Yes	No
N9	Yes	No	No	No	No	No	No	No	Yes
N10	Yes	No	No	No	No	No	Yes	No	No
N11	No	No	No	No	No	Yes	No	No	No

N12	Yes	No	No	No	No	No	No	No	No
N13	Yes	No	No	No	No	No	No	Yes	No
N14	Yes	No	No	No	No	No	No	No	No
N15	Yes	No	No	No	No	No	No	No	No
N16	Yes	No	No	No	No	No	No	No	No
N17	No	Yes	No	No	No	Yes	No	No	No
N18	Yes	No	No	No	No	No	No	No	No

Limitations in these studies concerning the targeted research are identified as mentioned in below table

Table 18: Limitations of the study and gap analysis

Article ID	**Author**	**Gap Analysis**
N2	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology**[33]**	Approached is towards deception technology which is a reactive mechanism. The advanced level protection mechanism is the next phase of the study which is pending for the next level of study.
N3.	Improving Forensic Triage Efficiency through Cyber Threat Intelligence	This study can be extended to detection and protection mechanisms as well. Threat prevention can be the next approach before the incident in endpoint, network, and core infrastructure. Digital forensic investigation and automatic prevention mechanisms can be considered. For further study in BYOD infrastructure which is pending
N4	BYOD Authentication Process (BAP) Using Blockchain Technology**[24]**	Authentication mechanism can be further studied with certificate-based authentication to automate BAP while keeping the same security level to protect the BYOD infrastructure
N6	Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology**[54]**	Instead of user interaction more, this can be reduced with certificate-based cryptographic authentication using the key, and authentication parameters

N15	Cybersecurity Threats Analysis for Airports**[13]**	The extended study required in threat hunting modeling in BYOD to build cyber secured BYOD ecosystem which is pending to explore
N8	Certificate-based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment**[52]**	The certificate-based advance level authentication mechanism proposed is a 3 tier model, but again next level BYOD authentication loophole mechanism is missed which arises post-authentication expiry date and if a valid certificate exists with the user.

Post-development of the new approach and technique for detection and protection mechanism comparison was done to represent the benefit. The below table shows the comparison and new approach.

Table 19: Comparison of existing study and the new approach

Problem	**How this is addressed**	**New Approach**
Unauthorized access-Data Leakage	Authentication user trust model basis	Integrated module of Certificate-based model/user id and pass. Then integrated with detection of forensic technique.
Authorized access- Data leakage	Record storing blockchain process	Detection and Protection new concept introduced in an existing system integrated with an integrated logs management system
Evidence for BYOD data leakage	Evidence collection using Blockchain	NG DFR model introduced for complete forensic investigation in BYOD

Deception Technology	BYOD Honeypot technology was used in 2016 (2002C,.1989d), and in 2019 "Threat intel platform introduced" for detection and FEMA framework in 2019.	NG DFR Model introduced for threat control for zero-day attack prevention in BYOD infra and back-to-back DFR developed.

The baseline existing approach and the new approach were also presented in the below-mentioned block/architecture figure.

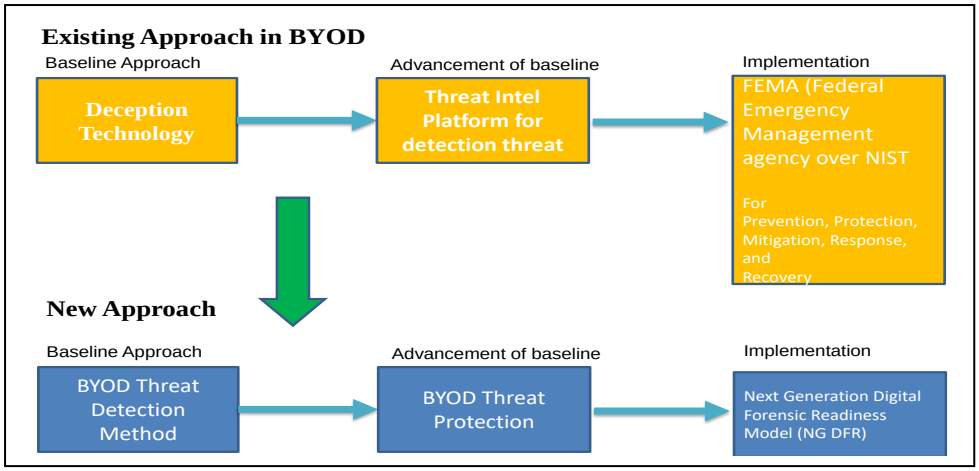

Fig. 14. Comparison between existing approach and New Approach

In the existing approach, deception technology is available and different framework were created for threat detection. As shown in the figure mentioned below, we finally designed the Next Generation Digital Forensic Readiness Model.

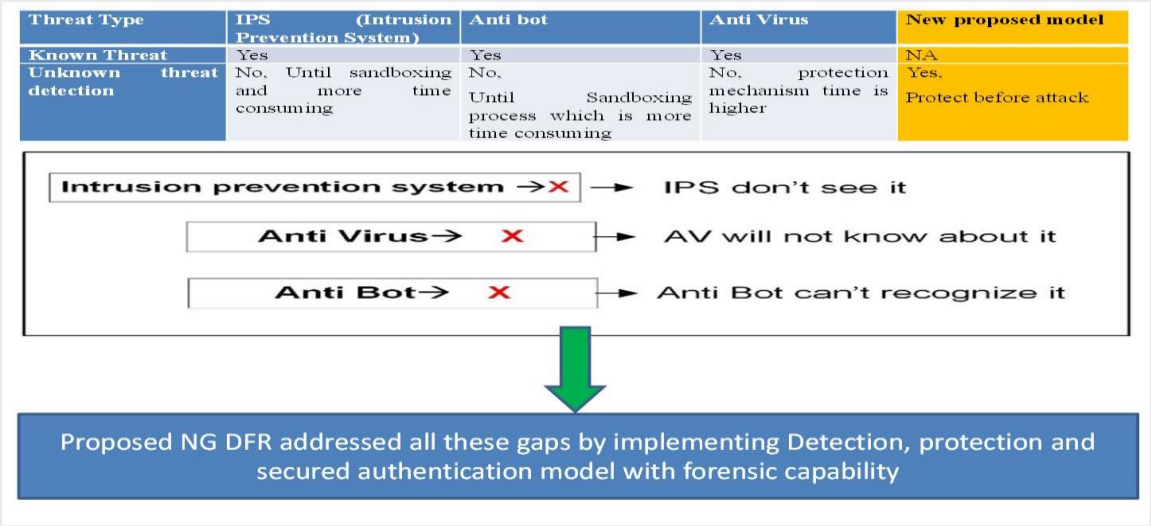

Fig. 15. New defined NGDFR Approach

4.8 Contribution

The increased trend of cyberattack is challenging the corporate business ecosystem and cybersecurity has also become a business survival reason . Identifying malicious category of traffic and proper behavioral analysis in BYOD environment is one of critical key requirement of the industry as they help to build cyber secured BYOD ecosystem. Most specifically identifying source of attack. From this simulation we have identified a mechanism for detection of malicious category of traffic.

For secure onboarding of the BYOD users, a certificate-based mechanism has been considered as the most secure method. In this research, we have identified and explained the loophole in a secure certificate-based authentication mechanism and also developed a novel approach and proposed as a solution to mitigate risk included with the identified loophole. After a cyber-attack, a major concern is to collect the logs and digital evidence for further analysis and threat hunting to trace the source of the attack to be presented for forensic analysis. This concern is also considered in this study and an advanced level log analysis mechanism is proposed. Finally, the "Protect" protocol is proposed to adopt while implementing BYOD infrastructure. "PROTECT" architecture successfully protects the critical infrastructure from malicious user access. Even after doing certificate based

authentication security risk to the infrastructure was observed. An extended study of practical approach of detecting and protecting malicious activity in various phases of BYOD is conducted for achieving cyber defense ecosystem.**[88]**.

4.9 Summary

This research demonstrated a practical approach to the secure BYOD implementation mechanism which can be applied to develop a cyber secure and forensic ready infrastructure for the organizations. A novel approach is also presented in this research to enhance the security layer of BYOD infrastructure. Initially, a loophole area is identified in the study with the secured certificate-based BYOD model. To mitigate the loophole and related vulnerabilities a detection technique is developed and the algorithm is designed which can detect malicious activities and unauthorized access to critical infrastructure. In the next step after detection, an advanced level of protection mechanism is designed. After a cyber-attack, a major concern is to collect the logs and digital evidence for further analysis and threat hunting to trace the source of the attack to be presented for forensic analysis. This concern is also considered in this study and an advanced level log analysis mechanism is proposed. Finally, the "Protect" protocol is proposed to adopt while implementing BYOD infrastructure. Future research in this landscape is more into traffic analysis of cloud environments with BYOD infrastructure.

Chapter 5: BYOD Cyber Forensic Ecosystem

5.1 Motivation

After Covid 19 , the world seems to be on halt and organizations are forced to adopt different working cultures such as work from home or work from anywhere which has developed need for BYOD infrastructure. In this challenging situation, onboarding untrusted devices in the corporate network becomes a necessity for enabling working from home for business sustainability. But it has augmented the substantial risk of the cyber-attack which lead to a major reason for business interruption.

Detecting cyberattacks, conducting forensic investigation post-incident and detecting malicious activities from the BYOD endpoints is the most challenging task. Thus, the advanced capability of threat detection and forensic readiness of BYOD model for evidence collection is a prerequisite to ensure secure onboarding of untrusted BYOD endpoints in the corporate network.

A strategic practical approach is presented in this research to detect malicious activities so that organizations can adopt to protect the critical infrastructure. To achieve the goal of detecting malicious activities in the BYOD environment, simulation was performed in 3 phases. In, the first phase, simulation was performed when the BYOD endpoint was outside the organization over the internet without a VPN. In the 2nd phase, simulation was performed where the BYOD user was securely onboarded using a corporate wireless network. The 3rd phase of the test was done where the BYOD endpoint was outside the organization with a VPN. In all phases, malicious events are detected and analyzed with different tools and techniques. A unique robust scalable model put forward significant results in conclusion for creating a secure cyber forensic ecosystem in a BYOD environment.

5.2 Challenges

This section presents the gap analysis between the existing architecture of BYOD and the secured model of BYOD authentication using different authentication mechanisms.

During onboarding of the BYOD users on corporate trusted network authentication mechanism has a significant role in reducing attack. An extended approach of the existing study [24] on Blockchain Authentication Mechanisms further studied to decrease the overhead of the user provisioning process for a secured BYOD. And to keep all the parameters of BYOD Authentication Process (BAP) for analysis purpose. Thus, for secured onboarding, the secured authentication process is developed to enhance Blockchain authentication mechanisms. After onboarding of the BYOD users, to protect the infrastructure from cyber attacks and malicious activities, a protection mechanism needs to be further explored.

Moreover, after an attack digital forensic investigation should be conducted, so BYOD infrastructure needs to be designed in such a way that digital evidence is available. Post cyber attack in BYOD infrastructure analysis of the crime, collection of the evidence, preservation, chain of the custodian, and presentation of the evidence with the court of law on time as a part of a digital forensic investigation become a mandatory requirement. BYOD forensic investigation is finding of evidences using multiple technologies. But if the onboarding process can be addressed, most of the incidents can be avoided. To combat with increased cybercrime, further study is required in digital forensic investigation and threat hunting mechanism. Study extended to explore existing model of DFR[33] for cluster deployment across multiple locations to analyze large-scale potential digital evidence and threat.

Digital Forensic readiness of BYOD infrastructure is required to combat today's advanced level of cybercrime. Multiple research in this area has been conducted for continuous evolvement of forensic technology since new technologies are adopted, deployment approaches changed, and methods of attacks evolved as stated in a study by Deloitte[45].

Due to the COVID-19 pandemic situation, network has become more vulnerable and attackers are targeting organizations due to changing traffic patterns during WFH. As the traffic patterns changed in the reverse direction, in some cases, the hybrid model of traffic has opened up a new threat corridor.

Lockdown has necessitated enterprise and government critical infrastructure to enable working from home using remote VPN services or to enable Bring Your Own Device service. Different VPN services have been enabled like Cisco Anyconnect on-premise solution and Global Protect Palo alto VPN services. Cisco Anyconnect usage has increased, which also opened up the channel to support the market[89]. Threat Roundup of Cisco Tallos[90] again reported a new threat due to an increased amount of load and traffic patterns.

The recent cyber incident in Cognizant Technologies has revealed that the cyber threat landscape has started adopting a new model of attack. Major security practice player organization like Cognizant[91] was hit by Maze ransomware attack on 18th April'20 [92]during Covid-19. Thus, the pandemic situation has triggered to re-architect the traditional IT infrastructure and build a cyber-confidence techno-centric architecture, an alternate method of the work environment so that the business ecosystem can be driven remotely and BYOD services are enabled widely.

In 2018 it was predicted that BYOD services will be increased by 2022[2] from 35% to 75% but due to multiple reasons it showed exponential growth. BYOD devices are unmanaged devices that might have more vulnerabilities and may not have minimum security defense mechanisms for malicious content[51]. Once BYOD user is onboarded and become corporate trusted device, risk of incident increased to 62% due to the inside users [87] increased.

5.3 Available existing approaches to address the challenges

There are different methods and techniques developed to mitigate the challenges which are formalized over time. The existing challenges and available approach, techniques , various methods to address them are described in below subsequent sections.

5.3.1 BYOD Certificate-based 3-Tier Secured Model

The multi-factor authentication and certificate-based hybrid model with 3 tier captcha is a successful model in the BYOD [52]. A secure communication mechanism with a dual-factor authentication method has been explored and tested for automatic verification using Scyther Tool for a secured approach in IoT[27] environment. While BYOD is in LAN, a

secured model of onboarding was also explored using the 802.1x authentication security control[53] mechanism.

5.3.2 Secure BYOD with Encryption Model

To secure corporate data, encryption in BYOD is a successful technique [26]. End-to-end encryption and cryptographic method of network security in recent research of 2019 has become a principle approach to secure BYOD model [62]. However, during Denial-of-Service Attack (DDoS) on remote access services network of BYOD, traffic gets congested and remote site authentication traffic traversing became a critical aspect [63] that need to be explored and mitigated with IDS/IPS technology.

5.3.3 Blockchain based Authentication for BYOD users

The multi-factor authentication model based on Blockchain was one of the progressive models to authenticate BYOD users and offer additional security [54] in the BYOD environment. The self-service authentication model was another aspect to be studied for reducing the risk of data leakage and protecting unauthorized access [24].

5.3.4 Deception Technology

In 2016, a Deception technology called Honeypot technology for the detection of threats in BYOD infrastructure was explored. Further, threat detection mechanism for root cause analysis became important aspect of this study[33]. Integration of honeypot technology with cyber risk management process of Federal emergency management agency (FEMA) mission where five preparedness FEMA [55] was also studied subsequently. Extended next-level research was also conducted in 2019 which was an improved version in the study of "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology [33]". In the same direction, Intelligent Threat Platform was another study for detecting the incident where accuracy has been analyzed [34]. To increase the accuracy level of malicious activities using audit logs collected from Intelligent Threat sources, accuracy has been analyzed as 90.73%, 96.16, and 93.71% [34].

5.3.5 Threat Interaction model

The threat interaction model proposed for analyzing different threats is a very important study in Stride based model[59] in the BYOD environment where internal and external threat interaction was studied which further helped in forensics analysis. Adoption of

GetVPN[61] in BYOD where segregation of traffic was another novel study. Encryption with Getvpn[61] in isolating corporate traffic from untrusted traffic is a reverse adoption for diversification of external and internal traffic[60]

For malicious activity detection in the BYOD infrastructure, different tools, methods and technologies already existed which are developed over time. But digital forensic ecosystem needs a more advanced level of detection mechanism. Unfortunately, due to the recent threat advancement and attacking methods with heterogeneous landscape, complexity, and advancement, this is an impending area for building a reliable forensic ecosystem. This required dedicated consistent effort towards the inclusion of new abstracts so that digital forensic evidence with end-to-end back-trace capability can be developed with a more accurate potential threat detection mechanism.

It is also possible to stumble potential evidence related to forensic due to lack of correlation of logs used in the BYOD infrastructure. What makes investigation difficult or non accomplishment of identity is lack of backtracing of logs. Also due to the huge amount of data, logs, traffic logs from various components, the lack of integration makes investigation challenging.

5.4 Design and Implementation

Analyzing the pattern of the attack, traffic from different sources and directions is required for diversified testing. So that best possible result from simulation can be captured for analysis and the cyber secured model can be industrialized.

In the first phase of the research, BYOD users were in remote area and used their personal devices. Their BYOD devices were onboarded in the corporate network to access internet using multi-layer security. This scenario was specially designed and tested considering the pandemic situation where work from home has become the only option for the workforce.

After Covid-19, organizations required to onboard BYOD users from office locations using corporate network and from remote as well. This is a challenging situation for the corporates where risk is included to overcome malicious attacks. Thus, a security focused compelling solution became key area in this research.

5.4.1 Phase 1: BYOD users overs the Internet without VPN.

In this phase, BYOD users were situated outside the organization and their personal devices were connected to the corporate network without VPN (Virtual Private Network) services.

5.4.2 Phase 2: BYOD users over the corporate network

In this phase, BYOD users were seated inside the organization, connected to the corporate wireless network using personal untrusted devices and malicious activities were inspected.

5.4.3 Phase 3: BYOD users Over the Internet with VPN

In this phase of testing, BYOD users were placed in an off-trusted network using VPN services to connect with the corporate network and suspicious activities were inspected.

5.4.4 The architecture of the BYOD from the Internet WITHOUT VPN

The architecture used during the testing is mentioned in Fig. 16 below.

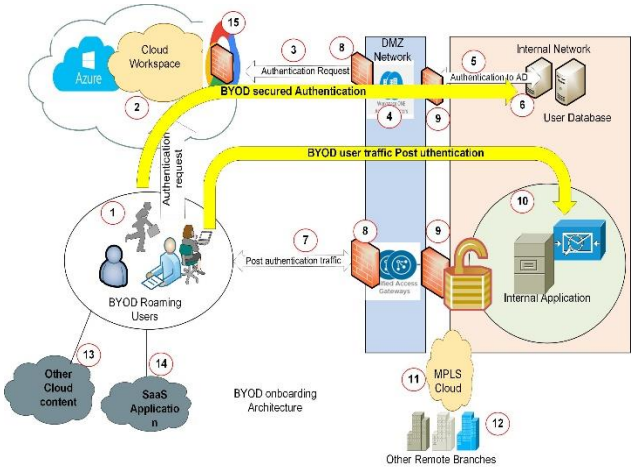

Fig. 16. BYOD onboarding architecture

As mentioned in the architecture of the traffic flow of BYOD users we used different components during the testing which are mentioned in Table 16.

Table 20: The index used in Fig. 16

Index	Description
1.	BYOD Remote Users
2.	Cloud onboarding workspace services
3.	Authentication Request

4.	DMZ segment Workspace Access connector
5.	Authentication to Active Directory
6.	Internal Active Directory
7.	Post Authentication traffic
8.	Enterprise DMZ firewall
9.	Internal Firewall
10.	Internal Application
11.	MPLS Cloud trusted
12.	Remote Branches
13.	Cloud-based traffic
14.	SaaS-based traffic
15.	Cloud Security

The two step method used during the research to onboard BYOD devices securely is as follows:

First step of authentication process was completed with an internal active directory, where remote users securely used access connector placed in the DMZ segment of the corporate network. After the authentication process was completed successfully,the actual traffic flow between BYOD users through the internal corporate network was tested securely. In the second step of the test, threats were monitored and detected using external security with cloud platform integrated with GCP (Google Cloud Platform).

5.4.4.1.1 BYOD Authentication traffic encryption to reduce cyber risk

For BYOD users onboarding, user authentication was the most critical process. So, to ensure secured onboarding, an encryption mechanism was used [83] for risk mitigation at the initial stage [84].

The traffic flow of this test is as mentioned in the below table.

Table 21: Traffic flow of BYOD users

Source	**Destination**	**Traffic**
BYOD user	Cloud Workspace	User Identity authentication

Cloud workspace	Access connector (DMZ)	Authentication
Access Connector	Active directory	User identity check
BYOD user	Unified Access (DMZ)	Secure tunnel
Unified Access (DMZ)	Internal Lan infrastructure	Secure traffic channel.

5.4.4.1.2 How end-to-end BYOD services enabled

Initially, BYOD users are required to authenticate to access the services, then this authentication request is forwarded to the cloud access enabler. After that, the access request is forwarded to the organization's access connector situated in the DMZ of the organization as mentioned in Fig. 16 index 3. The access connector forwards the request further to the internal active directory server as shown in Fig. 16 Index 4. Once the authentication request is processed, information is passed to the BYOD user. In 2nd session, BYOD users directly establish the connection to the internal corporate network to access the desired resources.

During the process of secure connection establishment, a DMZ secure gateway was used to establish the connection between the BYOD network and corporate internal network.

5.4.4.1.3 Cloud Security embedded to secure the infrastructure

During the research, the cloud security model was an important aspect which is used in the security infrastructure design of the BYOD for untrusted devices. The secure onboarding process was the most challenging component so the cloud security model was embedded to enforce the security while onboarding untrusted devices.

BYOD authentication traffic is routed to cloud workspace and then forwarded to the organization's DMZ Access Connector used for user identification with active directory server situated in the internal network of the organization. For the security inspection traffic was routed through the cloud security Firewall as shown in Fig. 16 index 15. All security posture check was conducted on the cloud firewall to minimize the attack surface and improve visibility of the traffic passing through the network.

For security control during this test, the Palo Alto network next-gen firewall was used.

The parameter configured on the firewall during the test is shown in the below figure.

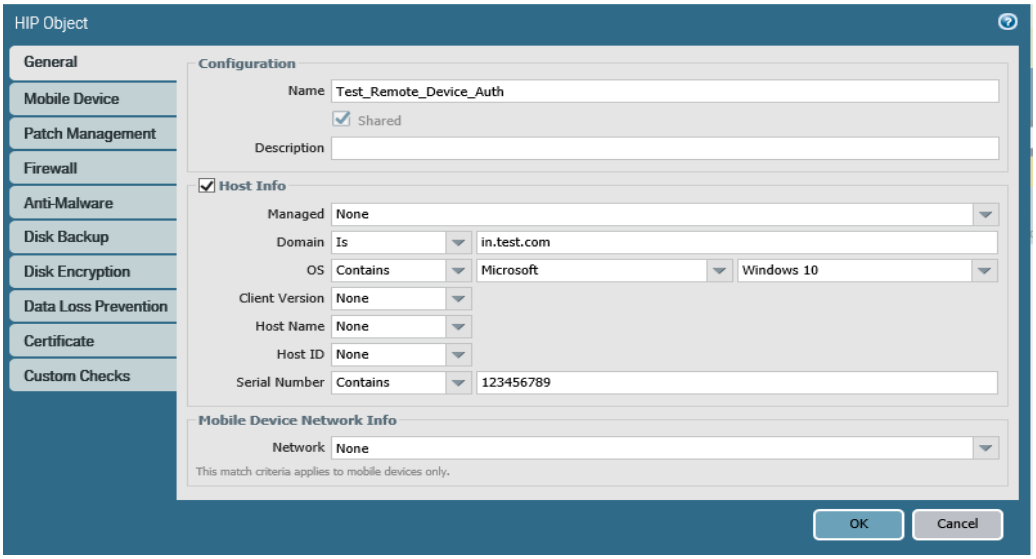

Fig. 17. For security check, HIP conditional parameter configured
(data source as per design architecture table 22, component#2 External Firewall)

This is an important parameter configured for security check and validation of the user when he is having a correct domain, then a specified serial number is assigned to his device. If devices are checked and validated then the first assessment of security check is passed through the configured parameter otherwise malicious traffic is detected and dropped on the firewall.

To check the security posture of the remote BYOD device, 2nd HIP parameter was configured which validates if antivirus is updated on the remote untrusted devices or not, as shown in Fig. 18 below .

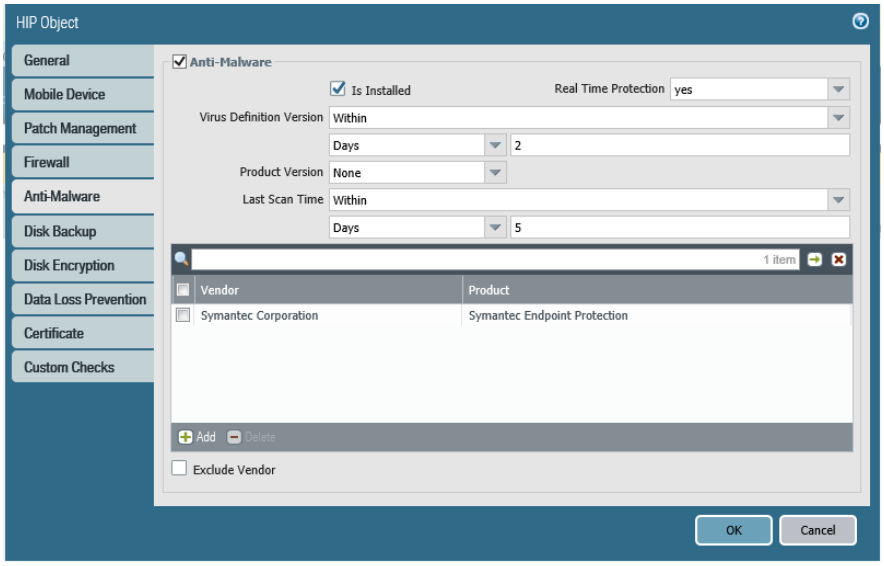

Fig. 18. The HIP conditional security parameter

(data source as per design architecture table 22, component#2 External Firewall)

Through this HIP parameter, remote devices were filtered out if the devices don't have anti-virus updated, while devices with updated Anitvirus status passed the HIP parameter, and traffic was allowed following other security checks.By following this 2 step process of cloud security, malicious BYOD traffic is detected and logs were collected for the analysis.

5.4.5 Architecture BYOD design over the Internet with VPN

In the 2nd phase of the simulation test, we have taken BYOD users sitting inside the organization and using personal untrusted devices connected with the corporate network using the BYOD wireless system.

During this phase of the research, a BYOD environment was established using an internal corporate network where multiple branch offices are connected over the MPLS network with the corporate head office network.

The architecture used during this research was shown in Figure below .

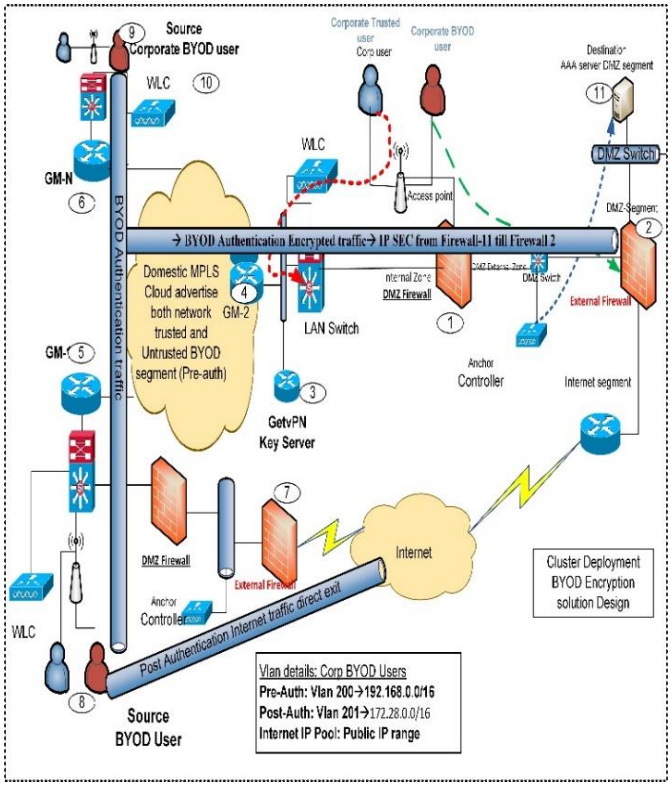

Fig. 19. Internal network design to connect BYOD users

During the pre-authentication, traffic was routed through the MPLS network from branch offices to head office using GETVPN encryption [61] in a secured method [60].

The components used in Fig. 19 during the research are mentioned in Table 22 below.

Table 22: Index of the components used in Fig. 19

Index	Components	Used for
1	Firewall	DMZ segregation firewall DMZ (cisco firewall)
2	Firewall	Internet-facing checkpoint firewall
7	Firewall	Internet-facing checkpoint firewall for BYOD Internet exit
8,9	BYOD user	BYOD user from remote Branch
10.	Anchor controller	Anchoring traffic of BYOD
11	AAA server	Cisco Identity Service Engine used

In this testing, 2 different IP address segments are used for pre and post authentication as per the secured authentication solution [25].

IP address used during the test is as mentioned in Table 23.

Table 23: IP address schema used

Sl No	Pre-auth subnet	Post-Auth subnet	Note
1	192.168.x.x/16	172.28.x.x/16	Subnetting used

During testing of IP addresses schema allocated to BYOD users was 192.168.x.x and user traffic is traversing through 2 layers of the firewall as shown in Fig. 19 (index 1 and Index 2). 2nd layer firewall was used to detect malicious traffic and control traffic as per the corporate requirement.

5.4.6 The architecture of the BYOD from the Internal network

In this scenario, the BYOD user was placed over the internet outside corporate infrastructure. BYOD users are using cloud-based VPN services to connect with the corporate network. A simulation was performed and malicious activities were detected in the testing.

This phase of the study focused on the business continuity plan for the organizations considering the covid-19 when corporates were struggling to continue their business. Most of the organizations were not prepared to handle this situation and after Covid-19, IT infrastructure requirement of the organization got changed and BYOD adaptation became more important for the organizations. The need for secure BYOD infrastructure has increased exponentially after COVID-19.

During the COVID-19 situation, enablement of the workforce for business continuity relies entirely on the enablement of remote VPN services with a collaborative approach. For enabling VPN services for all the employees, it was a challenge.

In this study, we analyzed and explored that both the major objectives , i.e. secure BYOD infrastructure and enabling VPN for all , with major roadblock of cyberthreat in this service is addressed. The major question to address is how to enable the BYOD users during COVID-19 and enable detection and control mechanisms against cyber threats.

In this study, we have done the simulation to build a cyber forensic ecosystem to achieve cyber readiness infrastructure of the organization for using BYOD services where malicious activities can be detected.

We have also analyzed enabling secure remote VPN services using a cloud platform where traffic is coming to the existing private data center of the organization.

In this phase of the study, we have used global protect services as IaaS. For the remote access VPN services, the Global Protect VPN service was used with the authentication of users. In this study step by step process performed is mentioned in Table 24.

Table 24: Sequential process step by step performed

Sl No	Procedures
1	Prisma Access used in GCP
2.	Policies used to protect unauthorized used
3.	Policies for the minimum requirement was as below The user has to be from the test domain Users should have very specific malware protection as Symantec was used.
4.	In case the above cases do not match then disable the access and action triggered as block the user from performing any activities.
5	Monitor and control

During this phase, we have explored that how to securely onboard BYOD users to enterprise networks and detect threats to protect corporate infrastructure.

The architecture used during this simulation is mentioned in Fig. 20 below.

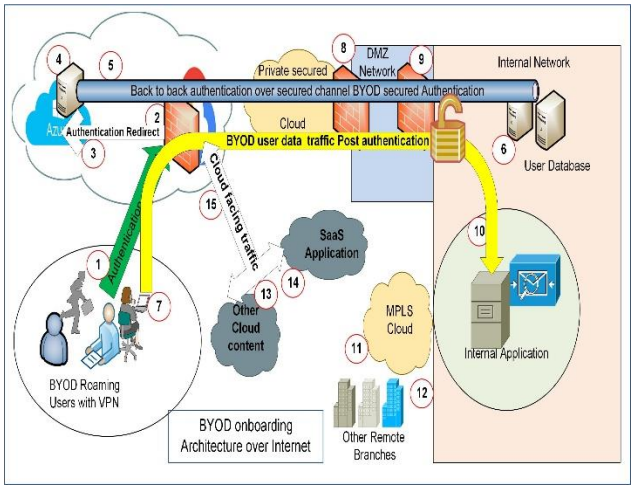

Fig. 20. Phase 2 simulation architecture of BYOD users over the Internet.

In this research, so many different technologies and products are analyzed with a simulation test which was performed to find the study results. Below mention Table 25 mentioned the components and products used during this simulation test.

Table 25: Index of the components used in this architecture

Index	Description
1.	BYOD Remote Users authentication traffic to cloud Palo Alto Firewall
2.	Cloud-native Palo Alto Firewall for VPN authentication
3.	Authentication request to Azure AD for user check
4.	Cloud Active Directory (Azure AD)
5.	Federation service Authentication to Internal Active Directory
6.	Internal Active Directory
7.	Post Authentication data traffic
8.	Enterprise DMZ firewall
9.	Internal Firewall
10.	Internal Network unfractured
11.	trusted MPLS Cloud
12.	Remote Branches
13.	Cloud-based traffic
14.	SaaS-based traffic
15.	The direction of cloud exit traffic

Implantation was done with a baseline standard configuration as per the description in Table 21.

5.5 Simulation traffic Direction and parameters

5.5.1 Simulation traffic Direction

In this case, traffic flow direction was tested as mentioned in Table 26.

Table 26: The direction of traffic in the simulation

Source	Destination	Traffic type
BYOD users	Cloud VPN gateway	Authentication

Cloud VPN Gateway	Cloud AD→Internal AD	Federated authentication service
BYOD users	Internal Network	Post authentication data traffic
BYOD users	SaaS application	Internal cloud-hosted services
BYOD users	Internet	Any cloud internet services

As mentioned above traffic was generated from different directions during the test.

During the covid-19 outbreak for enabling secured onboarding of BYOD users, Palo Alto Global protect [93] VPN services were used in the simulation. The users dialed to Palo Alto Prisma [94] [94] cloud using Global Protect VPN services. The service was hosted in GCP (Google cloud platform)[95].

The direction of the traffic flow was as per Fig.21 mentioned below

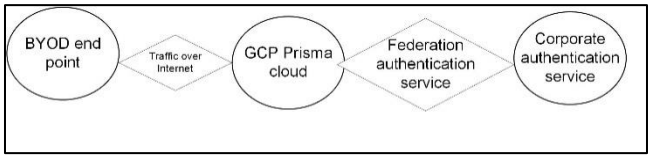

Fig. 21. Corporate authentication traffic flow

While Saas Application traffic flow was as mentioned in Fig.22 below

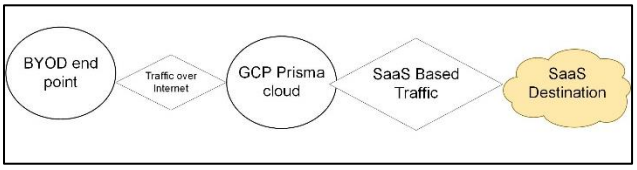

Fig. 22. SasS based traffic flow from BYOD.

And at last internet-facing traffic was filtered and the flow of traffic was as mentioned in Fig.23.

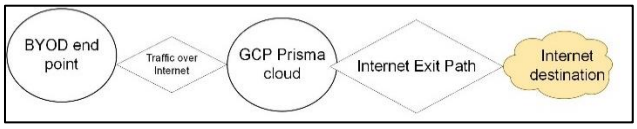

Fig. 23. Traffic from flow remote BYOD to the Internet.

Results and analytics of different traffic categories was detected during these simulations as mentioned in the relevant section.

5.5.2 Simulation parameters

In-order to capture different categories of attack, simulation was conducted in various phases so that attack sources can be back traced. Traffic was captured and analyzed in different traffic direction for BYOD users. Different tools and devices were used as mentioned in above architecture and component tables. During this simulation, few parameters were also defined as mentioned in below table.

Table 27: Simulation traffic parameters

Sl no	**Parameter**	**Protocol/components/reference**	**Design reference phase**
1	Authentication of BYOD users	SAML authentication	Phase 1
2	Access connector	Active directory	
3	Host information profile	OS=windows Domain=in.test.com	
4	Ip address used	Pre-auth=192.168.x.x/16 Post-auth=172.28.x.x/16	
5	BYOD device connected SSID, protocol, connected duration, SNR, Traffic	Detailed as per Table 24	

5.6 Result and Analysis

As the simulation was conducted with 3 different phases. Results are also analyzed in a different section as Phase 1, Phase 2, and Phase 3

5.6.1 Phase 1 result: detection and malicious traffic from internet-facing BYOD users

BYOD remote users are seating outside the corporate network over the internet is the primary focus in this section of the study. To protect the organization from malicious activities and data leakage to maintain the security compliance of the organization while enabling remote BYOD users in the corporate network was the core objective of this section.

Detecting malicious traffic is the first step towards BYOD readiness and data leakage traffic was also captured in the simulation testing as shown in Fig. 24.

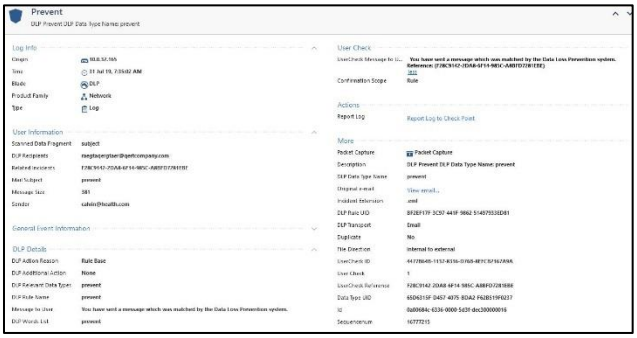

Fig. 24. DLP category malicious traffic

(data source as per design architecture table 19, component#2 internet facing firewall)

In this study cornerstone of the simulation testing outcome was data theft which is a major concern for the organization's integrity and security [96]. As per the test result, data theft traffic was captured from the BYOD endpoint. Fig. 24 shows that the traffic category was DLP and logs detected related to data loss.

While continuing the simulation one more important traffic category was covered which is related to the DoS attack, which was a major external threat that can lead to the data breach. DoS attack traffic detection is shown in Figure below.

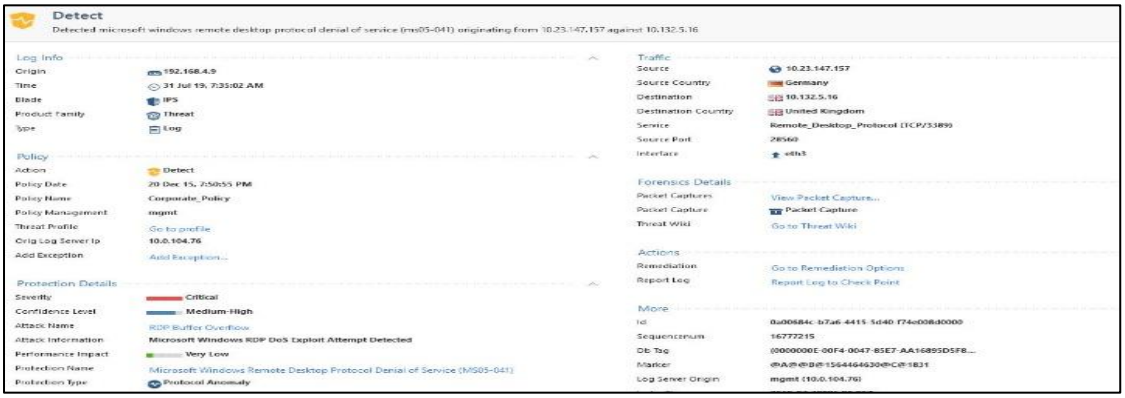

Fig. 25. DoS Exploited traffic

(data source as per design architecture table 19, component#2 internet facing firewall)

Details of the DoS attack traffic which was detected in above Fig.23 is mentioned below.

The detected attack type was "Protocol attack". A protocol anomaly which is not normally detected by rule-based model and DDoS attack detection was "Microsoft windows RDP DOS Exploit". In this case, the traffic was detected as a threat and severity turned critical. Further, it was found that name of the attack is "RDP buffer overflow" which is stack-based overflow. This attack is in the category of flooding attack which slows down the system and executes further attacks. The system kept in critical infrastructure was compromised. DDoS attack category was "Zero-day DoS Attack". Post this threat, it was also noticed that data theft occurred from internal to an external network from critical infrastructure using BYOD devices.

Further investigation was conducted to identify the users and devices as shown in result section phase 2. As we continued the test and moved one step ahead for further detection of the endpoint, we found the result of the BYOD device virus status from where malicious traffic triggered for different threat categories as shown in Fig. 26.

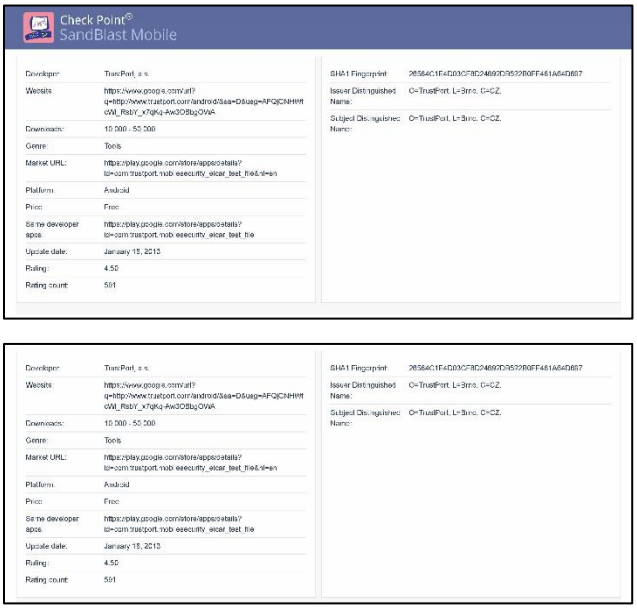

Fig. 26. Mobile device test remotely

(data source as per design architecture table 19, component#2 internet facing firewall)

This result also shows the device details of BYOD which was further investigated.

Finally, we explored the attack vector, threat factor and event category summary of the complete infrastructure and found the significant details which were beneficial for the complete landscape view as shown in Fig. 27.

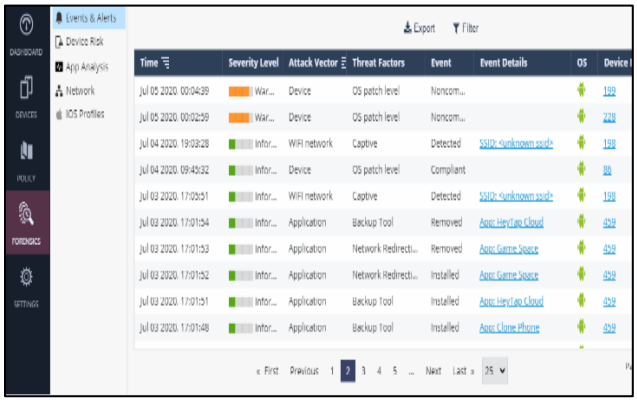

Fig. 27. The complete landscape of threat factors, attack vector and events

(data source as per design architecture table 19, component#2 internet facing firewall)

This was a significant summary result of the study and further details were also mentioned as per device category.

At the end of Phase 1, the result summarized the security compliance of all BYOD endpoints, where a cross functionality of different technologies used. Results are shown in Fig. 28.

Fig. 28. Security compliance dashboard

(data source as per design architecture table 19, component#2 internet facing firewall)

A security compliance dashboard was generated showing all security events, top threats, risks, and all BYOD devices. This dashboard is helpful in the analysis of user activity and behavior and gives the direction of the security policy across the platform.

5.6.2 Phase 2 result: detection and malicious traffic from internal segment Connected BYOD users

In this research, while exploring insider threats we have detected and observed that most of the malicious traffic generated is from the inside network to the outside network. Logs are collected at the external perimeter firewall as shown in Fig. 19 index 2. For security, traffic was encrypted through EoIP[97] tunnel of the corporate network and directly landed at the external firewall while BYOD untrusted devices were connected with corporate network access point. Fig. 17 index 1 firewall was used for the encryption and at 2nd firewall, all BYOD traffic was filtered. Using Ethernet-Over-IP Tunnel (EoIP) untrusted traffic is routed towards layer 2 and the gateway of the BYOD devices was used in the external firewall (Fig. 19, index 2) to isolate corporate trusted network from untrusted BYOD traffic. All BYOD traffic was securely routed through the corporate network without impacting the internal network and at the gateway level, all malicious traffic was decrypted and detected. BYOD users were using the IP address of 172.28.x.x segment to access the internet after secure authentication. In this research with the simulation testing, we have explored that pre-authentication and post-authentication traffic was filtered for malicious content at different levels as mentioned in Figure below.

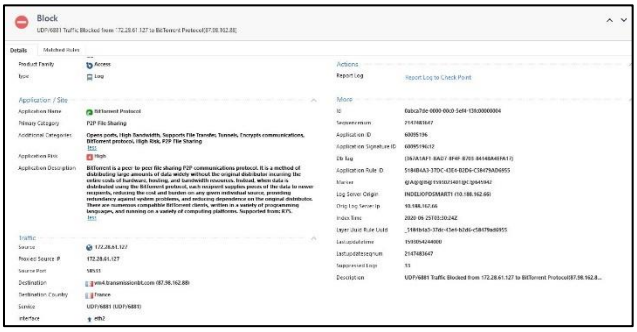

Fig. 29. Malicious traffic from internal BYOD devices

(data source as per design architecture table 19, component#2 internet facing firewall)

For the analysis, an internal threat from IP address 172.28.61.127 is detected. This BYOD device has generated malicious traffic to BitTorrent Protocol which is categorized in the primary category of P2P file sharing.

During the research, internal BYOD-generated threat was analyzed so that investigation can be done based on the evidence collected by the system. While proceeding further in the

research, BYOD user traffic was analyzed and it was observed that different types of malicious traffic were detected in the system and logs were captured for further investigation as shown in Fig. 30.

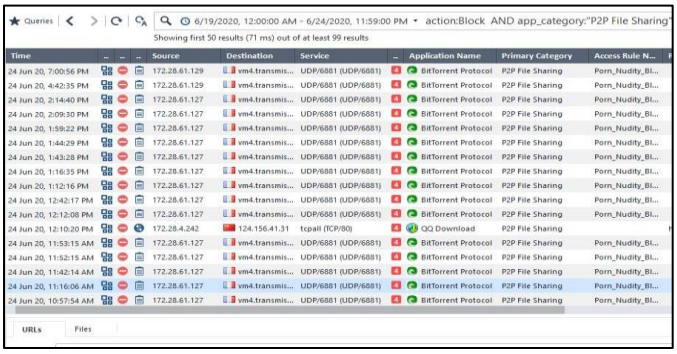

Fig. 30. BYOD malicious traffic logs

(data source as per design architecture table 19, component#2 internet facing firewall)

Malicious contents were detected using a Checkpoint advance application-layer control blade,[98]as shown in Fig. 30. Malicious traffic was triggered from IP address 172.28.61.127 and 172.28.4.242 and generated for BitTorrent protocol and P2P category file sharing. Logs were further used during the investigation of the user activity.

Also, the backtrace of the BYOD user was conducted during the research. This backtrace was performed with a AAA server where secure certificate-based authentication [25] was done and Cisco Prime was used to trace the identity of the user.

Identification of the IP and tracing BYOD user for malicious activity was the most critical part of this research. During the simulation, we used Cisco prime and Cisco Identity Service Engine for user identification and tracking. Since the user was connected on wireless access point, Cisco Prime logged the IP address with the user and the device identity found was as mentioned below.

As captured and shown in Figure below , 172.28.61.127 IP address was used by having an Android device with mac address 2E:70:8E:93:CF:6A. This shows that the user with IP 172.28.61.127 connected on the research SSID during the time of malicious activity.

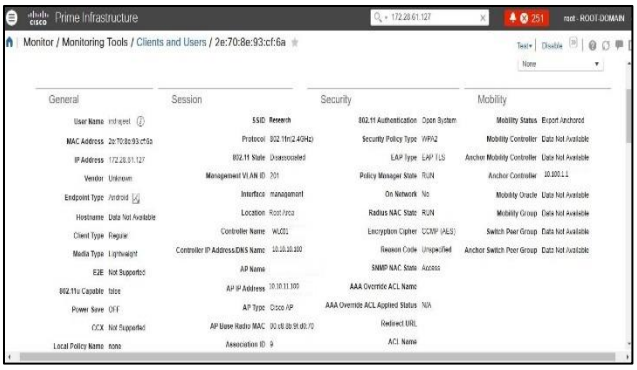

Fig. 31. BYOD IP to device identification

(data source as per design architecture table 22, component#2 internet facing clod native firewall)

The historical data of the BYOD user connectivity and associated IP address was also found from cisco prime. Table 28 shows that the IP address associated with the users and connection time matches with the logs are the evidence, leading to further investigation.

Table 28: BYOD device backtrace association details

(data source as per design architecture table 19, component#10 Anchor controller)

Association Time	Duration	IP Address	User Name	SSID	Protocol	RSSI (dBm)	SNR (dB)	Traffic (MB)
2020-Jun-24 11:16:43.462 IST	50 min 49 sec	172.28.61.127	indrajeet	Research	802.11n(2.4GHz)	-62	32	39.1
2020-Jun-24 12:07:33.510 IST	50 min 42 sec	172.28.61.127	indrajeet	Research	802.11ac	-48	46	0
2020-Jun-24 12:58:16.316 IST	1 hrs 45 min 38 sec	172.28.61.127	indrajeet	Research	802.11n (2.4GHz)	-50	49	80.7

2020-Jun-24 14:43:55.534 IST	3 hrs 18 min 0 sec	172.28.61.127	indrajeet	Research	802.11n (2.4GHz)	-49	49	34.3
2020-Jun-24 18:01:56.068 IST	1 hrs 29 min 27 sec	172.28.61.127	indrajeet	Research	802.11n (2.4GHz)	-49	45	0
2020-Jun-24 11:16:43.462 IST	50 min 49 sec	172.28.61.127	indrajeet	Research	802.11n (2.4GHz)	-62	32	39.1
2020-Jun-24 12:07:33.510 IST	50 min 42 sec	172.28.61.127	indrajeet	Research	802.11ac	-48	46	0

Our next step was to identify authentication and on-boarding details associated with the mac address 2E:70:8E:93:CF:6A so that the detection mechanism is correlated.

As result captured in Fig. 32 from the Identity Service Engine, malicious activity was captured from the BYOD device with mac address 2E:70:8E:93:CF:6A.

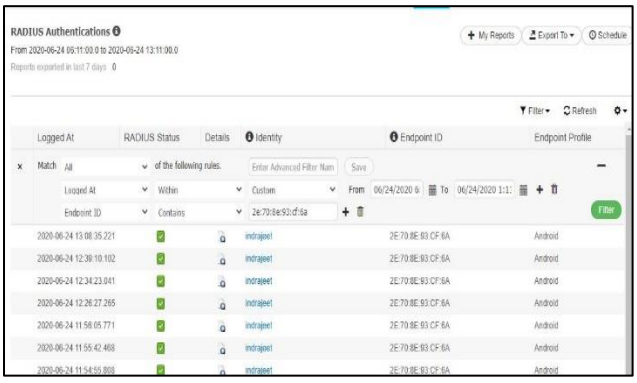

Fig. 32. User identification with detected mac address

(data source as per design architecture table 19, component#11 Identity service engine)

As per Fig. 32, we depict the association of the IP address 172.28.61.127 and the test username indrajeet with mac address 2E:70:8E:93:CF:6A from an android device.

Our final step was finding the authentication logs of the device through AAA to confirm the user information and complete ecosystem of the detection model.

To confirm this, AAA authentication logs were checked and it was found that the same device was authenticated as mentioned in Table 29.

Table 29: Authentication successful logs

(data source as per design architecture table 19, component#11 Identity service engine)

Authentication Details	
Source Timestamp	2020-06-24 11:54:30.583
Received Timestamp	2020-06-24 11:54:55.808
Policy Server	indelise03
Event	5200 Authentication succeeded
Username	indrajeet
Endpoint Id	2E:70:8E:93:CF:6A
Calling Station Id	2e-70-8e-93-cf-6a
Endpoint Profile	Android
Identity Group	RegisteredDevices
Audit Session Id	0abc9ac400002fa25ef2bdee
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC01
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.10.10.100
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	ChangeVlan
Response Time	17 milliseconds

This authentication message captured from the logs describes the detection mechanism of the malicious activity in the complete ecosystem.

After correlating logs and information it was concluded that the malicious activity happened in the BYOD environment on 24th June’20 which was detected at the external firewall with

the user Indrajeet having BYOD device with the mac address of 2E:70:8E:93:CF:6A and IP address allocated to him was 172.28.61.127. Malicious activity was detected and evidence was also captured for further investigation. The detection process was completed successfully and demonstrated in this testing.

Application wise malicious traffic was detected as shown in Fig. 33 below .

Fig. 33. Application-wise malicious traffic

(data source as per design architecture table 19, component#7 External firewall)

From the internal network of 172.28.x.x to the external network, traffic was generated for the destination of the restricted category and logs were recorded for further forensic investigation in the ecosystem. This process of threat detection and control mechanism is a continuous process that can be adopted by organizations with ease and optimum security can be achieved.

5.6.3 Phase 2 result: detection and malicIous traffic destined to Internal BYOD

In this phase, we also analyzed the reverse traffic which is found to be malicious in nature. Detection of traffic was completed as per architecture Fig. 19 index 2 firewall and we have identified and segregated traffic of all malicious categories. Traffic under attack category was also detected as shown in figure below

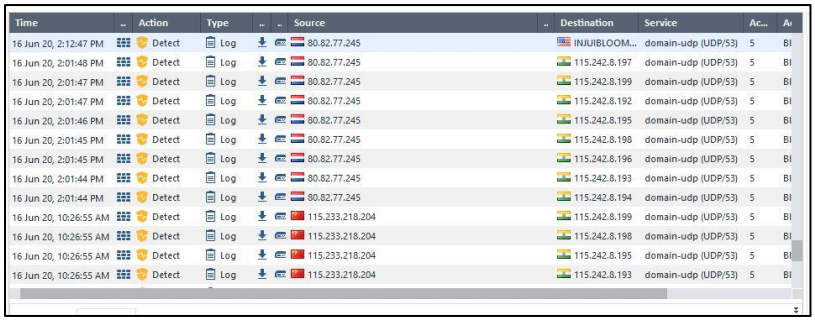

Fig. 34. Malicious traffic from outside destinated to BYOD external firewall

(data source as per design architecture table 19, component#7 External Firewall)

This category of traffic was generated outside network to a destination of the inside network and detected with the detection technique developed in this study.

In this exercise, traffic from random malicious IP was also captured from the external interface of the external firewall (Fig. 19, index 2) and the traffic packet was analyzed using the Wireshark tool.

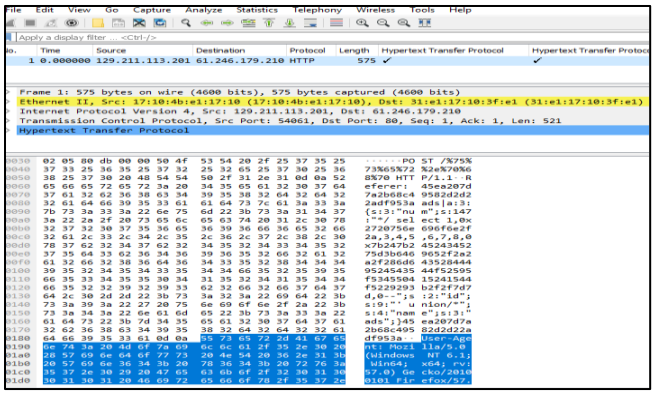

Fig. 35. External firewall packet capture logs from a malicious IP

(data source as per design architecture table 19, component#7 External Firewall)

Packet captured in internal facing firewall and analyzed using wire shark[99] logs.

5.6.4 Phase 3 result: detection and malicious traffic from internet-facing BYOD users with VPN

Results of phase 3 testing were collected and analyzed. In the testing, different category of traffic was processed and analyzed. To analyze different categories of traffic Palo Alto Panorama technology was used and results were captured at Prisma Cloud.

All the traffic traversing through the cloud gateway being inspected at the gateway level. The VPN used in the process is configured in full tunnel mode [100] so that all the traffic can be routed towards a loud gateway and traffic can't be bypassed without inspection. With the implementation of this model, it was assured that any traffic which is pointing towards the organization's internal network and originating from the BYOD endpoint was inspected at the cloud gateway itself. In the 2nd scenario, all the traffic originating from BYOD endpoint towards sanctioned SaaS application is inspected at cloud gateway. In the 3rd scenario, any traffic generated from the BYOD endpoint for the Internet destination was also examined and processed by the Prisma Cloud Gateway. In the simulation, threat landscape was determined and logs were captured as mentioned in Fig. 36.

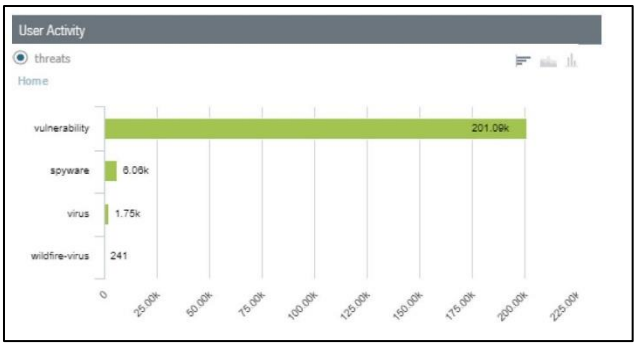

Fig. 36. Threat landscape from Prisma

(data source as per design architecture table 22, component#2 External Firewall)

The result shows that the total number of 6.06 K hits was captured under threat category spyware, the total number of vulnerabilities found was 201.09K during a period of 30 days and the number of virus attacks was calculated to be 1.75K hits.

In the threat landscape, DNS security threat is a major threat [101] which enabled legitimate traffic [102] and many threats and vulnerabilities. In this phase of testing, DNS security threat was inspected and 5.96K traffic hits captured was from the Spyware DNS security category.

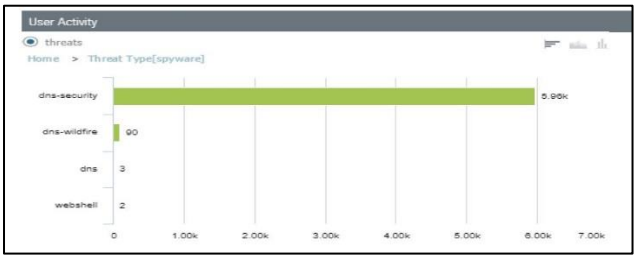

Fig. 37. DNS security threat

(data source as per design architecture table 22, component#2 External Firewall)

Below are the threats which were inspected and blocked.

Threat Name	ID	Threat Type	Threat Category	Severity	Count
generic:wpad.guest.wireless.com	150075	spyware	dns-security	medium	3.9k
generic:domclickext.xyz	283486	spyware	dns-security	medium	910
generic:corp.tmf.co.in	319014	spyware	dns-security	medium	595
DGA Domain	109000	spyware	dns-security	high	111
generic:mytectra.com	119899	spyware	dns-security	medium	85
generic:blog-pinger.com	193330	spyware	dns-security	medium	51
generic:ayefin.com	341034	spyware	dns-wildfire	medium	44
generic:css.digestcolect.com	344282	spyware	dns-security	medium	33
generic:www.aapsis.com	312698	spyware	dns-security	medium	32
generic:kohinoorsteel.com	198288	spyware	dns-security	medium	31
others	others	others	others		282

Fig. 38. Threat details detected and blocked

(data source as per design architecture table 22, component#2 External Firewall)

In the phase 3 simulation, all the traffic generated towards the internet from BYOD endpoint devices was inspected and with the test result, it was demonstrated that malicious traffic was detected for various threat categories with different levels of severity. This traffic was further analyzed using Cortex data lake for forensic investigation of threats and other malicious activities. During the COVID-19 lockdown situation, when employees are required to onboard using the BYOD endpoint in the corporate network, this method of onboarding showed a significant result of developing a secured model of cyber threat detection mechanism which furthermore helped to build a cyber forensic eco-system for the organization for threat handling.

5.7 BYOD malicious traffic pattern

In the testing, we observed that different category of restricted traffic was detected while a large amount of data was generated under different categories of traffic and overall secure BYOD network infrastructure was built to detect malicious activities and control them.

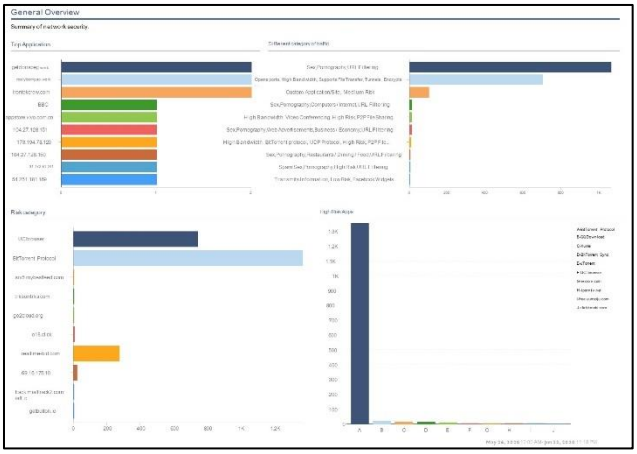

Fig. 39. Captured Different categories of the attack

(data source as per design architecture table 19, component#7 External Firewall)

Traffic was segregated and identified under different attack patterns such as risk wise, category wise as shown in Fig. 39. This broad categorization and assessment of traffic were used for defining the security landscape and policy for the organization. The security policy based on collected information was used by the organization for establishing a secured

BYOD environment. By detecting these risks and attacks which were critical for the organization, policy model was defined to address and to build a secured cyber forensic ready BYOD environment.

5.8 Proposed Cyber Forensic Ecosystem Model- Enhancement on Existing Techniques

A secured cyber forensic BYOD ecosystem needs an advanced level of malicious activity detection mechanism to identify and detect the modern threat landscape. In this study, we have analyzed detection mechanisms and then deployed proper security control so that internal infrastructure risk can be identified and eliminated. We have detected the malicious traffic using a cloud firewall placed between the cloud access broker and on-prem access connector with in-depth investigation done using the on-prem internal and external firewall. The subsequent objective was to protect the internal infrastructure from BYOD insecure and malicious traffic and to collect evidence for forensic investigation of BYOD malicious traffic. Using cloud firewall and DMZ access connector, untrusted BYOD malicious traffic was forbidden to enter inside organization's secure internal network. The most critical task of this model is the detection of cyberattack which was addressed by a detailed investigation process using Checkpoint and Palo Alto technologies.

From a diversified study done over threat landscape and cybersecurity, this was concluded that the major security risk of BYOD infrastructure [13] also carries danger if control and detect mechanism is not implemented cautiously. Thus, when infrastructure is not forensic ready then BYOD can result in "Bring Your Own Danger"[86].

During this research 3rd phase of the simulation was conducted for result analysis from different directions of traffic. Subsequently, different categories of attack and malicious activities were documented as below.

Table 30: Different models of malicious activity detection

Phase	**BYOD setup**	**Detection mechanism**	**Malicious activity detection**

Phase 1	In this phase, BYOD users were kept in remote places over the internet to connect corporate network without a VPN	Malicious activity detected using cloud Security	Yes
Phase 2	In this phase, BYOD users kept inside the corporate network and connected over wireless	Malicious activity detected using on-prem security	Yes
Phase 3	In this phase, BYOD users kept in remote locations over the internet without VPN and cloud services	Malicious activity detected using On-prem 3 layer security	Yes

As mentioned above 3 different phases of the simulation were conducted to conclude the detection process of suspicious activities. Post simulation of different types of BYOD onboarding process from different directions to the corporate network, a model of the standard process of BYOD environment which builds a secured cyber forensic ecosystem was derived as mentioned in Fig. 40.

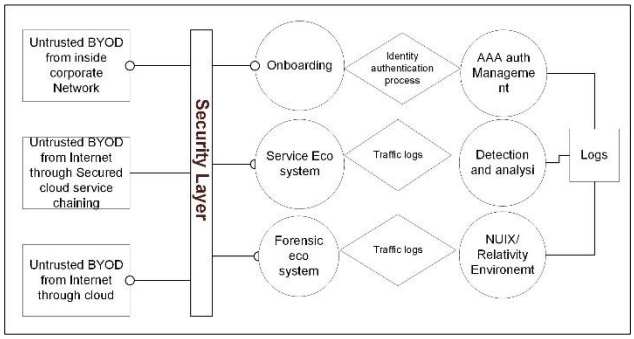

Fig. 40. The standard model of BYOD environment.

At the end of all 3 phase simulations, we also derived a systematic process for BYOD secured ecosystem development modes as mentioned in Fig. 41 below.

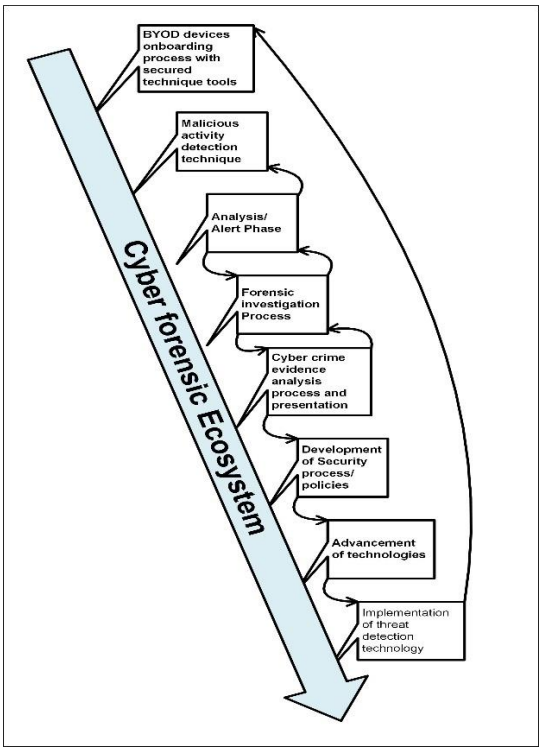

Fig. 41. BYOD malicious activity detection and forensic ecosystem model.

5.9 Contribution

The primary objective of this research was the detection of malicious traffic from the BYOD environment. COVID-19 situation has changed the entire traditional model and adopting BYOD infrastructure became requirement. Malicious traffic became critical risk for the corporates due to associating cybersecurity risk with BYOD. It was meant that alternate methods of the working environment should be cyber confident and reliable, so a secured model of BYOD infrastructure with cyber forensic capabilities was developed.

A very important contribution of this research was the detection of malicious traffic from BYOD untrusted users to protect the critical corporate network. While organizations continue to enable the BYOD services as per today's ongoing demand but onboarding of untrusted devices includes risk to the organization's critical IT infrastructure. This research contributes to defining a mechanism for detection and protection of malicious BYOD traffic. For the security control mechanism checkpoint and Palo Alto technology were used which also contributes to malicious content detection and analysis.

5.10 Improvement In Existing System

Advance level of detection technique and unique mechanism of detecting malicious activities is an ongoing requirement to create BYOD cyber forensic ecosystem. Primary components that are required post an incident in the digital Forensic ecosystem contain are [31] Network level forensic readiness infrastructure, Computer forensic, also forensic in the Mobile ecosystem, and forensic in the database area. The forensic ecosystem remains incomplete until it includes the [32] Process of Human and digital evidence. The major point is post an incident tracing back to the source of the attack[13]. Various tools and techniques were also explored in the past for network forensic[103] which needs an advanced technique for building a cyber forensic ecosystem and different frameworks also have been studied[104].

This research is focused on a new abstraction with more efficient technique and practical approach for detecting malicious activities in the BYOD environment.

5.11 Summary

This research aimed to build an advanced level detection mechanism and to control malicious activities in organizations. Checkpoint sandblast for threat extraction mechanism and Cisco ISE for AAA and Palo Alto technology was used in this research. By using all these techniques and tools, it was possible to build a secured BYOD infrastructure where malicious activities are detected and investigated. By using a certificate-based AAA authentication model with a combination of advanced security technology every user can be back-traced and collected evidence of all suspicious activities can be analyzed for further investigation. This research concludes the mechanism for detecting malicious activities by insiders as well as outsiders and protecting the organization’s critical infrastructure from cyber-attacks. 2nd part of the research was to control the BYOD insiders' malicious traffic and build a progressive level mechanism to build a cyber forensic ecosystem so that detection, control, and investigation correlate with logs and artifacts. Post analysis of this experimental study and simulation, it is observed that the proposed method provides an advanced BYOD forensic ecosystem. Furthermore, this mechanism is also beneficial not only to detect malicious activities and attacks but also to control the attack in today’s

advanced threat trend. In future work based on this research, we will focus on building an advanced level forensic ecosystem.

With this research we have combined and accompanied a multi-vendor community environment, but the outcome is not sufficient to combat today's threat landscape. Security OEMs need to adopt a collaborative approach and work towards developing a compatible standard ecosystem to protect the organization from existing and emerging cyberattacks.

Chapter 6: Next-Generation Digital Forensic Readiness Model (NG-DFR Model)

6.1 The motivation of the proposed Model

Intel's "Bring Your Own Device" (BYOD) as an alternative workplace solution quickly became popular. With the BYOD solution organizations can enable employees to use devices of their choice either personal or corporate to perform business activities, leading to increased productivity and employee satisfaction. However, BYOD also brought associated risks because of the untrusted traffic sources and loopholes in the design.

Since the inception of BYOD, there has been development in the design and implementation models whereas cybersecurity risk and attack methods have also got developed.

This research have two principle objectives: The first aspect of the study was to develop a mechanism to detect and protect the BYOD environment from advanced level attacks which cannot be detected by traditional tools and techniques even though available tools are quite effective and have the potential to defend against cyber attacks. To protect the organizations before the attack can trigger damage to the critical infrastructure due to BYOD threat, a strategy was indeed the principal requirement .The second focus area of the research was towards developing a forensic investigation model and proposing an effective approach by providing a reliable forensic investigation infrastructure to collect digital evidence and detect the source of the attack. As per the objective of this study this research work succeeded in developing and proposing two novel approaches. The proposed technique in this study leads to a significant contribution towards secured BYOD adoption by identifying threats before a cyber-attack causes disruption. The second approach of this study proposes a peculiar approach towards the Next-Generation Digital Forensic readiness (NG-DFR) model to develop a cyber forensic ecosystem and enable a cyber-secure BYOD environment. With this model, organizations can consolidate all digital information and malicious activities to strengthen the cyber forensic ecosystem.

6.2 Inside of the proposed NG-DFR and open challenges

Bring Your Own Device (BYOD) is one of the element of consumerization of information technology (IT). It helps the organization to save cost and increases employee productivity

and engagement, enhances collaboration and business agility as employees don't have to deal with multiple devices and they can choose a device of their choice to work.

As, the demand for BYOD services are increasing various studies conducted in this direction and concluded that BYOD users are expected to increase in coming years. During the initial stage of the BYOD solution adoption, most of the organizations did not give access through corporate networks due to involved security risks as organizations didn't have confidence over the BYOD model. However, in the later stage, organizations started moving towards a positive direction realizing that personal mobile devices are an integral part of employees' daily life and employees must be allowed to use personal devices in the corporate network infrastructure. But it increased cyber security risks, data leakage incidents, malicious activities as BYOD allows untrusted external devices to connect in the corporate wireless network and all the users don't understand the risk included while accessing the internet. Data theft, shadow IT, and cybersecurity constitutes a major concern in BYOD. Unmanaged devices might not be following the standard security practice, all the applications installed on personal devices are not safe as per the organization and are considered to be vulnerable to malicious content[51].

A study concluded that 62% of digital incidents are triggered by inside users either intentionally or unknowingly[87] which is known as insider threats. Using BYOD services, cybercriminals can try to get access to the internal network, leverage the cloud network, perform malicious activities, and damage the potential data which can cause the reputation loss of the organization and business disruption.

Internet users are increasing exponentially in every organization and internet usage will grow more in coming years due to IoT/BYOD, public environment, smart city environment, and digitalization. Cybercrime has become a major crime of the modern era and the government and public/private sector must gear up and come together to fight against this major crime.

In a study, the BYOD security impact assessment conducted for the airport smart system stated that compromised BYOD devices can have an impact on airport system integrity and

availability[21], while it can be leveraged by criminals to heinous terrorist attacks. The possibility of security breaches is prone to happen in terms of the network infrastructure where BYOD service is offered to employees, partners, and staff.

Cyberattack is a major risk in airport security because of BYOD which is a threat for the country [13]. Understanding BYOD-related cyber risk and cyber landscape are necessary, BYOD might become “bring your own danger”[86] if proper security control is not implemented and if the solutions do not include forensic investigation after the crime.

Due to increased vulnerability and modern attack techniques, cyber-attacks have grown periodically. According to CVE [105], Fig. 42 represents the growth of vulnerabilities in past years. Increased vulnerability has also increased the cyber attacks and interruption in business and services.

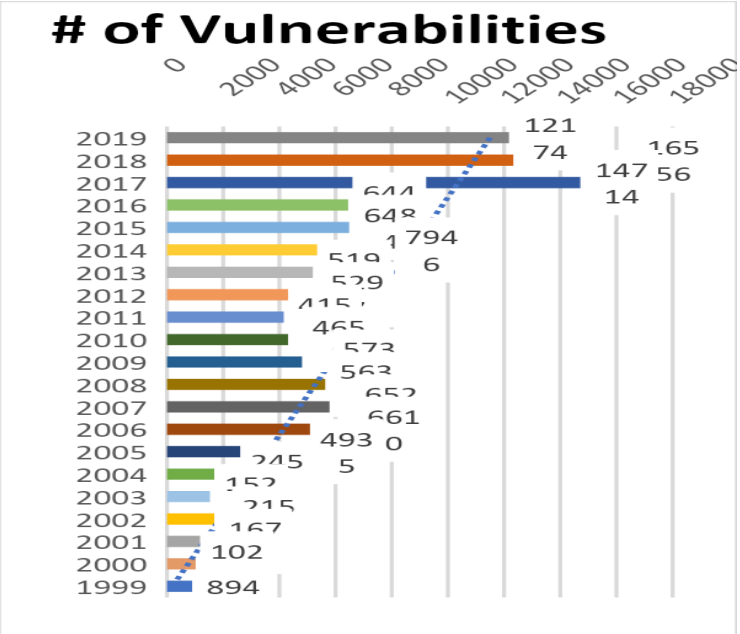

Fig. 42. Vulnerabilities by year (CVE).

The legal approach of the mitigation should be implemented by the organization [83], at every stage of the BYOD. Security policy is required to define to protect the corporate network, data, and business applications.

According to a Survey done by Juniper, 80% of BYOD devices will be considered unprotected. There is a crucial requirement for digital forensic infrastructure in BYOD to provide security and reliability. DFR (digital forensic readiness) in BYOD infrastructure is one of the models that detect malicious activities and user behavior using a deception technology known as a honeypot. To conduct a digital forensic investigation at optimal time and cost, researches have been conducted in the past so that the approach of DFR and CTI (cyber threat intelligence) can be improved. As of now with recent technology and research advancement up to 90.73%[34] accuracy level is achieved in analyzing the root cause after an incident.

A large-scale clustering deployment of BYOD infrastructure needs to coexist with an advanced model of digital forensic readiness infrastructure for the practice of detection and investigation[33]. There are some major components in the digital forensic investigation such as[31] Computer forensic, Network forensic, Database forensic, Mobile forensic. Major components of Digital forensic or cyber forensic includes [32] (a) humans, (b) digital evidence, and (c) process, which are the point of reference. There is a compliance requirement for legal action in the digital forensic investigation during and after a cyber-attack analysis to have event reconstruction, with reproducible and verifiable evidence [106]. Finding the source of attack[13] after an incident is essential in forensics analysis; for example, a novel study was conducted for identifying human behavior in an automated way based on handwriting[107]. BYOD has all those components to be covered in forensic investigation.

In this study, we have also evaluated that the cloud adoption rate is expected to be 83% by 2020 [108]. This increased rate of cloud adoption has increased the demand for BYOD at a much larger rate. All organizations are realizing the need for cloud infrastructure and moving towards cloud services for different applications and roaming user services. Since the increased demand for working anywhere by any device has increased the BYOD demand during the Covid-19 outbreak, which increased cloud service adoption. However, BYOD security and cyber forensic investigation for enterprise networks and cloud networks are major concerns that need to be addressed.

There is a serious need for BYOD forensics as BYOD devices are the most critical component in forensics and the source of evidence [109]. Due to the expanding cyber incident landscape, collecting, preserving, and analyzing digital evidence after an incident and presenting the analysis with integrity is required.

Administration and governments are concerned about this issue all over the world. Government of India has also taken an initiative to strengthen the infrastructure of the National Cybercrime Forensic Laboratory (NCFL) and started a new project called Cyber Prevention, Awareness & Detection Centre (CyPAD). Different questions arise: Are governments or private organizations are ready and capable to defend against evolving cybercrimes? How government and organizations will handle such big cyber forensic investigation and cyber fraud management in a smart city environment where IoT users are in large numbers or BYOD users are increasing every day? Who will supervise and drive the investigation? How and by whom those crimes will be handled? How to collect the evidence against crime activity logs of BYOD/IoT users?

All these questions can be addressed with the development of a cyber-secured BYOD infrastructure with cyber forensic preparedness.

6.3 Validation of the NG-DFR model and existing study

Progressive research has been conducted till now in digital forensic area. As the requirement is dynamic and increasing as per the threat landscape, many approach has been developed. But still those are insufficient to complete the analysis and lack of forensic readiness system, as there is a need for a standard and modular[47] approach to digital forensic. There is no stipulatory digital forensic process constructed[110] for handling end to end attack. Therefore, continuous advancement in forensic technology is required as stated in a study by Deloitte[45]. However, some of the existing methods and techniques are listed below.

6.3.1 Honeypot Technology

Honeypot is a deception technology that has been explored to detect threats in BYOD infrastructure in 2016. This technology is very efficient for root cause analysis after an incident [33]. An improved and extended study of a generic digital forensic readiness model

for BYOD using honeypot Technology[33] was again conducted in 2019 where a Threat Intelligence Platform was used to detect the incident, and accuracy has been analyzed [34]. Using audit logs of malicious activities collected from the Threat Intelligence Collector, accuracy has been analyzed and found to be 90.73%, 96.16%, and 93.71%[34]. Subsequently, the cyber risk management process of five preparedness mission areas of FEMA (Federal Emergency Management Agency) was integrated with honeypot [55].

6.3.2 Cryptographic blockchain method of Forensic

For secure authentication of BYOD users into the organization, the cryptographic blockchain authentication process has been used for the record-keeping of forensic investigations evidence [54]. In addition, the cryptographic method of record-keeping systems has been used for the multifactor authentication process [54]. This ledger provides an ease to conduct digital evidence investigation after the crime/malicious activity with the help of image haze removal technique[56], forward mechanism, or reverse mechanism in dual-tree complex wavelet transform (DTCWT) [57]. Advanced intrusion detection systems and distributed ledger technology is used for identifying malicious activity, finding the source of the attack, and storing the digital evidence to conduct a digital investigation [58].

6.3.3 Stride based threat model

Stride [59] based BYOD threat model is proposed to analyze threat landscape. BYOD internal and external threat interaction with the corporate network are analyzed so that security and forensic threats in BYOD can be understood to take a corrective approach towards secured BYOD infrastructure. Reverse adoption of encryption using the Group Encrypted Transport VPN (GETVPN) method is used to detect BYOD traffic and discover malicious activities a minimize threats and vulnerabilities. Therefore, internal and external traffic threats were analyzed for the enhancement of forensic analysis [60].

6.3.4 Smart city IoT Cloud data security Forensic

Data security on the cloud is also a concern for organizations as they do not have enough control over stored data in the cloud. Since cloud data is not stored in enterprise control data centers, data theft is a risk as it can be accessed by unauthorized entities. After an incident, data integrity is an important parameter for forensic analysis. The security threats are

identified in this research [72]. The scope of artificial intelligence affecting BYOD and the threat landscape is also one of the key areas that have been considered in this study.

6.3.5 IoT mobile Forensic

Smartphone and IoT devices were examined to find the logs of the incident for forensic investigation .Extracting the logs from IoT devices and analyzing them with Wireshark for finding out digital evidence was one of the investigation approach [111]. Utilizing smartphone devices for tracing threats and collecting the stored logs from the smartphones, and reconstructing the event of crime[112] for forensic analysis were very useful case studies done in DFRSW (Digital Forensic Research Workshop).

6.3.6 Integration of Digital forensic and Forensic science

The task of collecting digital evidence from a dynamic IoT environment is tedious and complex. The process even becomes more challenging due to the lack of proper tools and techniques [113]. An important study was conducted regarding the integration of different forensic sciences to develop a smart ecosystem [114]. With a collaborative effort of different tools and technologies, a powerful digital forensic ecosystem can be created by integrating cyber laws, policies, forensic experts and security practitioners all together. For instance, various mechanisms have been proposed and implemented to reduce cyberattacks. In some cases it is observed that image processing reduces the computation speed which has been addressed in the nondominated genetic algorithm[115].

As per an IBM study in 2018, 77% of organizations do not have a consistent cybersecurity incident response plan (CSIRP)[116]. even after the General Data Protection Regulatory (GDPR) has been in effect since May 2018[117]. As per the study, it is evaluated that on average it takes 23.6 hours [118] to address cybercrime aftermath. This indicates that there is a serious need for advancement in cybersecurity response systems, cyber defense mechanisms, and cyber forensic mechanisms.

BYOD cyber forensic ecosystem can be a more reliable environment for the organization and it can be adopted with cyber confidence if BYOD cyber forensic mechanism can be developed in a way that the incident can be analyzed to detect the crime with sufficient evidence in optimum duration.

This study has shown a flagrant result of BYOD malicious activity forensic analysis which can be helpful for organizations to implement cyber defense and cyber forensic ecosystem in the BYOD environment.

6.3.7 Wireless Drone Forensic Readiness Model

The wireless forensic readiness model was explored with a dedicated forensic server and drone architecture in the year 2011. To identify the attack, Packet decryption and Wireshark analysis were performed [119], and further digital evidence collection was discussed in the study. After the collection of logs, analysis of wireless LAN traffic using Newitness[110] was explored to conduct a digital forensic investigation.

As discussed above, a different BYOD cyber forensic model has been explored in different verticals, but then also due to the evolution of cyber-attack tools and innovative technologies, there is a significant need for continuous development in this area. This research is a progressive approach to secure the BYOD infrastructure using traffic encryption.

6.4 Cyber Forensic Model-NG-DFR

Next-Generation Digital Forensic Model of Cyber forensic has different segments. This includes the design of the NG-DFR model and implementation which is followed by detailed architecture of NG-DFR. Components of the NG-DFR model are also described in the next section.

6.5 Design and Implementation

This section presents an advanced level of the Next-Generation Digital Forensic Readiness model to secure BYOD environment . This model was proposed to detect cyber-attack, protect infrastructure from threats, and conduct a post-incident forensic investigation process. As honeypot technology for digital forensic readiness (DFR) [33] is not sufficient and large-scale evidence finding, processing technique was required, the deception technology has been used for digital forensic purpose. As the components of digital forensic or cyber forensic investigation include [32] (a) humans, (b) digital evidence, and (c) process, the advanced digital forensic model inclusively needs all these components together. Major components included in this study are represented in Fig. 43.

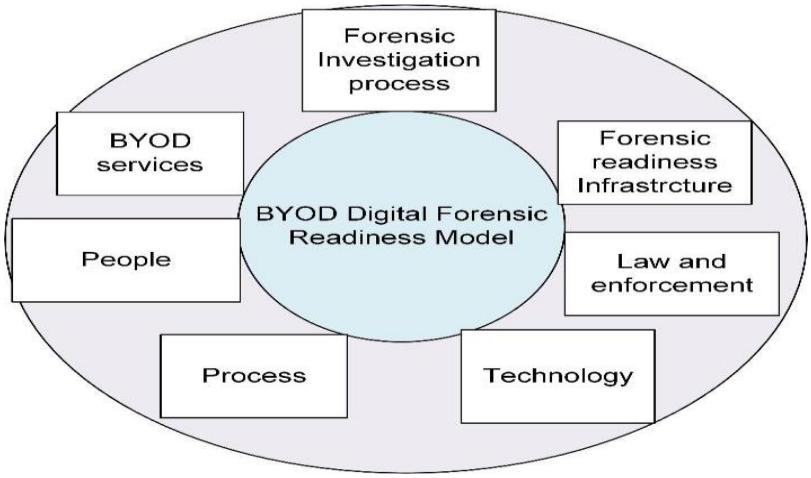

Fig. 43. Digital forensic readiness (DFR) model components.

Components that constitute the DFR model are people, process, technology, digital forensic infrastructure, and law enforcement together.

6.5.1 Detailed DFR model architecture

The architecture for BYOD in this study was done as per standard design. Multiple OEM products are used in the architecture. Initially, the BYOD setup was implemented for normal internet access using the corporate wireless infrastructure.

The same wireless infrastructure is used for corporate wireless and BYOD services. Identity Service engine [25] was used for authentication and Microsoft Active Directory server was used for user directory identity management. Table 31 shows the components used during the research.

Table 31 Components used to set up the BYOD infrastructure

Seq#	Product Name	Make	Model	Usage
1	ISE (Identity Service Engine)	Cisco	SNS-3495-K9	AAA server
2.	Internal Firewall	Cisco	ASA5516-FPWR-K9	DMZ firewall
3	Access point	Cisco	AIR-AP4800-D-K9	Access point

4.	External Firewall	Checkpoint	CPAP-SG4400-NGFW	External Firewall
5.	Anchor Controller	Cisco	AIR-CT5520-K9	BYOD Guest controller
6.	Foreign controller/Mobility controller	Cisco	C9800-40-K9	Master wireless controller
7..	Active directory	Microsoft		For user database
8.	Router	Cisco	ISR 4431	Routing
9.	BYOD devices	Different mobile, laptop	Android/iPhone	Test BYOD devices
10.	Internal network Endpoint	Lenovo	Laptop	For trusted zone device
11	Log management	Checkpoint	CPAP-SM225	For traffic log management

Components used for testing authentication traffic between branch locations and a central location are represented in Table 32, followed by additional forensic/investigation components used during the research for threat hunting and analysis in Table 32.

Table 32: Components for BYOD traffic

Sl. no	Components	Purpose
1.	MPLS connectivity	Traffic flow from Branch to Central location
2.	Internet link	BYOD internet traffic exit.

Table 33: Components used for forensic traffic analysis

Sl. no	Forensic components	Use
1	ISE	For authentication logs
2.	Checkpoint Forensic Blade	For Forensic traffic analysis
3.	Checkpoint Sandblast	For threat hunting
4.	Wireshark	Logs Analysis

6.5.2 Implementation of BYOD architecture

BYOD architecture was established to initiate the traffic from 2 different sources.

The first category of BYOD traffic is mentioned in Table 34.

Table 34: BYOD traffic source/destination

Sl. No	Source	Destination	Description
1	Local BYOD users	Internet	Without MPLS network
2.	Remote branch BYOD traffic	ISE for authentication	Across MPLS network

In this research, we conducted 2 different scenarios of BYOD forensic traffic analysis.

6.5.2.1 Scenario 1: Analysis with Checkpoint sandblast

We have used Check Point SandBlast for threat hunting mechanism, threat emulation, and forensic investigation[120]. SandBlast is deployed using a Check Point management server. The forensic module of Check Point was also used for the forensic investigation to find the source of the attack and logs of malicious activities. Multiple gateways clustering was done to conduct crime analysis for large-scale deployment in correlated viewpoint [33].

Analysis with Check Point SandBlast along with BYOD architecture and overall traffic flow with sandblasting as a forensic analysis mechanism is shown in Fig.44. and the same architecture with the Palo Alto cortex is shown in Fig. 45.

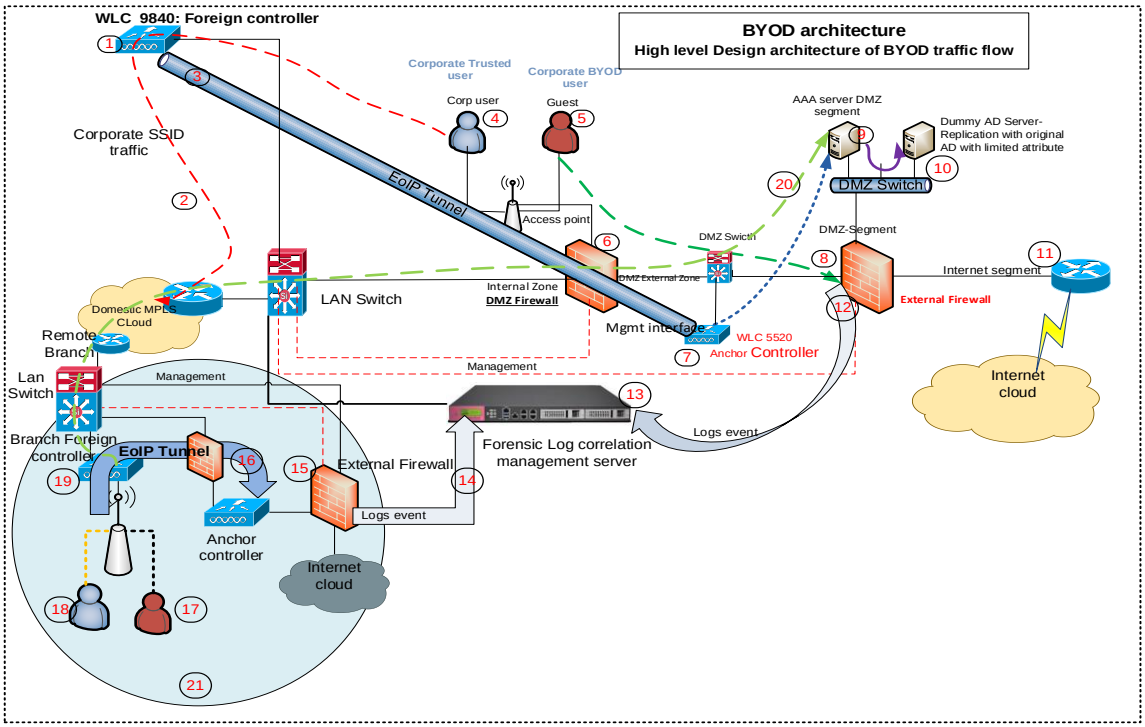

Fig. 44. High-level BYOD traffic flow architecture.

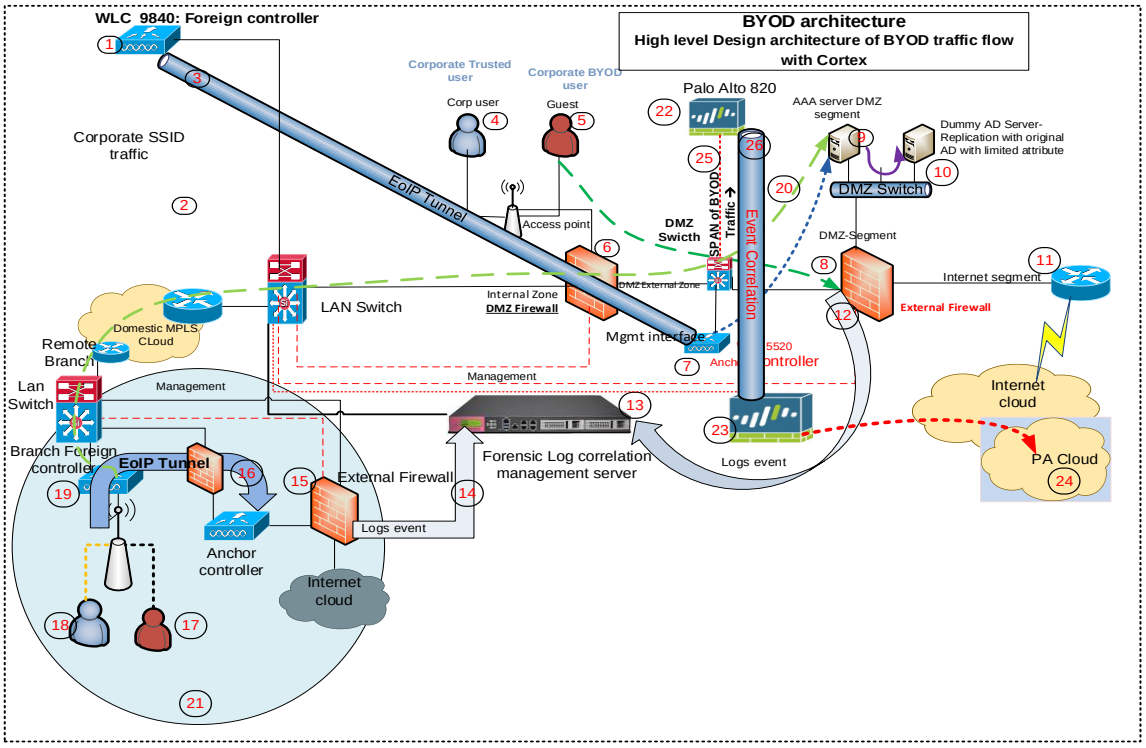

Fig. 45. BYOD architecture with Palo Alto Cortex.

The index used in Fig. 44 for the demonstration is mentioned in Table 35.

Table 35: The index used in Figure 44.

Index	Description
1	Wireless Lan Controller
2.	Authentication traffic from Branch to AAA server
3	Ethernet over IP (EoIP) tunnel between foreign controller to anchor controller
4.	Corporate users (Non-BYOD)
5.	BYOD untrusted users
6.	DMZ segregation Firewall
7.	Anchor controller (Guest controller)
8.	External Firewall

9.	AAA (Authorization, authentication, accounting) server for BYOD Authentication
10.	Active Directory for user identity
11.	External Internet Router
12.	Traffic logs from Gateway to management server for activity logs
13.	Management server (Log management)
14.	Traffic logs from Branch to central management server
15.	Branch external firewall
16.	EoIP tunnel
17.	Branch BYOD users
18.	Branch trusted users
19.	Branch foreign controller
20.	Authentication traffic from Branch to Central site AAA server
21.	Branch/remote location

6.5.2.2 Scenario 2: Analysis with Palo Alto Forensic Cortex and cloud instance for BYOD forensic analysis

In this scenario, we conducted an analysis of BYOD forensic traffic with Palo Alto Cortex. Fig. 43 shows additional components used in the test.

The additional components used in the second scenario are presented in Table 36.

Table 36: The index used in Fig. 45.

Index	**Description**
22	Palo Alto 3020 as Firewall for capturing BYOD traffic
23	PA event log management-M200

24	Palo Alto Cloud cortex
25	The span of BYOD traffic going towards the Internet
26	Event log traffic towards Panorama

In the second scenario of the testing, additional components used for forensic analysis of BYOD traffic are Cortex of Palo Alto network, an AI-based security platform for cyber defense mechanisms, Palo Alto Firewall, Palo Alto 820 and Panorama where Cortex was used for threat prevention, Firewall for capturing BYOD threat traffic, Palo Alto Cloud for threat management and Panaroma for reporting purposes were used.

6.5.3 Authentication mechanism and onboarding process of BYOD users

Secure onboarding mechanisms are used with certificate-based authentication[25]. During the study, for authentication procedures and traffic flow for authentication, ports are allowed on the DMZ firewall.

The ports opened on the DMZ firewall during the study index 6 (Fig. 44 and Fig. 45) for communication purposes of BYOD management traffic are listed in Table 37.

Table 37: DMZ firewall open ports for the testing

Sl. no.	**Firewall**	**Source**	**Destination**	**TCT/UDP Port**
1.	DM firewall	Foreign controller	Anchor controller	EoIP tunnel port
2.	DMZ firewall	Foreign Controller	ISE	1812
3.	DMZ Firewall	BYOD user	DNS	53
4.	DMZ firewall	BYOD user	ISE	8443
5.	DMZ firewall	BYOD	AAA server	8907

6.5.4 Cyber defense ready BYOD infrastructure

The proactive approach of implementing BYOD was developed in this study and followed cautiously so that malicious activities can be detected and protected against cyber threats and risks. Authentication traffic was segregated and encrypted using GETVPN technology to reduce the number of threats over the MPLS[61] network. The private MPLS network was secured using GETVPN which also reduced the initial risk of the infrastructure and protected internal infrastructure at the first stage.

6.5.5 Forensic Readiness BYOD implementation

This study was conducted in two phases, during the first phase of the study, we have used Check Point Sandblast for threat hunting mechanism, threat emulation, and forensic investigation[120]. SandBlast is deployed using a Check Point management server. The forensic module of Check Point was also used for the forensic investigation to find the source of the attack and logs of malicious activity can be recorded. Multiple gateways clustering was done to conduct crime analysis for large-scale deployment in correlated viewpoint [33].

During the second phase of the study, we have used Palo Alto Cortex which is an AI-based security platform for cyber defense mechanisms and Palo Alto Firewall for capturing BYOD threat traffic and analysis as well as Panorama is used for management and reporting purposes.

6.6 Result and Analysis

By implementing BYOD digital forensic infrastructure, we have captured and analyzed the results. The results have been also compared, and significant advancement of cyber defense mechanisms in BYOD forensic has been observed. Implementation of clustering approach shows multiple incidents and malicious activities in the results. The malicious activity was also captured using Wireshark logs, and it was analyzed [99]. The malware was created to test threat detection and capture the malicious activity in the network, for a post-incident forensic investigation and detailed analysis.

6.6.1 Detection of Critical attack in BYOD and Forensic analysis.

6.6.1.1 Critical attack view

Based on the analysis and detection of malicious activity in a BYOD environment, Fig. 46 represents the forensic analysis result of a critical attack. This was captured on the endpoint using Check Point SandBlast tool. The attack was captured as Process ID 9232 , and after recording entry of the malware, the file was renamed and deleted in the BYOD environment.

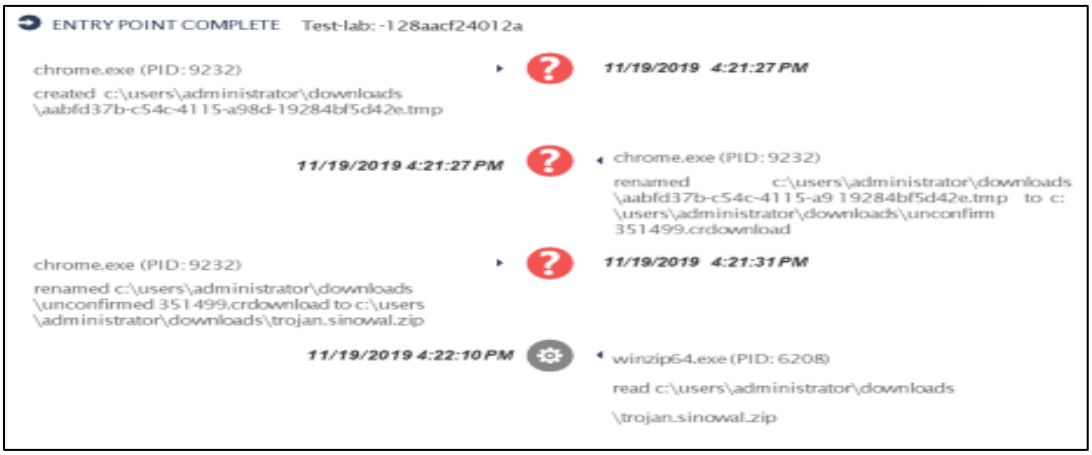

Fig. 46. Critical attacks in the BYOD environment captured.

The malicious activity was performed intentionally, the result was captured. Trojan which tried to damage the critical infrastructure in the BYOD environment was detected.

6.6.1.2 Critical attack View from forensic analysis view of Cortex

Similarly, from Palo Alto Cortex, attack information was captured and analyzed. After the attack in the BYOD infrastructure, an investigation was conducted to complete the analysis as per Fig. 47 below.

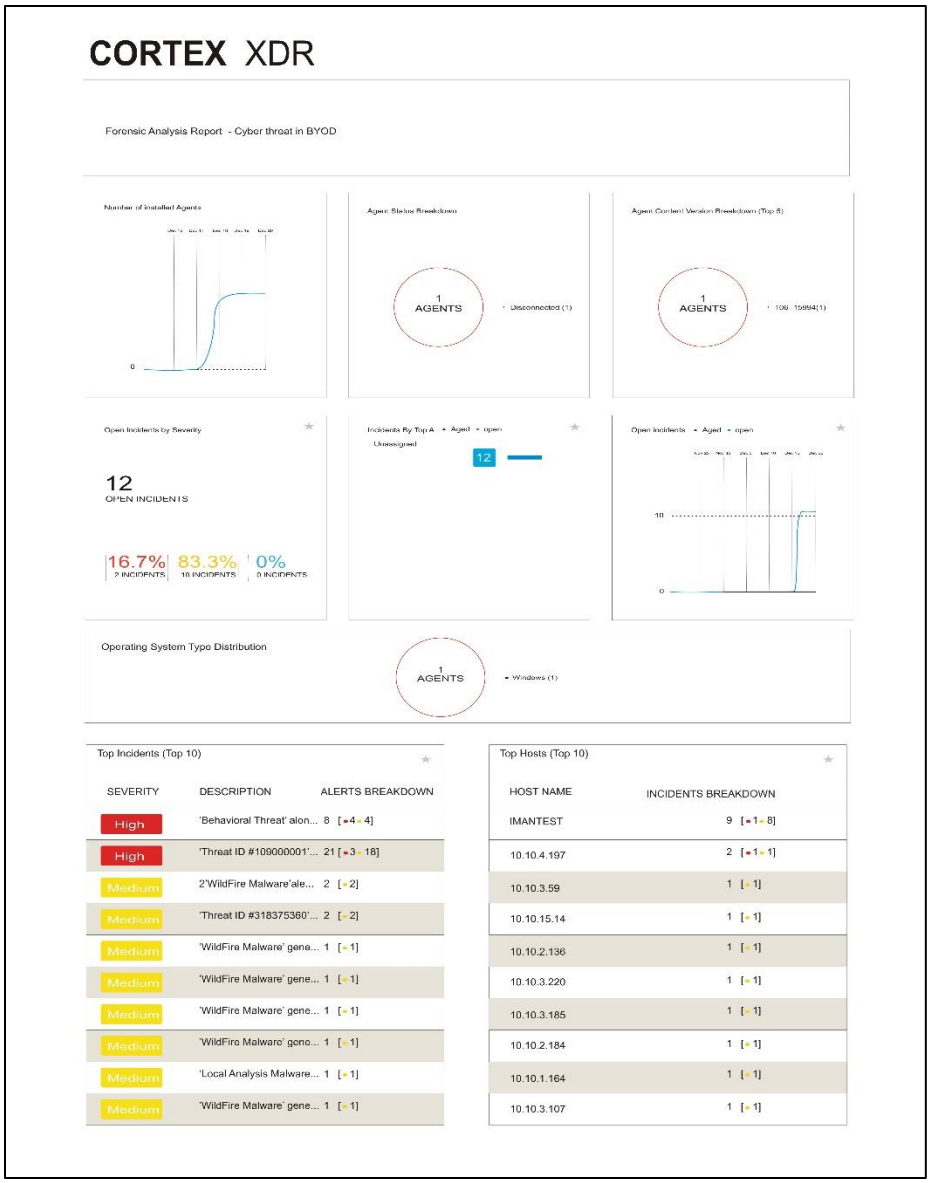

Fig. 47. Malicious traffic captured from external Firewall.

The result from Cortex is reflected in Fig. 47.

6.6.1.3 Critical Attack logs from Cortex

During the investigation, critical attack information was further analyzed with raw logs to track the source of the attack. Source IP address and destination are presented in Table 38.

Table 38: Attack traffic captured from index 23, Fig. 45

Alert Id	TimestampHost	Host IP	User name	Severity	Alert Source	Action	Category	Alert Name
	Description	Initiated By		Initiator CMD		Initiator signature	Initiator signer	Event
Type	CGO name	CGO CMD		CGO signature		CGO signer	CID	Target process name

	Target process CMD	Process execution signature			Process execution signer			Target process SHA256			
	File path	File MD5	File SHA256		Registry data		Registry full key		Local IP	Local port	Remote IP
	Remote port		Remote Host		App-ID	Excluded	Starred	External Id			
32	Dec 21st 2019 10:30:20		172.28.15.14		172.28.15.14				High	PAN	NGFW
	Detected (Raised An Alert)		Spyware Detected via Anti-Spyware profile					Threat ID #109000001			None
(Suspicious DNS Query (vltwox7zl7h1wv.com))							N/A	N/A	Network Event		
	N/A	N/A				N/A	N/A				
		172.28.15.14	39830	4.2.2.2	53			dns	False	False	4662551
14	Dec 18th 2019 14:25:15		INDELTEST		172.28.1.164			imanali	High	XDR	Agent
	Prevented (Blocked)	Malware	Behavioral Threat		Behavioral threat detected				mcpatcher.exe		
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "				N/A		Solimba Aplicaciones S.L.		Process Execution		
		N/A	N/A				N/A	N/A			
									False	False	
	1c1392bc217411eab7a1507b9d62f9c8										
12	Dec 18th 2019 14:25:08		INDELTEST		172.28.1.164			imanali	High	XDR	Agent
	Prevented (Blocked)	Malware	Behavioral Threat		Behavioral threat detected				mcpatcher.exe		
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "				N/A		Solimba Aplicaciones S.L.		Process Execution		
		N/A	N/A				N/A	N/A			
									False	False	
	1789333c217411ea8e44507b9d62f9c8										
9	Dec 18th 2019 14:18:39		INDELTEST		172.28.1.164			imanali	High	XDR	Agent
	Prevented (Blocked)	Malware	Behavioral Threat		Behavioral threat detected				mcpatcher.exe		
	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "				N/A		Solimba Aplicaciones S.L.		Process Execution		
		N/A	N/A				N/A	N/A			
									False	False	
	3007c51e217311ea9fad507b9d62f9c8										
1	Dec 18th 2019 12:46:58		172.28.3.220		172.28.3.220				High	PAN	NGFW
	Detected (Raised An Alert)		Spyware Detected via Anti-Spyware profile					Threat ID #109000001			None
(Suspicious DNS Query (7cfr5a9yjm3p.n9aupi94u3yt.com))							N/A	N/A	Network Event		
	N/A	N/A					N/A	N/A			
		172.28.3.220	58380	4.2.2.2	53			dns	False	False	
	3401539										

The attack was detected from the devices of IP addresses 172.28.15.14, 172.28.3.220, and 172.28.1.164, which were assigned to the BYOD devices as internal IP addresses. During the investigation process, we detected and traced user information and malicious activities performed by the users. Sensitive and robust analysis was done so that manual conventional results can be compared with the simulated analytical result in a study of pressure relief[121].

This traffic was captured from the architecture of Fig. 45 and index 23. The malicious traffic observed in Cortex and the cyber defense system was built to prevent those attacks as well, which is shown in Table 34.

6.6.2 Forensic analysis from BYOD Endpoint

After analysis of malicious activities from the gateway level, the next level investigation was conducted from the endpoint after identifying the attack source from sandblasting. Threat emulation shows the absolute result of malicious activities by endpoint BYOD devices as illustrated in Figure below.

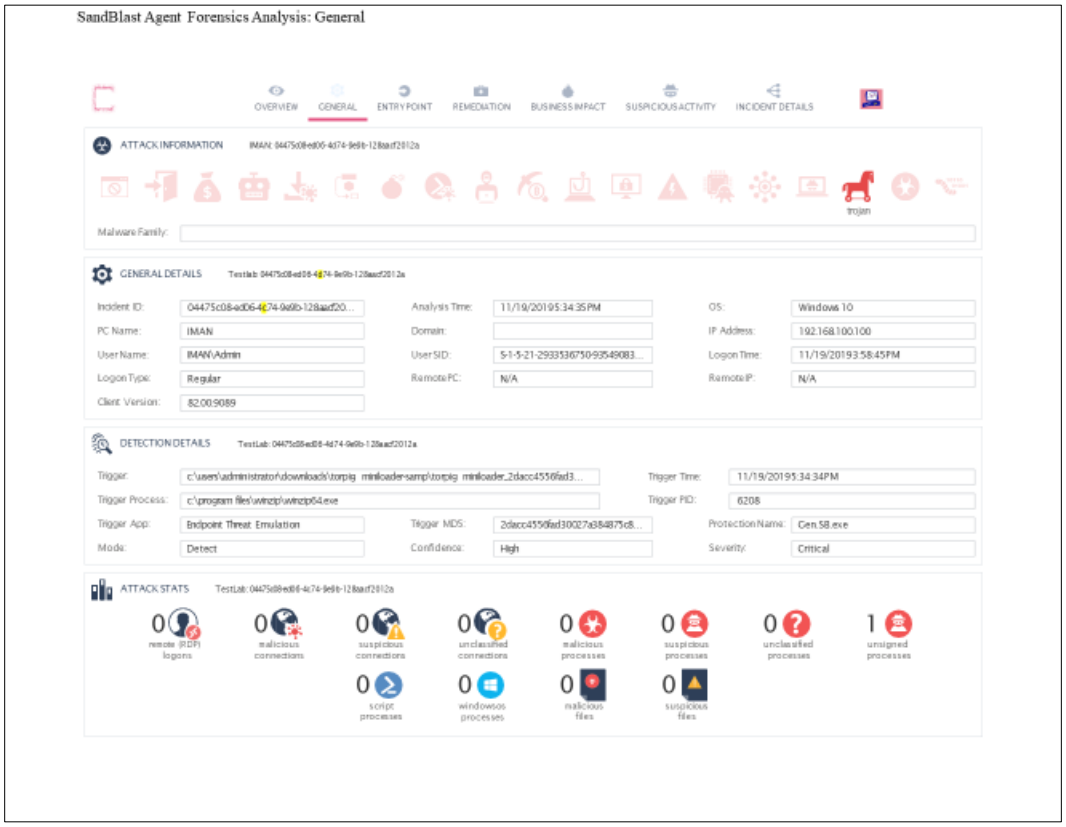

Fig. 48. Malicious activity analysis from BYOD endpoint using SandBlast Agent.

The result shows that malicious activity was detected during the pre-authentication of the BYOD users, with a pre-authentication segment IP address (192.168.1.x). One of the phishing attack packets was also captured after an attack, and the details of the attack are represented in Figure below.

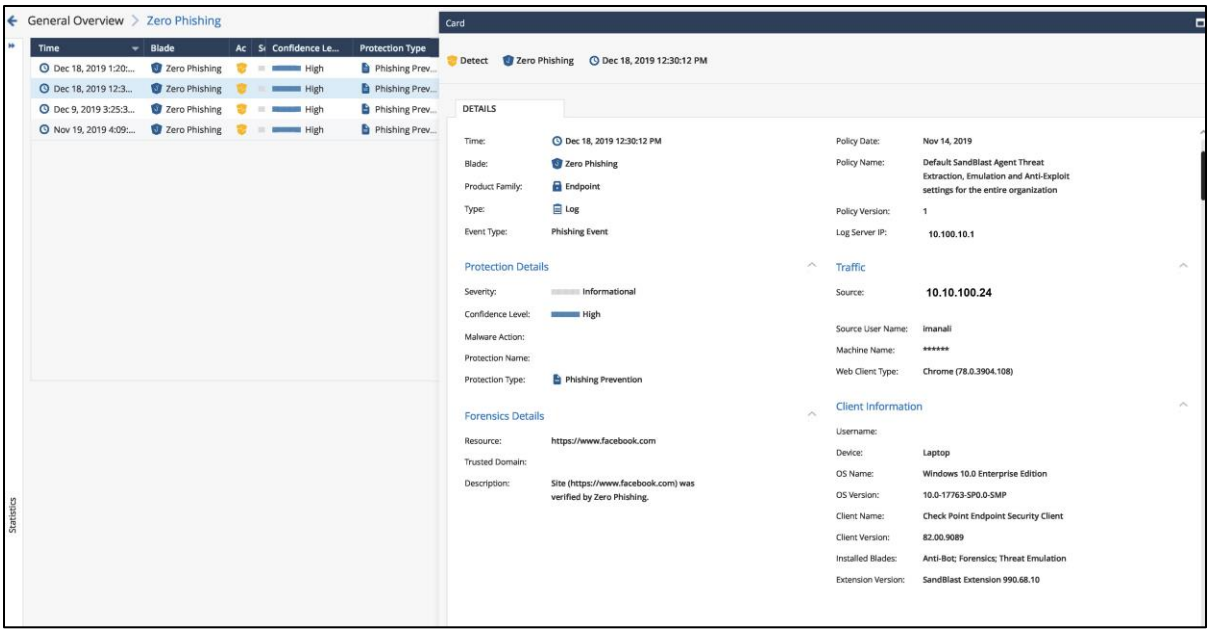

Fig. 49. Phishing attack analysis packet captured.

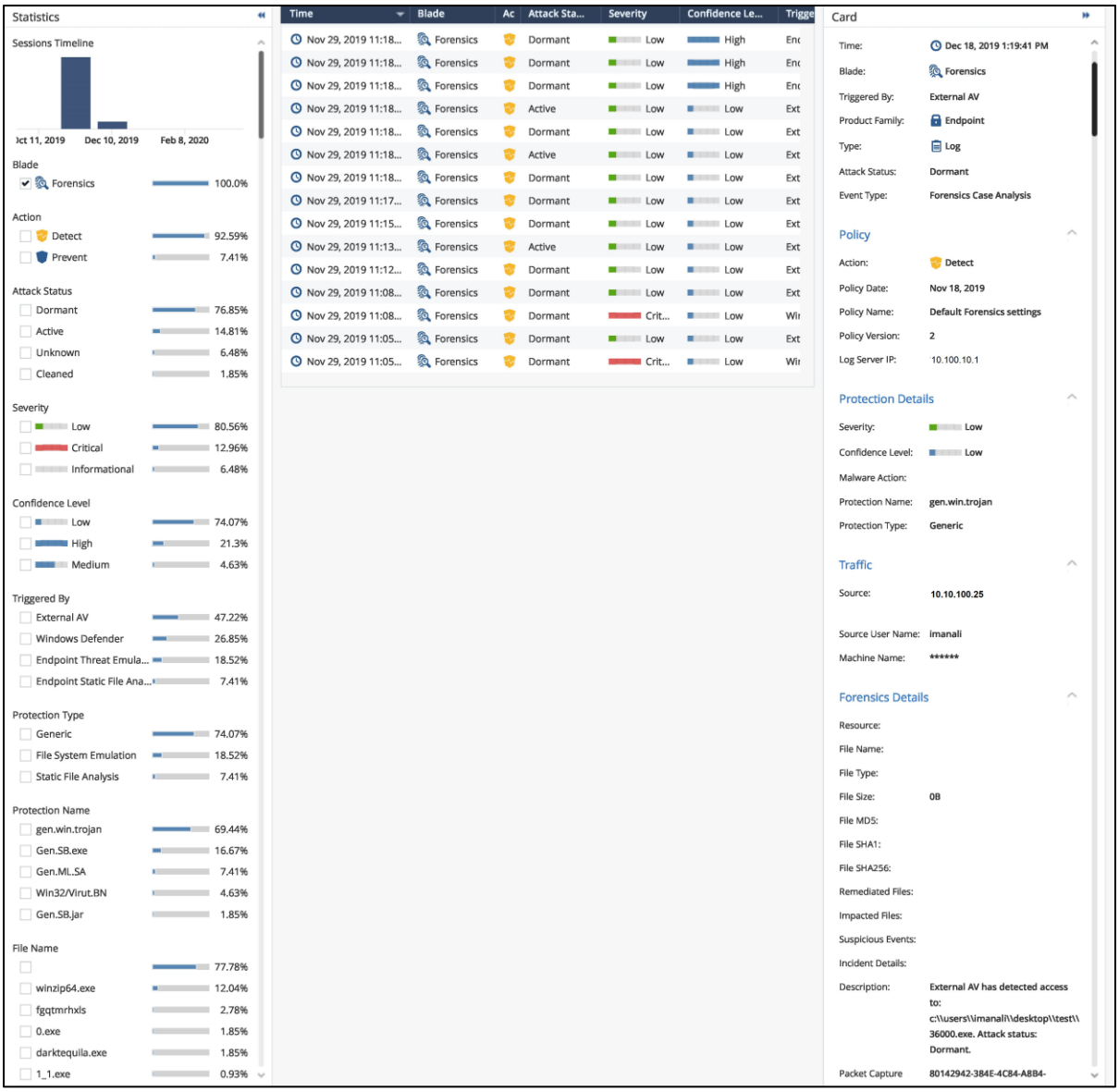

Fig. 50. The detailed cyber threat landscape in the BYOD environment.

This packet has the source IP address 172.28.1.164, the attack type was a phishing attack, and also user identity was traced from the Cisco Identity Service Engine during the test as per Fig. 44, index 9. This result was captured after detection of the endpoint performing reverse analysis from SandBlast from gateway level. Logs were captured for forensic analysis case event type from BYOD gateway as per Table 39.

Table 39: Forensic case analysis after attack

Nov 22, 2019 8:21:57 AM Testuser Anti-Bot; Forensics; Threat Emulation Log 2019-11-22T08:35:47Z
Forensics Case Analysis 2019-11-22T13:51:57Z 2019-11-18T14:19:55Z Detect a4640108-ce8b-af06-5dd7-9aa500050000 1 Active 1 ep-demo 0 @A@@B@1574380800@C@52 Gen.SB.exe 46133eec-f86a-480f-a2dc-7483e2c20adf 1.57441E+12 High Endpoint Threat Emulation has detected access to: c:\\users\\Testuser\\desktop\\340s.exe. Attack status: Active. Laptop TestDevice 2 Endpoint Threat Emulation 82.00.9089 Check Point Endpoint Security Client 0 Critical Endpoint Forensics ip-172-28-1-164.ec2.internal (172.28.1.164) 10.0-17763-SP0.0-SMP Default Forensics settings File System Emulation 0 (10.128.140.176) 164.100.1.8 true S-1-5-21-2933536750-935490830-805106884-1003 Generic", "Trojan", Windows 10.0 Enterprise Edition

The logs of this attack were captured after an incident, and we analyzed the threat. The attack ID is a4640108-ce8b-af06-5dd7-9aa500050000. Traffic from 172.28.1.164 was an attack, and traffic was decrypted at the gateway level. Besides, as seen in the result, the system was “Windows 10.0 Enterprise Edition” and the “Gen.SB.exe” was detected in the system which accessed c:\\users\\Testuser\\desktop\\340s.exe. Finally, Trojan was detected. The mentioned threat landscape detail was captured.

This was an artifact after BYOD threat analysis with different risk, attack, and forensic information.

6.6.3 BYOD environment Cyberattack category Analysis

During the research, the different types of attacks in the BYOD environment were reviewed and categorized by risk and criticality of the threat. The attack categorization framework was analyzed. Different attack event was framed.

We have captured a total of 966 packets from Check Point for analysis with different risk severity. The traffic analysis result is categorized based on risk and severity are shown in Figure below.

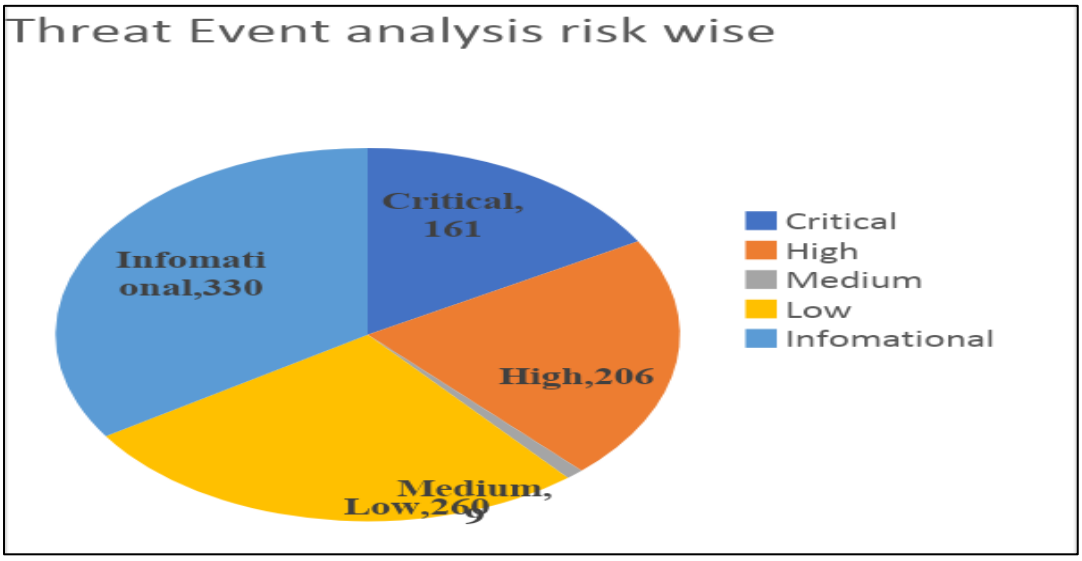

Fig. 51. Risk-wise traffic analysis out of 966 packets.

The attack categorization framework was captured as per MITRE ATT&CK as shown in Fig. 52 below.

Fig. 52. Attack framework as per MITRE ATT&CK.

6.7 Constraints and Challenges of Existing Technology

After conducting the research, comparison and analysis were done on the test results. Results and outcomes were compared with the existing traditional model of the threat detection process available. While existing methods and techniques are quite effective in detecting known threats and protecting the environment , the DNS layer security mechanism was observed to be inadequate and ineffective. As per research conducted by Cisco, 91% of the malware attacks are in the DNS Layer[122] while the majority of the organizations do not have a mechanism implemented for detection and protection over DNS attacks. Available solutions of sandboxing are effective, against unknown threat portfolios, but since the threat landscape is expanding with new behavior and methods being adopted, even an effective solution is not mitigating the advanced threats. For better understanding, a graphical representation is used in Fig. 53 to highlight available solutions and their limitations

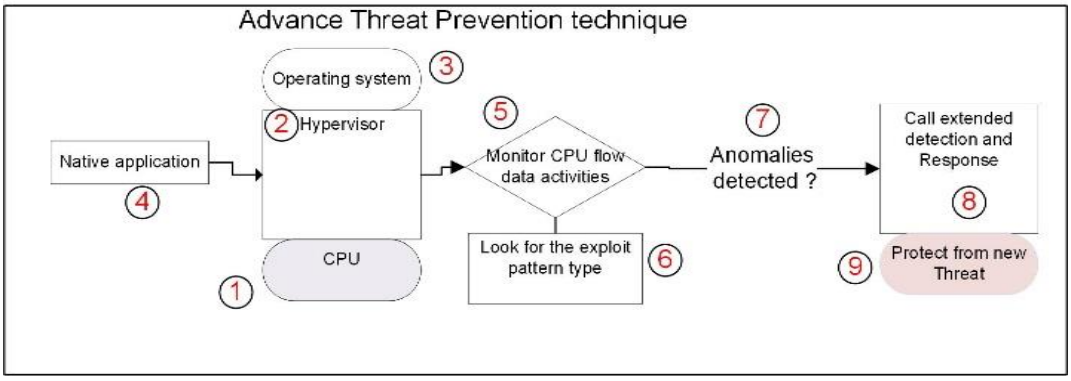

Fig. 53. The proposed new approach of the threat detection model.

Fig. 53. Shows the limitations to the mitigation of a new zero-day malware attack.

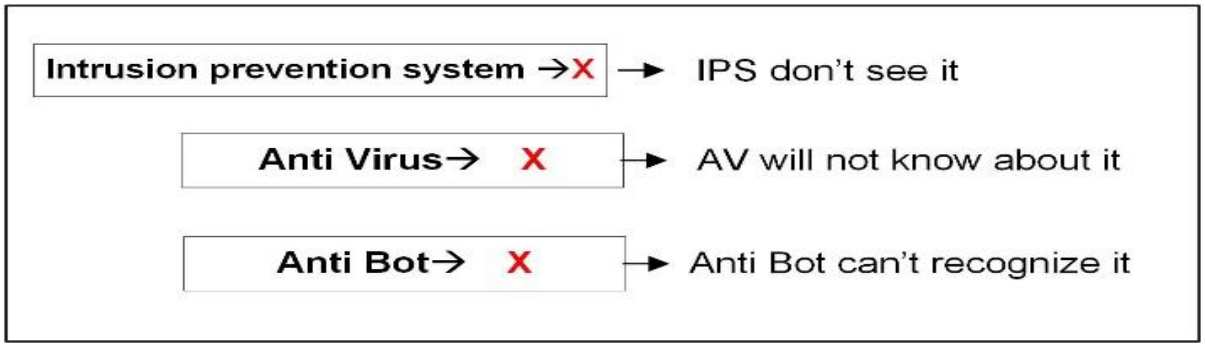

Fig. 54. Existing technology and limitations to handle the attack.

An attack cannot be detected if it is brand new or zero-day in nature, which might disrupt the business and system as threat behavior is not known. In order to eliminate this situation, an advanced level of detection and protection mechanism is an upcoming requirement.

This research has a potential mechanism to detect attacks targeting system memory or CPU level attacks. As shown in Table 40, a system-level attack that executes commands at the application process level was observed.

Table 40: A system-level attack that executes commands at the process level

Dec 18th 2019 14:25:08	Testuser	172.131.1.164	imanali	High	XDR	Agent
Prevented (Blocked)	Malware	Behavioral Threat		Behavioral		threat
detected	mcpatcher.exe	"""C:\Users\imanali\Downloads\mcpatcher.exe"" "				N/A
Solimba Aplicaciones S.L.	Process Execution					

This was a zero-day attack that has not been identified by AntiVirus, AntiBot, or IPS as this was a newly created malicious code that attacked the BYOD environment. Even sandboxing mechanisms failed to quarantine or to block it.The architecture of the advanced threat detection model proposed in this research is shown in Fig. 53.

The proposed model is shown in the sequential manner. In sequence 1, the CPU starts processing, and the hypervisor is running in sequence 2 along with OS in sequence 3. After the setup of the minimum requirement, the application is accessed through any native application. Monitoring of CPU activities is in sequence 5 which is a key focused area in this process. If any malicious activities are observed in sequence 6 as an alarming

mechanism, anomalies detection and protection mechanism is called in sequences 7 and 8. Sequence 9 protects the system before an attack takes place so that the BYOD environment cannot be exploited.

6.8 Proposed System Performance

Proposed system performance is measured by doing a comparison with existing methods and techniques. How proposed method is benefiting along with advantages of the new technique is mentioned in table below.

Table 41: Comparison of the existing solution and new simulated solution

Threat Type	**IPS (Intrusion Prevention System)**	**Anti-bot**	**Anti Virus**	**New proposed model**
Known Threat	Yes	Yes	Yes	NA
Unknown threat detection	No, Until sandboxing and more time consuming	No, Until The sandboxing process is more time consuming	No, protection mechanism time is higher	Yes, Protect before attack

The proposed mechanism is a comprehensive technique in protecting the organization before a potential attack as it analyze the behavior of the malicious activities from the CPU level in the BYOD environment. As a final outcome , the new approach of the NG-DFR model is mentioned below.

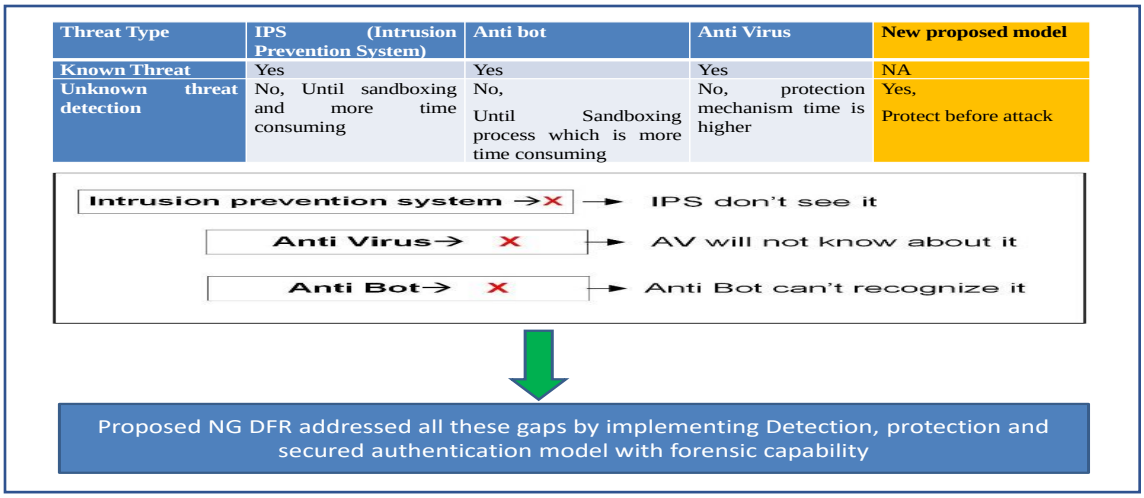

Fig. 55. The architectural flow for the new approach of the NG-DFR model.

6.9 PROPOSED CYBER FORENSIC NG-DFR Model

After the analysis of the results, the concept of the advanced level of the cyber forensic model is formalized. Next-Generation Digital Forensic (NG-DFR) model is proposed for investigation preparedness of secured BYOD detect and protect model. This model is proposed with 5 major stages where 1st is BYOD process definition, then BYOD technology enablement, threat hunting mechanism as the 3rd stage, thereafter protection mechanism as the 4th , and at last forensic process, law and enforcement as the 5th stage. All these 5 stages of collaboration approaches in the cyber forensic environment are presented to build a cyber forensic ecosystem and proving the concept of the next-generation DFR model.

6.9.1 BYOD Cyber Forensic Process definition

The primary task towards building a forensic ecosystem is defining the process layout of the BYOD environment. The framework for cyber secured BYOD policy is required where untrusted BYOD devices are provisioned for accessing an organization's critical network and resources. In this phase, the security policy is defined as per the organization's requirements and feasibility. A defined policy of detection mechanism in a BYOD environment can constitute multiple technologies, processes, and practices. In this phase, the attack detection mechanism is framed and defined for collaboration with other components of the BYOD model. After the detection policy, violations and acceptance policy are defined, the incident handling mechanism and security operation center

mechanism are defined with the integration of multiple products and the technology framework. At last, the complete security posture framework is laid down in this phase as shown in Fig. 39.

6.9.2 BYOD Technology enablement

BYOD technology enablement is an important key area in this proposed concept of NG-DFR. The association of different products and technologies enabled the complete service. While choosing products and technology of the BYOD design, the most important factor to consider is compatibility between different products and technologies to work together within a defined framework. If advanced level networking and security products and technology are placed but if these technologies don't work together as a single machine to leverage capabilities of all the components in the environment, then threat intelligence in NG-DFR will be a challenge.

Accordingly, in this phase, major services, products, and technology are factored to work in an integrated and enabled way so that each and every threat can be traced without any packet passing uninspected. As shown in Fig. 41, integration was done along with Cortex . Apart from this in Fig. 40, integration of next-generation endpoint protection is also introduced for the threat hunting process to enable critical infrastructure. In this section, actual threat detection technology is integrated with the authentication model of BYOD users. After secure authentication and onboarding [25], detection of malicious traffic mechanisms is proposed [123]. Log management and sandboxing for traffic analysis are considered in this phase.

6.9.3 Threat Hunting Framework

The most important part for the forensic investigation ecosystem to develop is the threat hunting mechanism. Monitoring is a continuous action to collect activity logs for potential threat detection in a cyber forensic system. After an attack, finding the source of the attack is a critical task[13]. Detection of malicious [88] traffic which is indeed a major dependent technique required in cyber forensic mechanism which was introduced in this phase. Primarily in this section, log analysis is conducted in order to track suspicious traffic. Once the threat is detected in this phase, the threat verdict and score are checked to determine whether it is malicious or not. If it is found to be a malicious and known pattern, then the

protection [123]module is called. If the threat pattern is unknown by the threat defender, for example, a zero-day attack[124], then, after extraction of hash, it is sent to threat cloud for verdict and score of the threat and retrospective event is triggered[125]. Finally, logs are preserved for further investigation. In this section, endpoint traffic logs are captured in the external gateway as shown in Fig. 42 index 8 and Fig. 43 index 23 so that later on logs can be investigated further. Apart from this, all traffic including source IP, destination IP, user information, and user MAC address is captured with all activity details.

6.9.4 Threat Protection Mechanism

Protection from threats is the foremost task before an attack on the organization. Consistently, researchers are focusing on developing new tactics for threat protection. Different types of novel approaches have been developed in threat protection. One of the advanced level protection mechanisms was developed in BYOD cyber forensic ecosystem study[123]. In this phase, the concept of protection of critical infrastructure is covered. After getting the threat category, traffic dropped and logs are preserved for analysis as shown in Fig. 42 index 13, and results are shown in Fig. 47.

6.9.5 Forensic investigation, Law and Enforcement module

In this phase, a forensic paradigm is presented. To complete the forensics of the attack, a few key areas need to be focused on such as analysis of the logs, preservation of the traffic, and stored log. After analysis, presentation and documentation need to be done. Preserving evidence and log correlation is focused on the integration of different technologies and products as shown in Fig. 42 and Fig. 43, where all the gateway perimeter security devices along with AAA, controller, and BYOD users are integrated with the Active Directory user database. After integration, an end-to-end logs analysis mechanism is developed to enable the forensic system. Finally, forensic correlation of related facts and findings are documented and presented.

6.10 NEXT-GEN DFR MODEL ECOSYSTEM

In this phase, the final framework is represented by the next-generation digital forensic readiness (NG-DFR) model. Step by step sequential process is explained to complete the cyber forensic ecosystem. The complete ecosystem comprises processes, policies, humans, technology, and integration. Integration of process and technology with human interaction

area is covered to build cyber forensic BYOD environment. As shown in Figure below complete steps are proposed for the next-generation DFR model.

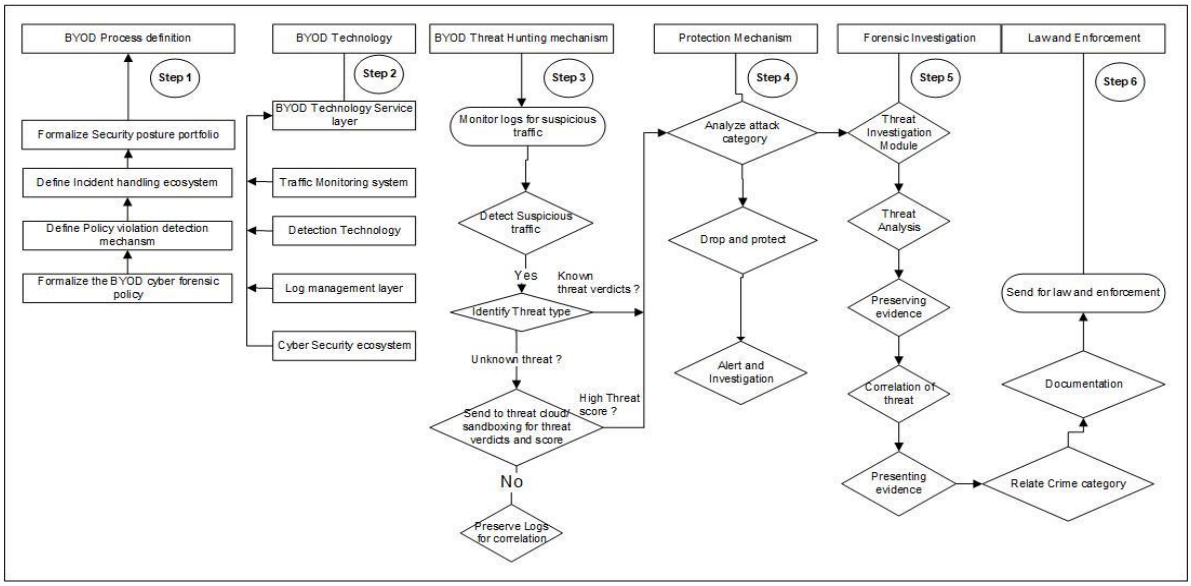

Fig. 56. Next-generation digital forensic framework.

In Step 1 of the NG-DFR model in Fig. 56 above planning, policy frameworks are defined with related security and technology enablement paradigm. Service enablement policy, security policy, and detection policies alert mechanism are defined. The integration process is defined.

In Step 2 Service enablement area is focused on. In particular, building secured BYOD infrastructure with all required products and technology is a key component of this phase.

In Step 3 specially, a detection mechanism is proposed. Detection of various threats and then categorization of the threats are sequential events. Malicious traffic and known threats are detected, and unknown threats are filtered. Unknown threats are sent to the threat cloud in this phase to be analyzed and get the threat score so that appropriate action can be taken.

In Step 4, the protection of critical infrastructure is focused on. Protection from different threats before exploiting up to the best possible options is taken care of so that the threat landscape can be reduced.

In Steps 5 and 6, the focus area of NG-DFR that is a thorough investigation of the threat is covered. In this phase, the outcome of the integration of all tools, techniques, products, and technology is leveraged to build a cyber forensic ecosystem. After analysis from preserved

logs, the threat hunting mechanism is enabled to carry out the investigation. Finally, storing the logs and artifacts and preparing documentation for submission to law and enforcement are covered.

In a nutshell, this proposed approach of the NG-DFR model covered an end-to-end system to complete the forensic investigation in order to build an advanced level of the cyber forensic ecosystem.

Algorithm 3: Detailed algorithm of NG-DFR model.

```
Step 1: Start
Step 2: Define BYOD security process and policies variables
        P1=Security policies
        P2=Detection Polices
        P3=Incident Response
        P4=Security violation Protection policy
        P5=Forensic call policy

Step 3: Technology variables and users
        T1=Technology portfolio
        T2=Monitoring system
        T3=Detection System/Decoy system
        T4=Protection technology
        T5=Log management
        T6=Forensic technology ecosystem
        T7=Threat category
        U1=BYOD users
Step 4: action and category variables
        violation=V
        Risk acceptable level=A
        Protection=P
        Forensic=F

Step 4: Monitoring of threat
        push  U1 through T3 and compare  P1
        If Result=A
                then accept request
                stop
        else
                call Step 5
        Then process U1 in T4 for P2
                send  U1 logs to T5
        else
                call step 5
Step 5: Detection and Protection
        Push U1 through T3 for P4
```

```
                    if Result=V
                    Drop traffic

          Else
                    call step 7
Step 7: identify threat
          If threat category is known
                    if verdict/score =A
                              pass the traffic
                    else
                              drop and send Call step 10 for forensic
          else
                              call step 8 for T7 Sandboxing for threat verdicts to
                              call step 9
          else
                    call step Sandboxing for threat verdicts

step 8: Analyze threat category
                    Analysis of threat type with threat Hash
                    return T7=verdict and score of  threat category
Step 9: Unknown threat for forensic
                    If T7==A compare to P5
                              pass and send T5
                    else
                              send for forensic T6
Step 10: Forensic ecosystem
                    if P5=Investigate attack
                              do analysis
                    Present
Step 9: Present to Law and enforcement
Step 11: Stop
```

An algorithmic approach for the NG-DFR model is proposed post analysis.

6.11 Research Outcomes: Advantages of Detection and Protection Mechanism

There are two major novel contributions from this research. The first research contribution is a unique attack detection mechanism. This unique attack detection mechanism helps to detect and protect against zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AV, and AntiBot. The second key contribution is to build a cyber defense BYOD ecosystem. This research has contributed to the area of cyber forensic analysis of a BYOD environment. The complexity of forensic analysis of the malicious activity in a BYOD environment was organized to simplify and implement easily. The different approaches to

forensic investigation are compared using different tools and techniques. Finding the source of an attack in BYOD is analyzed from internal and external threats. The threat prevention mechanism and the end-to-end BYOD cyber forensic ecosystem framework are also defined in this research.

6.12 Discussion

With BYOD, being external devices connected in the infrastructure, it turns out sensitive and critical in nature to control threats and post-incident analysis of the attack, and detecting the source of the attack. According to Check Point technology research, 99% of organizations[126] do not have a protection mechanism to fight against ongoing cyber-attack threats. The proposed approach of NG-DFR has addressed the need for an end-to-end cyber forensic ecosystem.

After an attack, during the investigation process in BYOD, we analyzed all different categories of attack and behavioral analysis of crime. As it was also an important target to protect the infrastructure, detection and prevention. Prevention technologies were needed after detection by the system without manual intervention. The STRIDE-based threat model, which is an interaction between the threat and the corporate network, can be integrated with this model to get a better result.

End-to-end visibility, analysis, investigation, and integration between tools and technologies for building up an advanced model of cyber defense system were needed to fight against today's advanced cyber threat landscape. During the research, an advanced level of the cyber forensic model was developed.

Moreover, one important aspect was analyzed during the research, which is run time detection of attack endpoint, the status of connection and blocking, and preventing the endpoint from the infrastructure. Detection of threat, visibility of threat associated risk, incident response, and post-incident forensic model are key areas explored in this research.

6.13 Summary

Attacks on the critical infrastructure of the organizations increased, caused by the lack of a cyber defense ecosystem in the BYOD environment and therefore business ecosystem gets fragmented. Cyber secured BYOD infrastructure is one of the crucial requirements for organizations nowadays to protect from the advanced level of threats.

This study includes a framework of the cyber forensic model along with a cyber-secure BYOD model. In the first phase of this research, the detection technique of threat is explored with various tools and techniques for further research and analysis.

In the second phase of this research, a major finding is a novel approach of detection and protection mechanism of zero-day attacks which is hardly possible to detect by traditional tools like IPS, IDS, AntiBot, and AntiVirus. The aforesaid method of detection and protection model contributed to the protection of the organization's critical infrastructure. A significant advanced incremental positive result derived by the comparison of the outcomes and adoption of this method was found helpful to build the whole cyber forensic ecosystem.

In any cyber forensic investigation post-incident threat hunting is a critical task that is addressed in this research using different tools and techniques like sandblasting and Cortex. At last, an advanced level of cyber forensic readiness BYOD infrastructure is developed. To mitigate the ongoing need for conducting end-to-end digital forensic investigation Next-generation digital forensic readiness (NG-DFR) model is proposed including the detection and protection framework, the BYOD policy framework and service enablement technology area.

Chapter 7: Conclusions and Future Work

7.1 Conclusion

All the findings, conclusion from different analysis and simulation performed during this research are sequentially mentioned below

7.1.1 Secure onboarding of BYOD

The foundation of this thesis explains the secured onboarding process of BYOD devices and reduces risk in BYOD infrastructure. Cyber secured BYOD infrastructure is one of the major requirements for organizations today to protect from the advanced level of threats. In order to build a cyber secured BYOD infrastructure, a secured BYOD onboarding process is required. This research contributes a secured framework of the BYOD implementation in a centralized and distributed model. A novel approach of secure BYOD model is developed while following all organizations' security policy and practices. In this approach critical infrastructure can be protected while providing internet access to BYOD users by using same infrastructure. Apart from this, a novel approach was simulated where reverse encryption technique is used to reduce cyber attacks in BYOD environment and protect corporate infrastructure.

7.1.2 Detection and protection of malicious traffic

While developing and implementing a secure working environment with BYOD, it's important to focus on threat areas and open loopholes to minimize the risk of cyberattacks. To minimize the risk included with BYOD in the corporate networks, malicious activity, and threat detection technique is an important research area. Continuous advancement is required in this area of research as cyber threats and risks are also increasing over the time. For secure onboarding of the BYOD users, a certificate-based mechanism has been considered as the most secure method. In this research, we have identified and explained the loophole in a secure certificate-based authentication mechanism and also developed a novel approach to mitigate risk included with the identified loophole. In an industrial practice of BYOD services attackers target to enter in the network for conducting cyberattack and damage the critical infrastructure. In order to build a secure BYOD cyber

forensic ecosystem- an advance level of detection and protection mechanism is required to reduce cyber attacks. Detection algorithm is designed which can detect malicious activities and unauthorized access to critical infrastructure. In the next step after detection, an advanced level of Protection mechanism is designed to resolve the major concern of collecting the logs, digital evidence for further analysis and threat hunting to trace the source of the attack for forensic analysis. Finally, the "PROTECT" protocol is proposed to adopt while implementing BYOD infrastructure. Along with this, an advanced level log analysis mechanism is also proposed.

Major conclusion from this research is detection and protection mechanism of zero-day attacks which cannot be detected by traditional tools like IPS, IDS, AntiBot, and AntiVirus. The proposed method of detection and protection model contributed to protect organization's critical infrastructure from unknown threats or zero-day attacks. Simulation and analysis concluded that the methods and techniques explored in this study can help in secure adoption of BYOD services in the corporate environment so that cyber secured BYOD ecosystem can be created.

7.1.3 Next Generation Digital Forensic Readiness Model

The third objective of the research was, finding the evidence of the crime. Threat hunting is primary requirement post-incident so that cyber forensic investigation can be addressed in timely manner with various tools and techniques. The important steps are tracing source of the attack, analyze, preserving the evidences and then present that as per the requirement. DFR system in BYOD infrastructure is a mandate in the industry today to complete the digital forensic investigation, therefore designing a Digital Forensic Readiness model in BYOD infrastructure post cyber attack is an important objective to achieve. Finally, an advanced level of cyber forensic readiness BYOD infrastructure is developed to mitigate the ongoing need for conducting end-to-end digital forensic investigation. Study also concluded the policy framework which showcases the secure adoption of BYOD services in the industry.

7.2 Summary

Step by step practical work was conducted to get the result of the objectives defined for this research. For the 1st objective of implementing a secured model of BYOD environment, this research was conducted with original equipment and demonstrated in the lab to simulate the result. All the hardware including controller, AP, Firewall, etc used in the lab environment to test results. Post simulation BYOD services, anomalies identified of the secured certificate-based model and finally logs detected on the external device. Finally, architectural model developed to provide secure access and related algorithm developed. Post detection protection architecture and algorithm developed to protect critical infrastructure. Finally summarization of the overall conducted research work outcome is mentioned in Figure below.

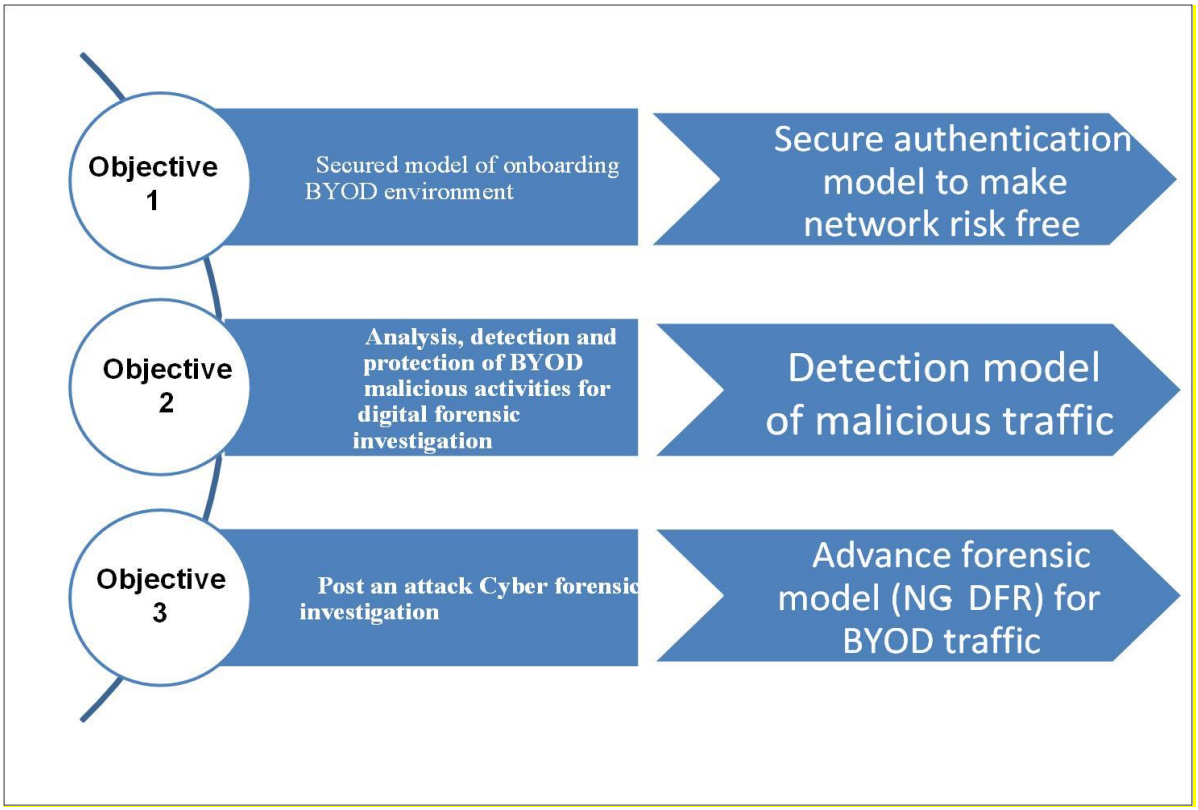

Fig. 57. Overall summary of conducted work in the research and outcome.

7.3 Limitation of the proposed system

This proposed schemed is focused more into BYOD environment in a private data center and very less focus on cloud environment. As current trend in moving towards cloud based structure which invites additional threats, so additional attention is required. Also, extended objective on cloud enable BYOD environment for cyber forensic ecosystem is the limitation in this study.

7.4 Future work

This research has opened up many doors for future research. Future research in this direction will be more into traffic analysis of cloud environments where BYOD infrastructure is hosted. The development of the Cyber-secured cloud ecosystem is one of the open areas for further research.

Digital forensic investigation is a complex task due to the deficiency of standard protocols depending upon the categories of digital crime. The nature of crime becomes complex day by day due to the advancement of crime tools and techniques. BYOD implementation is a fast-growing area, criminals are using innovative methods, tools, and technologies to conduct crimes in zero-day attack nature. Also, an important zone of future research is the collaboration of cyber tools, technology, and cyber law with additional collaboration with multiple countries. The ultimate way forward of the “One team with one common goal” approach of cyber defense system is the only successful model[127] which is further research open area like PPP model of the cyber defense system.

References

[1] FTMS College, O. U. Franklin, M. Ismail Z., and FTMS College, “THE FUTURE OF BYOD IN ORGANIZATIONS AND HIGHER INSTITUTION OF LEARNING,” International Journal of Information Systems and Engineering, vol. 3, no. 1, pp. 110–128, Apr. 2015, doi: 10.24924/ijise/2015.11/v3.iss1/110.128.

[2] H. Shetty, L. Unden-Farboud, and P. Arriandiaga, “Competitive Landscape: Managed Mobility Services,” p. 20.

[3] “94% enterprises will use IoT by end 2021: Microsoft report,” https://www.livemint.com.https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-1565165449842.html (accessed Aug. 08, 2019).

[4] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, “Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments,” Journal of Information Privacy and Security, vol. 11, no. 1, pp. 38–54, Jan. 2015, doi: 10.1080/15536548.2015.1010985.

[5] N. Singh, “B.Y.O.D. Genie Is Out Of the Bottle – ‘Devil Or Angel,’” Journal of Business Management, vol. 1, no. 2319, p. 12, 2012.

[6] “IT Consumerization - A Theory and Practice Review. | PUMA.” https://puma.ub.uni-stuttgart.de/bibtex/102385360787b0d8cb54b3a0fd7c976a8 (accessed Apr. 30, 2022).

[7] T. Noda, “Solving BYOD issues a must says HP,” Philstar.com. https://www.philstar.com/business/2013/03/16/920437/solving-byod-issues-must-says-hp (accessed Apr. 30, 2022).

[8] “COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013,” p. 320.

[9] “PwC’s Global Crisis Survey 2019,” p. 22.

[10] “Consumer Loss Barometer 2019_KPMG International,” p. 32, 2019.

[11] Z. Mitrovic, I. Veljkovic, G. Whyte, and K. Thompson, “Introducing BYOD in an organisation: the risk and customer services viewpoints,” p. 26, 2014.

[12] “Cyber security - a necessary pillar of smart cities,” Smart City, p. 24.

[13] G. Suciu, A. Scheianu, I. Petre, L. Chiva, and C. S. Bosoc, “Cybersecurity Threats Analysis for Airports,” in New Knowledge in Information Systems and Technologies, vol. 931, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham: Springer International Publishing, 2019, pp. 252–262. doi: 10.1007/978-3-030-16184-2_25.

[14] G. A. Marin, “Network Security Basics,” IEEE Secur. Privacy Mag., vol. 3, no. 6, pp. 68–72, Nov. 2005, doi: 10.1109/MSP.2005.153.

[15] J. M. Kizza, Guide to Computer Network Security. Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-55606-2.

[16] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, “A Survey of Game Theory as Applied to Network Security,” in 2010 43rd Hawaii International Conference on System Sciences, Honolulu, Hawaii, USA, 2010, pp. 1–10. doi: 10.1109/HICSS.2010.35.

[17] G. Pavlov and J. Karakaneva, “INFORMATION SECURITY MANAGEMENT SYSTEM IN ORGANIZATION,” Trakia Journal of Sciences, vol. 9, no. 4, p. 7, 2011.

[18] V. Y. Dronov and G. A. Dronova, “Principles of information security management system,” J. Phys.: Conf. Ser., vol. 2182, no. 1, p. 012092, Mar. 2022, doi: 10.1088/1742-6596/2182/1/012092.

[19] M. Nieles, K. Dempsey, and V. Y. Pillitteri, “An introduction to information security,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-12r1, Jun. 2017. doi: 10.6028/NIST.SP.800-12r1.

[20] “Risk or reward: What lurks within your IoT?,” p. 24, 2017.

[21] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, “Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls,” Sensors, vol. 19, no. 1, p. 19, Dec. 2018, doi: 10.3390/s19010019.

[22] V. Samaras, S. Daskapan, R. Ahmad, and S. K. Ray, “An enterprise security architecture for accessing SaaS cloud services with BYOD,” in 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), Southbank, Australia, Nov. 2014, pp. 129–134. doi: 10.1109/ATNAC.2014.7020886.

[23] J. Skorupa, A. Lerner, C. Canales, and M. Toussaint, “Magic Quadrant for WAN Edge Infrastructure,” p. 38.

[24] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “BYOD Authentication Process (BAP) Using Blockchain Technology,” Control Systems, vol. 10, no. 11, p. 8, 2018.

[25] “BYOD Secured Solution Framework,” International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 1602–1606, Aug. 2019, doi: 10.35940/ijeat.F8202.088619.

[26] P. K. Gajar, A. Ghosh, and S. Rai, “BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES,” p. 9, 2010.

[27] “International Journal of Scientific Research in Computer Science, Engineering and Information Technology,” p. 7, 2018.

[28] Weltwirtschaftsforum and Zurich Insurance Group, Global risks 2019: insight report. 2019. Accessed: Apr. 20, 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[29] “The Global Risks Report 2020,” World Economic Forum. https://www.weforum.org/reports/the-global-risks-report-2020/ (accessed Apr. 20, 2020).

[30] “Union Home Minister inaugurates Cyber Crime Unit of Delhi Police and National Cyber Forensic Lab.” http://pib.nic.in/newsite/PrintRelease.aspx?relid=188700 (accessed May 15, 2019).

[31] Vishnu Institute of Technology, B. V. P. santhi, P. Kanakam, and S. M. Hussain, “Cyber Forensic Science to Diagnose Digital Crimes- A study,” International Journal of Computer Trends and Technology, vol. 50, no. 2, pp. 107–113, Aug. 2017, doi: 10.14445/22312803/IJCTT-V50P119.

[32] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia, Y. Prayudi, A. Ashari, and T. K Priyambodo, “A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia,” International Journal of Computer Network and Information Security, vol. 7, no. 11, pp. 1–8, Oct. 2015, doi: 10.5815/ijcnis.2015.11.01.

[33] V. R. Kebande, N. M. Karie, and H. S. Venter, “A generic Digital Forensic Readiness model for BYOD using honeypot technology,” in 2016 IST-Africa Week Conference, Durban, South Africa, May 2016, pp. 1–12. doi: 10.1109/ISTAFRICA.2016.7530590.

[34] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, “Improving Forensic Triage Efficiency through Cyber Threat Intelligence,” Future Internet, vol. 11, no. 7, p. 162, Jul. 2019, doi: 10.3390/fi11070162.

[35] “Cybercrime Damages $6 Trillion by 2021,” Cybercrime Magazine, Nov. 09, 2020. https://cybersecurityventures.com/annual-cybercrime-report-2017/ (accessed Apr. 19, 2022).

[36] H. S. Lallie, “An overview of the digital forensic investigation infrastructure of India,” Digital Investigation, vol. 9, no. 1, pp. 3–7, Jun. 2012, doi: 10.1016/j.diin.2012.02.002.

[37] “Atlanta ransomware attack was worse than originally thought.” https://statescoop.com/atlanta-ransomware-attack-was-worse-than-originally-thought/ (accessed Apr. 19, 2022).

[38] R. G. G. Alam and H. Ibrahim, “CYBERSECURITY STRATEGY FOR SMART CITY IMPLEMENTATION,” Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., vol. XLII-4/W17, pp. 3–6, Sep. 2019, doi: 10.5194/isprs-archives-XLII-4-W17-3-2019.

[39] “Creating cyber secure smart cities,” p. 32.

[40] M. M. Ratchford, “BYOD: A Security Policy Evaluation Model,” in Information Technology - New Generations, vol. 558, S. Latifi, Ed. Cham: Springer International Publishing, 2018, pp. 215–220. doi: 10.1007/978-3-319-54978-1_30.

[41] “S&T Mobile Device Security Study,” Department of Homeland Security, Apr. 14, 2017. https://www.dhs.gov/publication/st-mobile-device-security-study (accessed Aug. 16, 2021).

[42] “DoS vs. DDoS: What Is the Difference?,” Fortinet. https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos (accessed Sep. 22, 2021).

[43] “Oracle and KPMG Cloud Threat Report 2019,” p. 60, 2019.

[44] D. Ferbrache, “How vulnerable are governments to cyber crime? | KPMG Global,” KPMG, May 22, 2018. https://home.kpmg/xx/en/home/insights/2016/05/how-vulnerable-are-governments-to-cyber-crime.html (accessed Aug. 09, 2019).

[45] “Digital Forensics in the Mobile, BYOD, and Cloud Era,” p. 4.

[46] J. Grover, “Android forensics: Automated data collection and reporting from a mobile device,” Digital Investigation, vol. 10, pp. S12–S20, Aug. 2013, doi: 10.1016/j.diin.2013.06.002.

[47] S. L. Garfinkel, “Digital forensics research: The next 10 years,” Digital Investigation, vol. 7, pp. S64–S73, Aug. 2010, doi: 10.1016/j.diin.2010.05.009.

[48] C. Utter, “The ‘Bring your own device’ conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges,” Journal of Digital Forensics, Security and Law, 2015, doi: 10.15394/jdfsl.2015.1202.

[49] B. Morrow, “BYOD security challenges: control and protect your most sensitive data,” Network Security, vol. 2012, no. 12, pp. 5–8, Dec. 2012, doi: 10.1016/S1353-4858(12)70111-3.

[50] “To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity,” World Economic Forum. https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/ (accessed Sep. 14, 2019).

[51] B. Tokuyoshi, “The security implications of BYOD,” Network Security, vol. 2013, no. 4, pp. 12–13, Apr. 2013, doi: 10.1016/S1353-4858(13)70050-3.

[52] U. Raj, “Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment,” vol. 13, no. 12, p. 7, 2015.

[53] K. AlHarthy and W. Shawkat, “Implement network security control solutions in BYOD environment,” in 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, Nov. 2013, pp. 7–11. doi: 10.1109/ICCSCE.2013.6719923.

[54] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology,” International Journal of Engineering, p. 6.

[55] A. Marotta and M. McShane, “Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach: A Holistic Cyber Risk Management Approach,” Risk Management and Insurance Review, vol. 21, no. 3, pp. 435–452, Dec. 2018, doi: 10.1111/rmir.12109.

[56] M. Kaur, D. Singh, V. Kumar, and K. Sun, “Color image dehazing using gradient channel prior and guided L0 filter,” Information Sciences, vol. 521, pp. 326–342, Jun. 2020, doi: 10.1016/j.ins.2020.02.048.

[57] M. Kaur, D. Singh, K. Sun, and U. Rawat, “Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5 D chaotic map,” Future Generation Computer Systems, vol. 107, pp. 333–350, Jun. 2020, doi: 10.1016/j.future.2020.02.029.

[58] S. Brotsis et al., “Blockchain Solutions for Forensic Evidence Preservation in IoT Environments,” arXiv:1903.10770 [cs], Mar. 2019, Accessed: Oct. 05, 2019. [Online]. Available: http://arxiv.org/abs/1903.10770

[59] D. A. Flores, F. Qazi, and A. Jhumka, “Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information,” in 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, Aug. 2016, pp. 1008–1015. doi: 10.1109/TrustCom.2016.0169.

[60] I. Ali and S. Kaur, “Detection and Control of Malicious activity and Digital Forensic in BYOD,” “International Journal of Recent Technology and Engineering” vol. 11, no. 4, P.7, doi:10.35940/ijrte.D8151.118419.

[61] “Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide,” p. 165.

[62] K. Joshi, M. Pathak, S. Jose, S. Dahiya, and S. Jose, “(71) Applicant: Gigamon Inc., Santa Clara, CA (US),” p. 18.

[63] M. Mahinderjit Singh, S. Sin Siang, O. Ying San, N. H. A. Hassain Malim, and A. R. Mohd Shariff, “Security Attacks Taxonomy on Bring Your Own Devices (BYOD)

Model," International Journal of Mobile Network Communications & Telematics, vol. 4, no. 5, pp. 1–17, Oct. 2014, doi: 10.5121/ijmnct.2014.4501.

[64] N. Shah, "Do Not Underestimate the Challenge of Securing SD-WAN," Fortinet Blog, Feb. 04, 2019. https://www.fortinet.com/blog/business-and-technology/do-not-underestimate-the-challenge-of-securing-sd-wan.html (accessed Sep. 23, 2019).

[65] K. Sharma and B. B. Gupta, "Towards Privacy Risk Analysis in Android Applications Using Machine Learning Approaches:," International Journal of E-Services and Mobile Applications, vol. 11, no. 2, pp. 1–21, Apr. 2019, doi: 10.4018/IJESMA.2019040101.

[66] P. Baillette, Y. Barlette, and A. Leclercq-Vandelannoitte, "Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users," International Journal of Information Management, vol. 43, pp. 76–84, Dec. 2018, doi: 10.1016/j.ijinfomgt.2018.07.007.

[67] "International Journal of Scientific Research in Computer Science, Engineering and Information Technology," p. 7, 2018.

[68] S.-K. Kim, U.-M. Kim, and J.-H. Huh, "A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security," Energies, vol. 12, no. 3, p. 402, Jan. 2019, doi: 10.3390/en12030402.

[69] A. Retnowardhani, R. H. Diputra, and Y. S. Triana, "Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 2, p. 753, Apr. 2019, doi: 10.12928/telkomnika.v17i2.10165.

[70] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," Forensic Science International: Synergy, vol. 1, pp. 61–67, 2019, doi: 10.1016/j.fsisyn.2019.03.006.

[71] S. R. Srivastava, S. Dube, G. Shrivastaya, and K. Sharma, "Smartphone Triggered Security Challenges - Issues, Case Studies and Prevention," in Cyber Security in Parallel and Distributed Computing, D. Le, R. Kumar, B. K. Mishra, M. Khari, and J. M. Chatterjee,

Eds. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2019, pp. 187–206. doi: 10.1002/9781119488330.ch12.

[72] Z. A. Baig et al., “Future challenges for smart cities: Cyber-security and digital forensics,” Digital Investigation, vol. 22, pp. 3–13, Sep. 2017, doi: 10.1016/j.diin.2017.06.015.

[73] P. K. Gajar, A. Ghosh, and S. Rai, “BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES,” p. 9, 2010.

[74] C. Walker-Osborn, S. Mann, and V. Mann, “to Byod or ... not to Byod,” ITNOW, vol. 55, no. 1, pp. 38–39, Mar. 2013, doi: 10.1093/itnow/bws142.

[75] L. Maccari, R. Fantacci, T. Pecorella, and F. Frosali, “Secure, fast handhoff techniques for 802.1X based wireless network,” in 2006 IEEE International Conference on Communications, Istanbul, 2006, pp. 3917–3922. doi: 10.1109/ICC.2006.255693.

[76] K. W. Miller, J. Voas, and G. F. Hurlburt, “BYOD: Security and Privacy Considerations,” IT Professional, vol. 14, no. 5, pp. 53–55, Sep. 2012, doi: 10.1109/MITP.2012.93.

[77] M. Ph. Stoecklin et al., “Passive security intelligence to analyze the security risks of mobile/BYOD activities,” IBM Journal of Research and Development, vol. 60, no. 4, p. 9:1-9:13, Jul. 2016, doi: 10.1147/JRD.2016.2569858.

[78] “BYOD—Identity and Authentication Solution Design Guide—August 2013,” p. 146, 2013.

[79] P. Iyengar, “IP ADDRESSES AND EXPEDITIOUS DISCLOSURE OF IDENTITY IN INDIA,” vol. 9, p. 28.

[80] C. Z. Tu, J. Adkins, and G. Y. Zhao, “Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory,” Journal of the Midwest Association for Information Systems, vol. 2019, no. 1, p. 19, 2019.

[81] S. Jose, “Cisco Identity Services Engine Administrator Guide, Release 2.2,” p. 1240.

[82] P. Kaspian, “ARUBA CLEARPASS NETWORK ACCESS CONTROL,” p. 5.

[83] M. Ratchford, P. Wang, and R. O. Sbeit, “BYOD Security Risks and Mitigations,” in Information Technology - New Generations, vol. 558, S. Latifi, Ed. Cham: Springer International Publishing, 2018, pp. 193–197. doi: 10.1007/978-3-319-54978-1_27.

[84] M. P. Souppaya and K. A. Scarfone, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,” National Institute of Standards and Technology, NIST SP 800-46r2, Jul. 2016. doi: 10.6028/NIST.SP.800-46r2.

[85] “Cisco SAFE Reference Guide,” p. 354.

[86] P. Beckett, “BYOD – popular and problematic,” Network Security, vol. 2014, no. 9, pp. 7–9, Sep. 2014, doi: 10.1016/S1353-4858(14)70090-X.

[87] J. Collie, “A Strategic Model for Forensic Readiness,” Athens Journal of Sciences, vol. 5, no. 2, pp. 167–182, Jun. 2018, doi: 10.30958/ajs.5-2-4.

[88] M. I. Ali et al., “Security Challenges and Cyber Forensic Ecosystem in IOT Driven BYOD Environment,” IEEE Access, pp. 1–1, 2020, doi: 10.1109/ACCESS.2020.3024784.

[89] “As the Number of Remote Workers Rises, Cisco Supports Customers with Expansion of Free Security Offerings - Cisco Blogs.” https://blogs.cisco.com/security/cisco-expands-free-security-offerings-to-help-with-rise-in-remote-workers (accessed Apr. 23, 2020).

[90] W. Largent, “Threat Roundup for April 10 to April 17.” http://blog.talosintelligence.com/2020/04/threat-roundup-0410-0417.html (accessed Apr. 23, 2020).

[91] A. Rao and C. T. Solutions, “Combating Cybersecurity Challenges with Advanced Analytics,” Digital Systems, p. 24.

[92] O. Johnson, “Cognizant Left With ‘No Good Options’ After Maze Attack: Security Expert,” CRN, Apr. 20, 2020. https://www.crn.com/news/channel-programs/cognizant-left-with-no-good-options-after-maze-attack-security-expert (accessed Apr. 23, 2020).

[93] “Palo Alto Networks | TechDocs Home.” https://docs.paloaltonetworks.com/ (accessed Jun. 28, 2020).

[94] “Prisma Access.” https://docs.paloaltonetworks.com/prisma/prisma-access (accessed Jun. 28, 2020).

[95] S. Challita, F. Zalila, C. Gourdin, and P. Merle, A Precise Model for Google Cloud Platform. 2018, p. 183. doi: 10.1109/IC2E.2018.00041.

[96] A. Al-Bataineh and G. White, "Analysis and detection of malicious data exfiltration in web traffic," in 2012 7th International Conference on Malicious and Unwanted Software, Fajardo, PR, USA, Oct. 2012, pp. 26–31. doi: 10.1109/MALWARE.2012.6461004.

[97] "Monitoring and Validating Mobility," p. 4.

[98] "Application Control Software Blade." https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_NextGenSecurityGateway_Guide/Content/Topics-FWG/Application-Control-Blade.htm (accessed Jun. 26, 2020).

[99] "Wireshark · Go Deep." https://www.wireshark.org/ (accessed Oct. 06, 2019).

[100] D. I. Wolinsky et al., "On the Design and Implementation of Structured P2P VPNs," p. 16.

[101] "DNS Security and Services | Akamai." https://www.akamai.com/us/en/solutions/security/dns-security-services.jsp (accessed Jun. 30, 2020).

[102] "Cyber Security Report 2020," p. 80, 2020.

[103] G. Shrivastava, "Network forensics: Methodical literature review," in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Mar. 2016, pp. 2203–2208.

[104] G. Shrivastava, S.-L. Peng, H. Bansal, K. Sharma, and M. Sharma, New Age Analytics: Transforming the Internet through Machine Learning, IoT, and Trust Modeling. 2020.

[105] "Browse cve vulnerabilities by date." https://www.cvedetails.com/browse-by-date.php (accessed Nov. 03, 2019).

[106] S. Soltani and S. A. H. Seno, "A formal model for event reconstruction in digital forensic investigation," Digital Investigation, vol. 30, pp. 148–160, Sep. 2019, doi: 10.1016/j.diin.2019.07.006.

[107] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, “Graphology based handwritten character analysis for human behaviour identification,” CAAI Transactions on Intelligence Technology, vol. 5, no. 1, pp. 55–65, Mar. 2020, doi: 10.1049/trit.2019.0051.

[108] L. Columbus, “83% Of Enterprise Workloads Will Be In The Cloud By 2020,” Forbes. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/ (accessed Feb. 16, 2020).

[109] D. Kim and S. Lee, “Study of identifying and managing the potential evidence for effective Android forensics,” Forensic Science International: Digital Investigation, p. 200897, Jan. 2020, doi: 10.1016/j.fsidi.2019.200897.

[110] S. J. Ngobeni, “Digital Forensic Readiness for Wireless Local Area Networks,” p. 695.

[111] F. Servida and E. Casey, “IoT forensic challenges and opportunities for digital traces,” Digital Investigation, vol. 28, pp. S22–S29, Apr. 2019, doi: 10.1016/j.diin.2019.01.012.

[112] X. Zhang and K.-K. R. Choo, Digital Forensic Education An Experiential Learning Approach. 2020. Accessed: Oct. 04, 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-23547-5

[113] S. Sathwara, N. Dutta, and E. Pricop, “IoT Forensic A digital investigation framework for IoT systems,” in 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, Jun. 2018, pp. 1–4. doi: 10.1109/ECAI.2018.8679017.

[114] E. Casey, “The chequered past and risky future of digital forensics,” Australian Journal of Forensic Sciences, vol. 51, no. 6, pp. 649–664, Nov. 2019, doi: 10.1080/00450618.2018.1554090.

[115] A. Gupta, D. Singh, and M. Kaur, “An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps,” Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 3, pp. 1309–1324, Mar. 2020, doi: 10.1007/s12652-019-01493-x.

[116] “IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses - Mar 14, 2018,” IBM News Room, Oct. 04, 2019. https://newsroom.ibm.com/2018-03-14-IBM-Study-Responding-to-Cybersecurity-Incidents-Still-a-Major-Challenge-for-Businesses (accessed Oct. 06, 2019).

[117] “General Data Protection Regulation (GDPR) guidance,” NHS Digital. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance (accessed Sep. 26, 2019).

[118] “2017 Norton Cyber Security Insights Report - Global Results,” p. 30, 2018.

[119] B. Cusack and T. Laurenson, “Systems architecture for the acquisition and preservation of wireless network traffic,” p. 9.

[120] D. Ghimire, E. Valle, and S. Robin, “Check Point Software Technologies Check Point SandBlast Agent Next Generation AV E80.82.,” p. 14.

[121] S. Osterland and J. Weber, “Analytical analysis of single-stage pressure relief valves,” International Journal of Hydromechatronics, vol. 2, no. 1, p. 32, 2019, doi: 10.1504/IJHM.2019.098951.

[122] “Cisco Security Report: Majority of Orgs Do Not Monitor DNS,” Cisco Umbrella, Jan. 21, 2016. https://umbrella.cisco.com/blog/cisco-security-report-more-orgs-should-be-monitoring-dns (accessed Dec. 27, 2020).

[123] I. Ali and S. Kaur, “BYOD CYBER FORENSIC ECO-SYSTEM,” International Journal of Advanced Research in Engineering and Technology, vol. 11, no. 9, p. 22, doi: 10.34218/IJARET.11.9.2020.043

[124] A. Lamba, S. Singh, and B. Singh, “Mitigating Zero-Day Attacks in IoT Using a Strategic Framework,” SSRN Electronic Journal, 2016, doi: 10.2139/ssrn.3492684.

[125] “Firepower Management Center Configuration Guide, Version 6.0 - File/Malware Events and Network File Trajectory [Cisco Firepower Management Center],” Cisco. https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html (accessed Dec. 18, 2020).

[126] "Security CheckUp | Check Point Software." https://pages.checkpoint.com/security-checkup.html (accessed Feb. 16, 2020).

[127] M. I. Ali and S. Kaur, "The Impact of India's Cyber Security Law and Cyber Forensic On Building Techno-Centric Smartcity IoT Environment," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, Feb. 2021, pp. 751–759. doi: 10.1109/ICCCIS51004.2021.9397243.

List of Publications

[1] "BYOD Secured Solution Framework," International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 1602–1606, Aug. 2019, doi: 10.35940/ijeat.F8202.088619.

[2] I. Ali and S. Kaur, "Detection and Control of Malicious activity and Digital Forensic in BYOD," International Journal of Recent Technology and Engineering, vol.8, no.4, pp. 11392-11398, Nov 2019, DOI: 10.35940/ijrte.D8151.118419

[3] M. I. Ali et al., "Security Challenges and Cyber Forensic Ecosystem in IOT Driven BYOD Environment," IEEE Access, pp. 1–1, 2020, doi: 10.1109/ACCESS.2020.3024784.

[4] M. I. Ali and S. Kaur, "Next-Generation Digital Forensic Readiness BYOD Framework," Security and Communication Networks, vol. 2021, pp. 1–19, Mar. 2021, doi: 10.1155/2021/6664426.

[5] M. I. Ali and S. Kaur, "BYOD Cyber Threat Detection and Protection Model," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, Feb. 2021, pp. 211–218. doi: 10.1109/ICCCIS51004.2021.9397105.

[6] M. I. Ali and S. Kaur, "The Impact of India's Cyber Security Law and Cyber Forensic On Building Techno-Centric Smartcity IoT Environment," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, Feb. 2021, pp. 751–759. doi: 10.1109/ICCCIS51004.2021.9397243.

[7] I. Ali and S. Kaur, "Systematic Review of BYOD Cyber Forensic Ecosystem," Global Emerging Innovation Summit (GEIS-2021), 2021, 62-76, Doi**:** 10.2174/978168108901012101001**0**

[8] I. Ali and S. Kaur, "BYOD CYBER FORENSIC ECO-SYSTEM," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 9, p. 22, doi: 10.34218/IJARET.11.9.2020.043.

[9] I. Ali, P. Jha, D. A. Sharma, and D. S. Kaur, "Security Analysis and Prevention in Cloud Computing," *The Role of IoT and Blockchain: Techniques and Applications*. CRC Press, 2022. 401-418.