A LIGHT WEIGHT PROTOCOL FOR IOT SYSTEMS

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Science & Engineering

By

Saurabh

Registration Number: 41700279

Supervised By	**Co-Supervised By**
Dr. Chirag Sharma (16717)	**Dr. Sahil Verma**
Computer Science & Engineering	**Computer Science & Engineering**
Associate Professor	**Professor & Dean**
LPU, Jalandhar	**Chandigarh University, Mohali**

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB
2025

DECLARATION

I, hereby declared that the presented work in the thesis entitled "**A Light weight Protocol for IoT Systems**" in fulfilment of degree of **Doctor of Philosophy (Ph.D.)** is outcome of research work carried out by me under the supervision **Dr. Chirag Sharma**, working as Associate Professor, in the Department of Computer Science and Engineering of Lovely Professional University, Punjab, India. In keeping with general practice of reporting scientific observations, due acknowledgements have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.

(Signature of Scholar)
Name of the scholar: Saurabh
Registration No.: 41700279
Department/school: Computer Science and Engineering
Lovely Professional University,
Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled **A Light weight Protocol for IoT Systems**” submitted in fulfillment of the requirement for the reward of degree of **Doctor of Philosophy (Ph.D.)** in the Department of Computer Science & Engineering, is a research work carried out by **Saurabh**, 41700279, is bonafide record of his original work carried out under our supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

Chirag

(Signature of Supervisor)
Dr. Chirag Sharma
Associate Professor
Computer Science & Engineering
Lovely Professional University
Jalandhar

(Signature of Co Supervisor)
Dr. SahilVerma
Professor & Dean
Computer Science & Engineering
Chandigarh University, Mohali

ABSTRACT

The rise of Internet of Things (IoT) gadgets has led to the need, for effective methods of confirming identities to safeguard data transmission and prevent entry. Traditional ways of confirming identities often reliant on third party servers come with challenges like heightened security risks, delays in communication and compatibility issues in settings. These difficulties are made worse by the computing power and energy capacity of devices. To tackle these issues this study proposes a authentication system that uses fog computing and location based checks to create a decentralized, efficient and secure authentication framework for IoT setups.

At the core of this suggested system is the use of fog devices positioned strategically at the networks edge to handle authentication duties and process data locally. This method reduces reliance on cloud servers cutting down on delays in communication and conserving bandwidth. Additionally the system utilizes the Euclidean distance formula in a location based verification process to make sure that only devices within a range can verify their identity and access specific network resources. This extra layer of security is especially useful in applications requiring location verification, like healthcare systems asset tracking solutions and secure access control setups.

The study involved a simulation analysis conducted in the NS3 environment to confirm the effectiveness of the protocol, against common security risks like man in the middle replay and impersonation attacks. The results showcased the protocols strength and resilience emphasizing its ability to ensure dependable communication across network scenarios. Furthermore a detailed performance evaluation was carried out comparing the approach with RSA and ECC based authentication methods. The assessment covered factors such as computational complexity communication overhead end to end delay and throughput. The outcomes indicated that the new protocol significantly reduces both load and communication requirements making it a suitable solution for devices with limited resources.

Moreover the research delved into integrating the authentication protocol into a fog cloud setup that optimizes task distribution between fog nodes and central cloud servers. This hybrid model enhances system scalability by supporting devices and adapting to changing network structures and IoT device mobility patterns. The study also discussed enhancements, for IoT advancements by suggesting advanced cryptographic techniques integration utilizing machine learning for adaptive security measures and incorporating blockchain technology for secure and transparent authentication logs.

Overall this study introduces a creative approach, to authentication tackling the crucial requirements of security, effectiveness and scalability. The protocols integration of fog computing and location based strategies marks a progress from conventional approaches establishing a stronger and more flexible structure for safeguarding IoT environments. The discoveries from this analysis carry implications for shaping the future of systems presenting a route to improved security and efficiency, in our ever more interconnected society.

ACKNOWLEDGEMENT

The completion of this PhD thesis marks a significant milestone in my academic journey, one that would not have been possible without the support, guidance, and encouragement of many remarkable individuals.

First and foremost, I am deeply indebted to my supervisor, **Dr. Chirag Sharma**, whose exceptional expertise, insightful advice, and unwavering patience were crucial to the success of this work. Your ability to inspire and challenge me intellectually has profoundly shaped this research, and I am truly grateful for your mentorship.

I am also grateful to my colleagues and fellow researchers. The collaborative spirit, stimulating discussions, and shared knowledge within this community have been a constant source of inspiration and motivation. I am fortunate to have worked alongside such talented and dedicated individuals.

To my friends, who have provided both intellectual and emotional support throughout this journey, thank you for your constant encouragement and for believing in me, even when I doubted myself. Your friendship has been a vital part of this experience.

To my family, especially my parents, my wife, my kids and my brothers, your unconditional love, understanding, and patience have been my foundation. Your unwavering support has been my anchor through the challenges of this PhD journey. I cannot express enough how much your belief in me has meant.

Finally, I dedicate this thesis to my father, whose passion for knowledge and learning has been a lifelong source of inspiration. Your influence has shaped my path, and this work is a testament to the values you instilled in me.

Thank you all for being part of this journey. Your support has been my greatest strength.

Saurabh

List of Figures

List of Tables

INTERNET OF THINGS

CHAPTER-1

1.1 Background

With its potential to help people tremendously, the Internet of Things has fascinated a number of people recently. The IoT(Internet of Things), which offers the infrastructure of pervasive wireless sending and identification systems with billions of uniquely identifiable smart sensing devices to connect everything at any time and everywhere at any time and everywhere, is widely acknowledged as the next generation of the internet [1,2]. Kevin Ashton first proposed the idea in 1999, to connect anything anytime, anywhere [1]. The devices in the IoT collaborate with each other to support innovative and intelligent services on their own. They have built in facilities for sensing, processing, and actuation. IoT applications include those for healthcare, transportation, agriculture, industry, smart homes and so on [2]. An overview of fundamental ideas behind IoT is given in the chapter. It discusses the definition of the Internet of Things, its uses, the architecture that accommodates heterogeneous devices, and related communication protocols. The chapter also covers the security needs and solutions that are necessary to connect IoT devices and provide end users with services.

1.2 Definition of IoT

“Internet of Things” (IoT) describes an innovative and invisible network that entails interconnections of a plethora of wireless or wired devices. It makes it possible to transform devices with Internet access into a networked ecosystem where digital data is always and everywhere available. These machines without human involvement smoothly connect with one another [9]. Figure 1.1 shows that when the devices get interconnected and begin exchange of the data then how the Internet of Things will develop has been publicized.

As per Gartner’s report, there are currently fifty billion devices linked to the Internet [2, 41, 54]. IoT devices are outfitted intelligently to detect the environment & actuators to carry out operations on their own [10]. Figure 1.2 displays numerous IoT device illustrations. These devices' low processing speeds, tiny memory capacity, and inadequate computational power result in fundamental resource constraints.

Figure 1.1 Connections of IoT Devices

The IoT paradigm has emerged with numerous supporting technologies, such as radio frequency identification, CC, gateway devices, WSNs, and more [11]. Several contemporary technology examples are given in figure 1.3.

Figure 1.2 IoT Devices

i. In order to regulate the environment, a Wireless Network of Sensors (WSN) is made up of a number of physically installed autonomous sensors [1].

ii. To identify and track IoT things, radio frequency identification (RFID) is employed to enable short-distance data transmission via radio waves [1].

iii. Due to the availability of infinite processing and storage capacity, cloud computing is considered as an important component to the Internet of Things [12].

iv. For devices with constrained resources, the CoAP is an AL protocol. [4,13]

v. By integrating IPv6 with LoWPAN, 6LoWPAN enable IPv6 packet transfer across 802.15.4 networks. Several IoT support components can be used with 6LoWPAN. [4]

vi. Because of its improved precision, low energy consumption, and security characteristics, Ultra Wideband (UWB) is useful for a range of Internet of Things applications. [14]

vii. Low-power connections for personal space items are made possible by WPANs, which use the 802.15.4 protocol for both the physical and MAC layers [4].

viii. Near Field Communication may be used with a variety of IoT devices, such as those for payment and authentication, to aid in data interchange and network access [15].

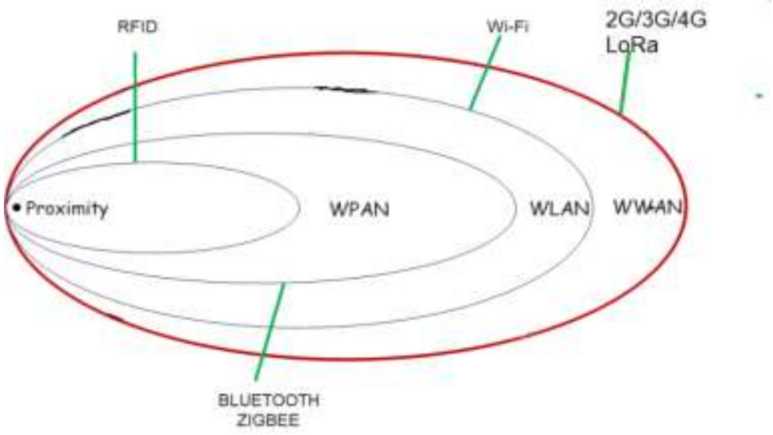


Figure 1.3 IoT Enabling Technologies

1.3 IoT Architecture, Elements and Protocols

The conventional structure of IoT includes perception, network and application layer [16] presented in figure 1.4.

1.3.1 Perception Layer

The 1st level i.e. Perception Layer, which consists of several physical IoT devices, is in charge of IoT device interaction and data collecting. Data collecting tools include sensors and other smart devices with radio frequency identification (RFID) tags.

1.3.1.1 Wireless Sensors

Wireless sensors are essential to IoT because to their capacity to sense and communicate.

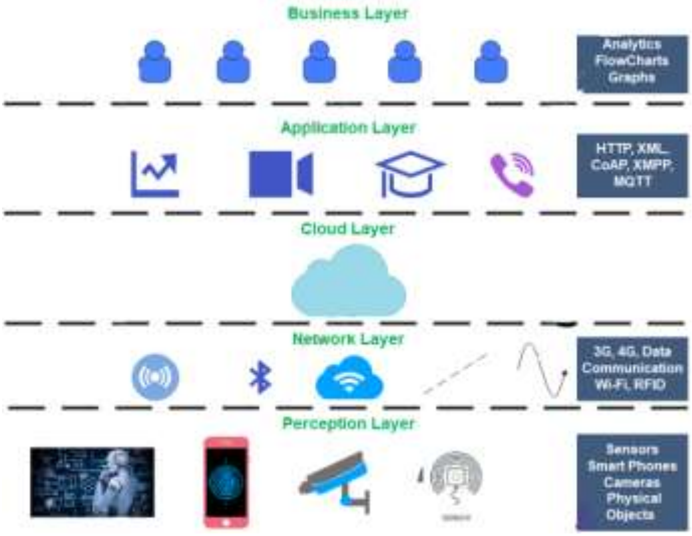


Figure 1.4 IoT Layered Architecture

A Wireless Network with Sensor (WSN) is an assembly of multiple quick sensors dispersed throughout distant areas with the purpose of detecting and collecting data regarding various parameters are illustrated in figure 1.5.

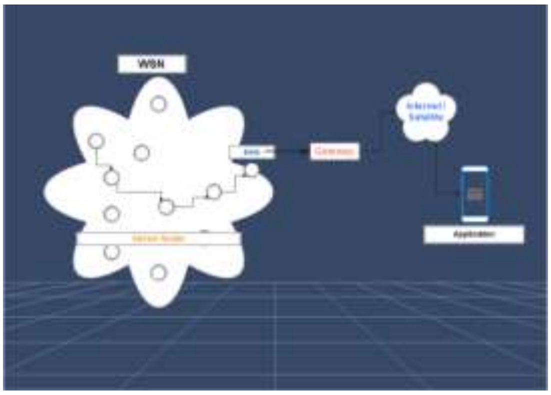


Figure 1.5 Wireless Sensor Network Architecture

1.3.1.2 RFID (Radio Frequency Identification)

These technologies are an important part of IoT since they can track and monitor goods using radio waves, as well as passively identify them [16]. Among the parts of RFID are a tag or radio signal transponder, which records an object's unique identity, and a tag reader, which uses radio waves and one or more antennas to identify an object. The tag reader sends the tag's identifying number to a computer so that the object can be tracked and monitored, as given in Figure 1.6.

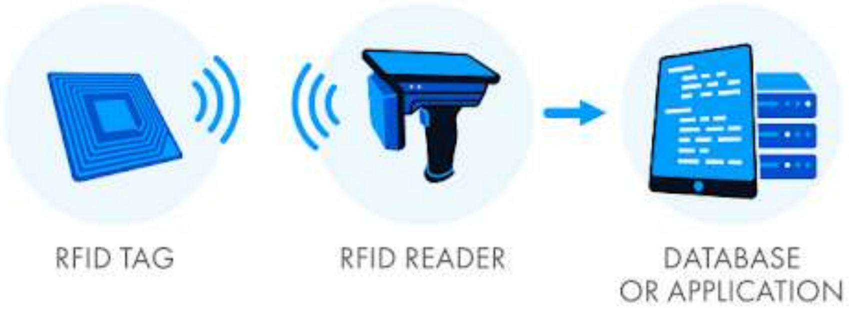


Figure 1.6 RFID Systems [16]

1.3.2 Network layer

Data is gathered, processed, and sent to AL (application layer) and received from 1st level (perception layer) via this layer. To support the networking of IoT devices, it includes a variety of communication methods, making it the crucial component of the IoT architecture. ZigBee, BLE, LRWAN, and IPv6 over Low Power technologies (LoRaWAN) are some of the widely used communication technologies. Table 1.1 compares the researched IoT wireless technologies and helps in choosing the best protocol for an identified Internet of Things system.

Table 1.1 Comparisons of IoT Wireless Technologies

Wireless Technology	**Frequency Band**	**Data Rate**	**Range**	**Power Consumption**	**Network Topology**	**Security**	**Scalability**	**Interoperability**	**Cost Efficiency**
Wi-Fi	2.4 GHz, 5 GHz	Up to Gbps	30-100 meters	Moderate	Point-to-Point, Point-to-Multi-Point	WPA2/WPA3, Enterprise Security	High	Good	Moderate-High
Bluetooth	2.4 GHz	Up to Mbps	10-100 meters	Low	Point-to-Point, Piconets	BLE: AES-CCM, Classic: PIN/PASSKEY	Moderate	Good	Low
Zigbee	2.4 GHz	Up to 250 Kbps	Up to 100 meters	Low-Moderate	Mesh Topology	AES-128, Link-layer Security	High	Moderate	Moderate

Z-Wave	908/916 MHz	Up to 100 Kbps	Up to 100 meters	Low	Mesh Topology	AES-128, Network Layer Security	High	Moderate	Moderate
LoRa	Sub-GHz Bands	Up to Kbps	2-10 km (Urban)	Low-Moderate	Star/Peer-to-Peer, LPWAN	AES-128 (end-to-end), Packet Forwarding Security	High	Moderate	High
NB-IoT	Cellular Bands	Up to Kbps	10-100 km	Low-Moderate	Cellular Topology	Cellular Security, SIM-based Authentication	High	High	Moderate-High
LTE-M	Cellular Bands	Up to Mbps	1-10 km	Moderate	Cellular Topology	Cellular Security, SIM-based Authentication	High	High	Moderate-High
Sigfox	Sub-GHz Bands	Up to Kbps	Up to 50 km	Low	Ultra-Narrowband	RC4-based	High	Moderate	High
Weightless-N	Sub-GHz Bands	Up to Kbps	Up to 5 km	Low-Moderate	LPWAN, Star/Peer-to-Peer	AES-128, Network Layer Security	High	Moderate	Moderate
Wi-SUN	Sub-GHz Bands	Up to Mbps	Up to 5 km	Low-Moderate	Mesh Topology	AES-128, Network Layer Security	High	Moderate	Moderate-High

1.3.2.1 ZigBee

Among the wireless communication technologies available for short-distance transportation is ZigBee [22]. Intelligent home systems, intelligent meters, and intelligent healthcare can all get advantages from their use. Components of ZigBee include layers i.e network, MAC, application & physical level.

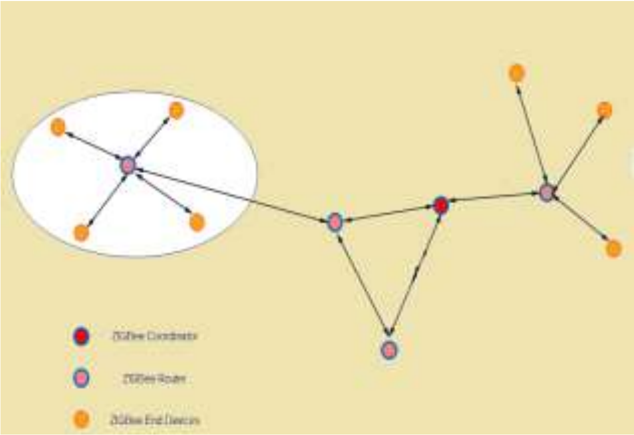


Figure 1.7 ZigBee Communication Architecture

The foundation of these layers is derived from the 802.15.4 standard. Unlike mesh or tree networks, which utilize intermediate routers to extend the network, star networks incorporate end devices that are straightforwardly linked to the coordinator, as depicted in Figure 1.7. To facilitate data routing, the network layer utilizes ADhoc on-demand distance vector (AVODV) and modified cluster-tree algorithms [21]. Owing to its limited interoperability, a ZigBee device is only capable of connecting with other ZigBee devices.

1.3.2.2 BLE

A popular low-power, short-range communication method in IoT automobile systems is BLE. BLE, in contrast to traditional Bluetooth, is energy-efficient by design. The L2CAP, an ARP, MAC layer, and PHY layer make up the BLE protocol stack.

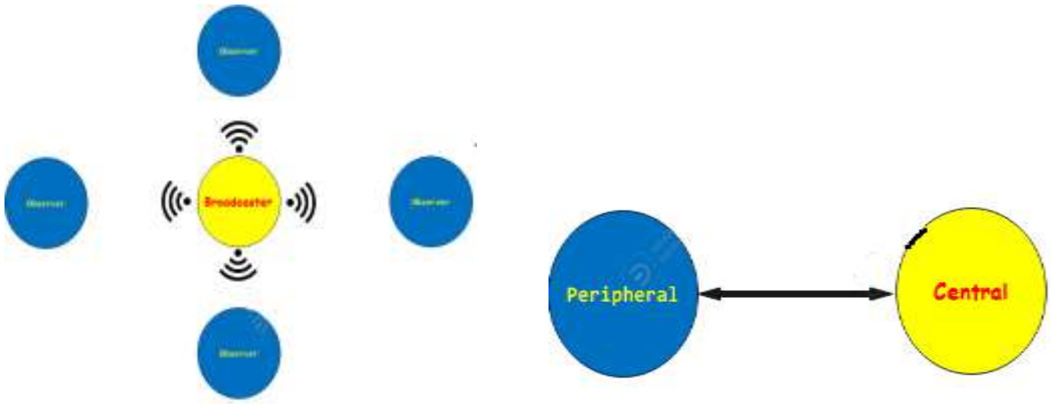


Figure 1.8(a) One Way Communication (b) Connection Oriented Communication

Multiple communication modalities are supported by BLE, as seen in figures 1.8(a) and (b), where every slave node is linked to a single master node. Th main responsibility of the master node is to establish a connection and send a time-division multiple access (TDMA) scheduling table.

1.3.2.3 6LoWPAN

The combination of IPv6 and LoWPAN introduced 6LoWPAN [21]. It makes IPv6 data transmission possible for devices with restricted capabilities via wireless channels and side by side minimizes transmission costs, and facilitates mobility making it appropriate for devices with limited resources. Smart agriculture, smart homes, and industrial IoT are the most prevalent use cases for 6LoWPAN. Devices supporting 6LoWPAN support both 802.15.4 and 6LoWPAN protocols, in contrast to ZigBee. Sixth-generation Wi-Fi networks, such as Wi-Fi, can be connected to 6LoWPAN, as Figure 1.9 shows. Within the 6LoWPAN network, an effective routing system created for lossy and low-power networks is utilized. Directed acyclic graph (DAG) serves as the foundation for Remote Protocol Layer (RPL), which facilitates P2P, P2M & M2P communication.

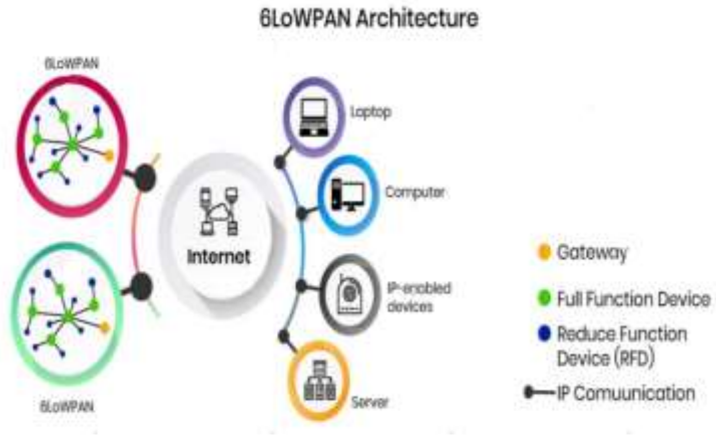


Figure 1.9 6LOWPAN Architecture [21]

1.3.2.4 LoRaWAN

For scalable and low-power Internet of things applications, a long distance protocol used is LoRaWAN, as shown in figure 1.10. Using one-hop connectivity, the end devices can use the ALOHA scheme to interact with one or more gateways. Internet protocol is used to link the gateways to the network server. The end device opened the lines of communication in both directions.

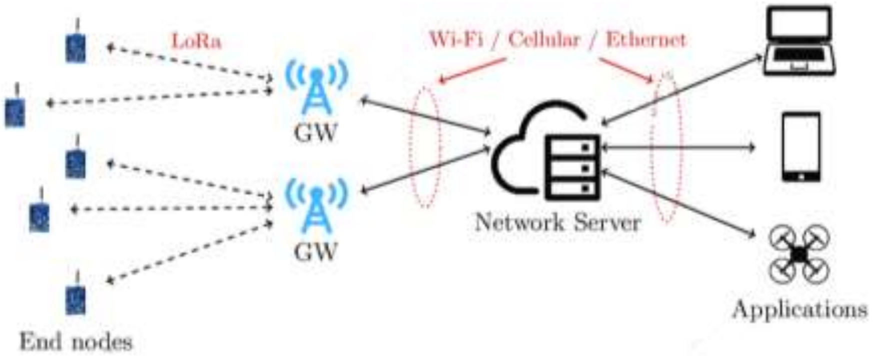


Figure 1.10 LoRaWAN Architecture

1.3.3 Application layer

Upon receiving data from the NL, AL delivers the necessary services to users of IoT. MQTT, CoAP, XMPP, VSCP, and AMQP are communication protocols specific to IoT and M2M applications, each possessing unique attributes. MQTT is a compact machine-to-machine (M2M) protocol that employs a publish/subscribe paradigms and functions over TCP/IP with SSL/TLS security enabled. XMPP facilitates communication between clients and servers utilizing the publish/subscribe and request/response paradigm over TCP/IP, with security provided by SASL/TLS. VSCP is a machine-to-machine (M2M) protocol that relies on a request/response paradigm over TCP/IP. It operates without specified security measures and is event-based, with a 4-byte header payload. AMQP is a web transfer protocol that facilitates point-to-point and publish/subscribe communication over TCP/IP. It is protected by SSL/TLS and SASL algorithms and offers Quality of Service (QoS) and a versatile message system. The protocol has an 8-byte header and a minimum packet size of 60 bytes. Each protocol differs in its data exchange methodology. MQTT, CoAP, and AMQP employ broker-based systems; XMPP applies a bus-based method, while VSCP functions on an event-based system.

The most popular application protocol (MQTT) is message queuing telemetry transmission, and it supports a large variety of application protocols (CoAP).

1.3.3.1 CoAP

The intricacy of the HTTP protocol renders it inappropriate for low-power devices, given the constrained resources of Internet of Things devices. Constrained Application Protocol (CoAP) is a better option since it is based on the REST structure. Four different message kinds are used by CoAP: acknowledgement, reset, non-confirmable, and confirmable messages. With the help of this protocol, the server can deliver messages to devices that are inaccessible via HTTP and provide functionality like resource discovery and push notifications. These devices might also be listed by the server.

1.3.3.2 MQTT

A lightweight messaging protocol called MQTT was created to facilitate communication between people, networks, and applications. It uses a publish/subscribe architecture with publishers, subscribers, and a broker, given in figure 1.11. IoT subscriber’s servers store applications and receive data, and publisher’s embed devices that transmit data.

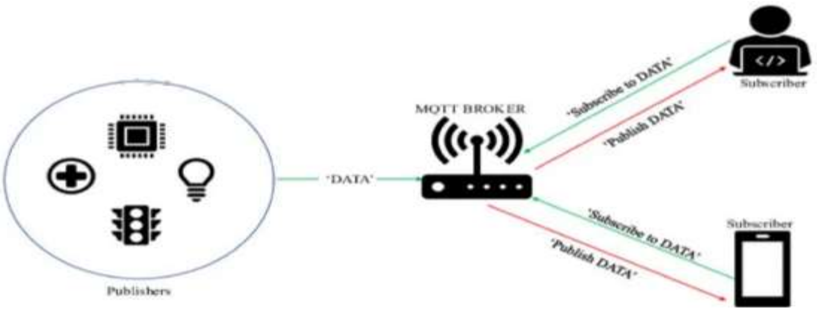


Figure 1.11 Topology of the MQTT Protocol in IoT [74]

1.4 Applications of IoT

Industrial IoT offers a wide range of applications depicted in figure 1.12. A collection of installed smart appliances that communicate locally over wireless channels is referred to as a "smart home." A smart lock, baby monitor, and fire alarm are a few examples. It is feasible to access home devices remotely by utilising a home gateway.

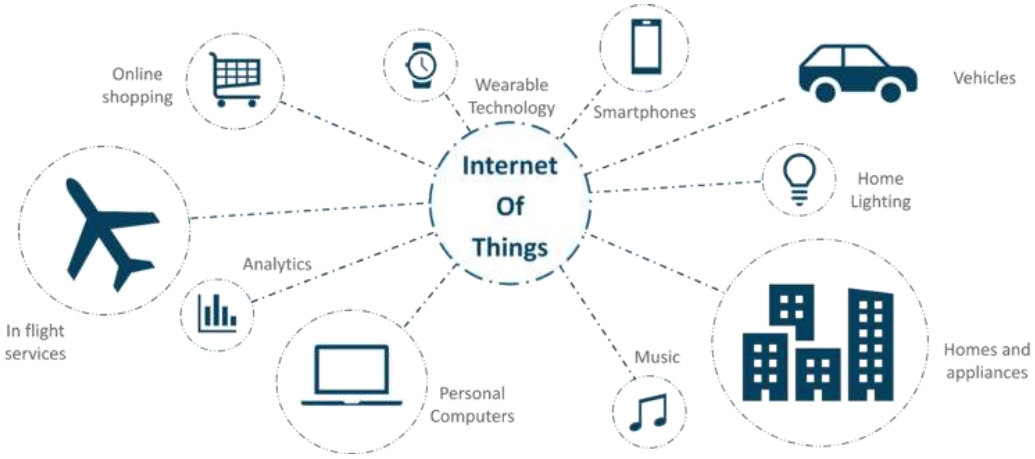


Figure 1.12 IoT Applications

Patient physiological parameters may be easily collected, transmitted, and stored with the help of smart healthcare. For example, a hospital server receives a patient's heart rate data that was captured by medical sensors for monitoring and diagnosis.

Smart agriculture provides high yield and prevents financial losses by allowing management of humidity, temperature, irrigation, soil moisture, and microclimate variables remotely. Animal’s activities as well as the physical problems in an intelligent farming system also get monitored with the help of the sensors connected to them.

Smart retail allows for the tracking of goods while they are being transported or stored in the warehouses. To follow the state of a vend article, sensors can be attached. Various intelligent ecommerce platforms were developed to provide clients with smart services and so draw in more customers.

Smart industry, Industrial IoT (IoT) automates the production process with little human involvement by using machine-to machine technology. To produce end goods that are reliable and efficient, the IoT attempts to better regulate the manufacturing process, data, and challenges.

1.5 IoT Security

Numerous security-related concerns are being faced by the IoT even though the concept of IoT has fascinating development & to enhance people's lives and creation of probable services going on at a very high pace. Security weaknesses of various technologies like WSN, RFID, and Bluetooth are inherited by IoT [6]. In addition, as per Gartner’s report it is expected that billions of gadgets will be connected to the Internet by 2050 [7]. There will be a huge amount of flow of data over the Internet during the coming years [8]. As a result, the information privacy of the user will be compromised [28]. For instance, a Software Defined Radio (SDR) allows an attacker to intercept a baby monitor system, jeopardizing the privacy of the user [29]. IoT network security is a significant issue that must be addressed. The academic community has focused particular attention on the security of IoT [30, 31]. Critical analysis of security vulnerabilities and IoT attachment vectors is necessary to develop a secure system. To safeguard IoT systems, specific security requirements and characteristics, such as authentication, confidentiality, integrity, and others, must be ensured.

The various IoT attacks are classified according to their levels, goals, and available definitions. Security needs are also categorized according to the gals of attackers.

1.5.1 IoT security attacks

Emerging IoT technologies are progressing rapidly, but the associated security vulnerabilities are also increasing. Efficiently incorporating security needs into IoT systems requires first a thorough analysis of IoT vulnerabilities and attacks. IoT attacks vary in nature since they integrate WSN & RFID, thereby inheriting the security vulnerabilities inherent in both technologies. The security attacks that provide risks to IoT networks are enumerated in Table 1.2.

Table 1.2 Different Attacks and their Threat Levels

Attack	Behaviour	Threat Level	Layer Applicable	Suggested Solution
Injection	Malware or additional code may get injected inside the program to steal sensitive information	Low-Medium	Application Layer	Blocking malicious traffic
Interruption	Preventing users to access the network by making the network unavailable	High	Application Layer	Authorization so that only the authorized users shall get the access of the network
Sniffing	Using a packet sniffer to capture the network traffic to intercept the data or theft	Medium	Application Layer	Using encryption while sharing data, installing antivirus or firewall, continuously monitoring the network, using VPN while connecting public network
Poisoning	Bad data is injected into the program module or manipulating the data	High	Cloud Layer	Training data filtering, robust learning, usage of auxiliary tools will help in prevention
Flooding	Sending massive amount of traffic, also a type of denial of service attack forcing a server to be unavailable for legitimate	High	Cloud Layer	Installing intrusion prevention system, firewall filtering, network fragmentation

	traffic			by dividing bigger network into smaller networks
Impersonate	Identity of an authorized person used by the attacker to gain monetary benefits, mostly happen through email	Medium	Cloud Layer	Analysis of relationship of sender and receiver, identification of compromised accounts,
Denial of Service Attack	Sending bulk messages, packets again and again, modifying a packet to disturb the normal functioning of the network	Extremely High	Communication Layer	Authentication techniques to protect the network, cryptographic techniques to ensure security of the network
Encryption Attack	Passive attack and active attack, target is to hack cryptographic solutions, identify weakness or flaws and retrieve plaintext from ciphertext	High	Communication Layer	Manage keys effectively, test system for vulnerabilities, updation of cryptographic algorithms regularly
Man in the Middle Attack	Alteration of the messages and eavesdropping are the main purposes of this attack. Intruder may also modify the data.	Low-Medium	Communication Layer	Apply confidentiality and integrity of the messages by using encryption to avoid alteration
Sybil Attack	Introduced by John R. Douceur, malicious node using identities of some other legible nodes for masquerading, degrade data integrity, security and resource utilization	Medium	Communication Layer	Message authentication method, identity validation, application-specific defense

Blocking	One of the types of DoS attacks, jamming of the network and the malware injection. Viruses like Trojan Horse, worms can disrupt the network	Extremely High	Communication Layer	Activating firewall, updated licensed anti-virus programs to protect the network
Routing Diversion	By showing heavy traffic on a route inappropriately which leads to high response time to the requests	High	Communication Layer	Ensuring connectivity
Eaves Dropping	Privacy of the data may get leaked as the eavesdropper may capture the data for analysis purposes	Low-Medium	Perception Layer	Encoding of the data can be done depending upon the type of the device as well as the energy levels
Malware Injection	Insertion of some specific code to alter the regular operations of the system, most commonly used one is SQL injection attack	Medium	Perception Layer	Usage of antivirus software, firewalls, updating OS regularly

1.5.2 IoT security threats

In accordance with the research on security assaults, in Figure 1.13 taxonomy of IoT attacks based on levels, goals, and countermeasures has been illustrated. The three IoT layer security problems have been taken into account when analysing the three tiers of IoT security flaws in this section. Important IoT components like WSNs and RFID have been the target of security attacks that have targeted their perception layer. Examples of AL dangers are attacks on end-user devices and IoT software.

IoT attacks are mostly motivated by the following:

i. Obtaining unapproved access to correspondence.
ii. Exposing or changing data.
iii. Turning off the resources on the device.

Security measures are put in place to counter these threats and address the goals that IoT attacks have been recognized to pursue. These precautions cover communication security, data security, and device security. Important security needs including integrity, confidentiality, and privacy taken into account to protect data. To fulfil crucial operational needs, IoT devices must also be dependable and available in a variety of settings.

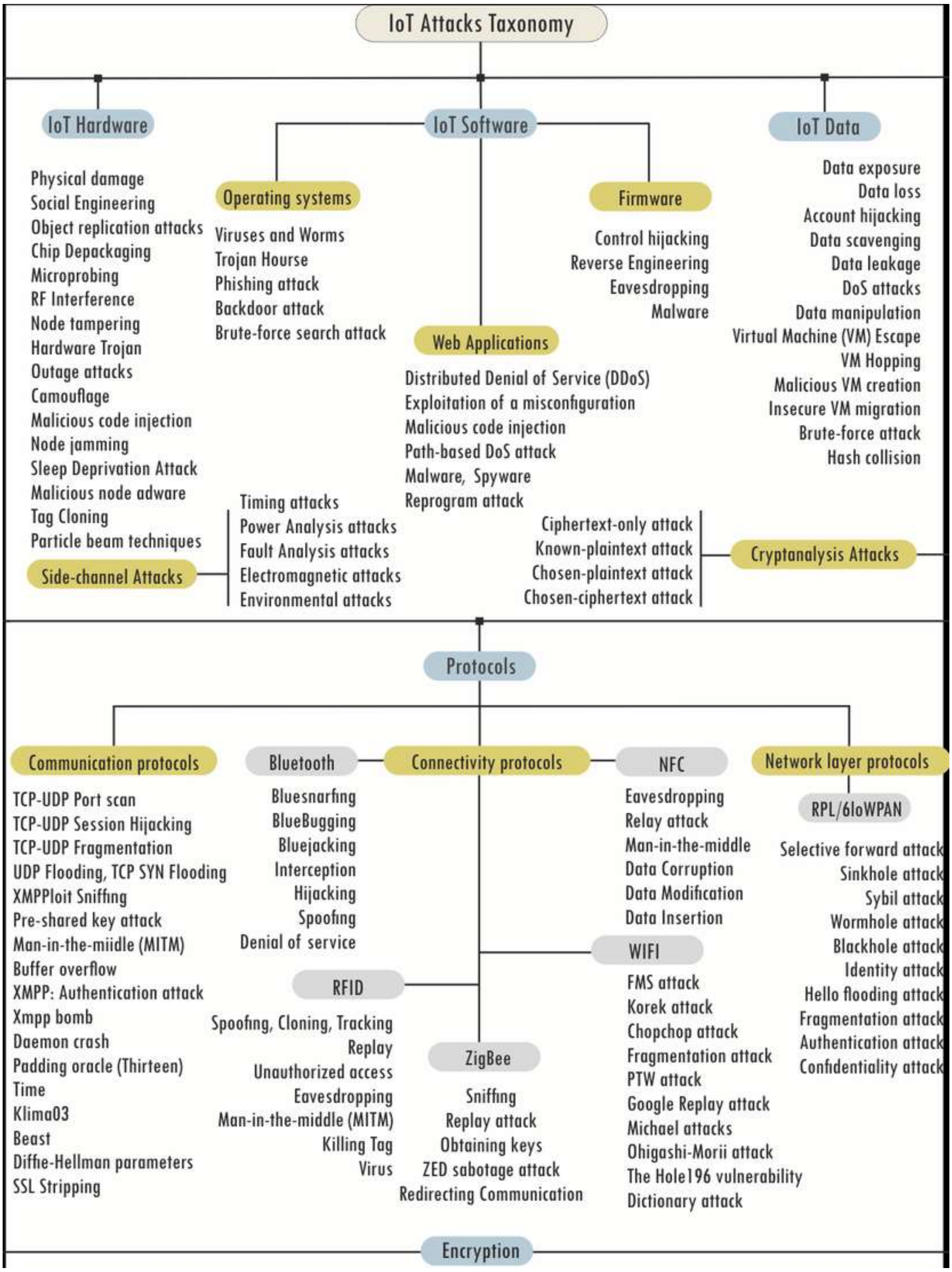


Figure 1.13 Classifications of IoT Attacks [37]

1.5.2.1 Perception layer threats

IoT devices are susceptible to a number of security vulnerabilities due to their resource limitations and diverse design. As WSNs are typically placed in harsh, unmanaged situations, they are vulnerable to a number of threats. Sinkhole, BH, wormhole, Sybil, DoS, Node capture, & node injection attacks are frequently used security attacks against WSNs [43]. In Table 1.2 quick summaries of several security attacks are given. Just like the WSN, Table 1.2 highlights various attacks RFID networks are susceptible to. Hence the IoT inherits their security risks.

1.5.2.2 Network layer threats

To guarantee secrecy, authentication, and data integrity, the ZigBee protocol uses a number of security measures, including the MIC & AES-CCM. A link key is used for broadcasting, whereas a network key is used for unicast. The connection key and network key are generated by means of a master key that is integrated in the device during production, as mentioned in [44]. However, since the master key is kept in the device's memory, an attacker can obtain it by reading it there in the event of a successful node capture attempt. A different potential attack drains the energy of the ZigBee nodes. Three ZigBee-based smart lighting systems were demonstrated by the authors in [47] to be vulnerable to a number of attacks, including code injection, denial of service (DoS), and network key extraction.

Using the same 128-bit AES-CCM algorithm as ZigBee, BLE protocol offers authentication and secrecy. Pairing is used to create the symmetric key. In order to authenticate each other; IoT devices must first share the required data. Then they produce temporary keys based on a paring process and exchange those keys with each other.

Resource-constrained devices with the help of 6LoWPAN protocol get connected to the Internet using IPv6 addresses. To cut down on transmission overhead, it employed packet fragmentation and IPv6 header compression. Unfortunately, it does not offer secrecy, authentication, or integrity preservation. Receiver node utilizes injected fragment which results in creation of damaged packet as an adversary injected some fake fragments during the transmission. As a result, the receiver node’s buffer space will be set aside an unable to accept new fragments [53]. Consequently, a DoS attack is noticed due to repeatedly reusing a fragment injection attack [54].

In the packet header, RPL specifies unsecured, preloaded, and authenticated. When the MAC layer provides security, the insecure mode is used. Pre-installed keys are used to connect to RPL in preloaded mode. According to RPL's specification, authenticated mode is not entirely described. On the RPL networks an attacker can carry out several forms of assaults including a sinkhole, black hole, flooding, Sybil, and DoS if security is not provided at any tire [54-56].

Communication at the MAC layer or the application layer must be secure for 6LoWPAN to be secure. With the help of MIC and AES-CCM, the MAC layer is secured. The key management process is not, however, specified in the IEEE 802.15.4 specification.

To ensure data integrity and secrecy, the LoRaWAN protocol used the 128-bit AES algorithm. Two sessions the network session key and the application session key are sent to the end device by the network server when permitting an IoT device to join the LoRaWAN network. Data encryption and decryption as well as MIC are performed with the help of these keys. The LoRaWAN protocol's key management flaw is its fundamental security vulnerability; because session keys are kept on the end device, and the attacker can obtain them through side-channel attacks and discover the communication with all the devices. The LoRaWAN network's susceptibility to man-in-the-middle and DoS assaults was shown by the authors in [58].

1.5.2.3 Application layer threats

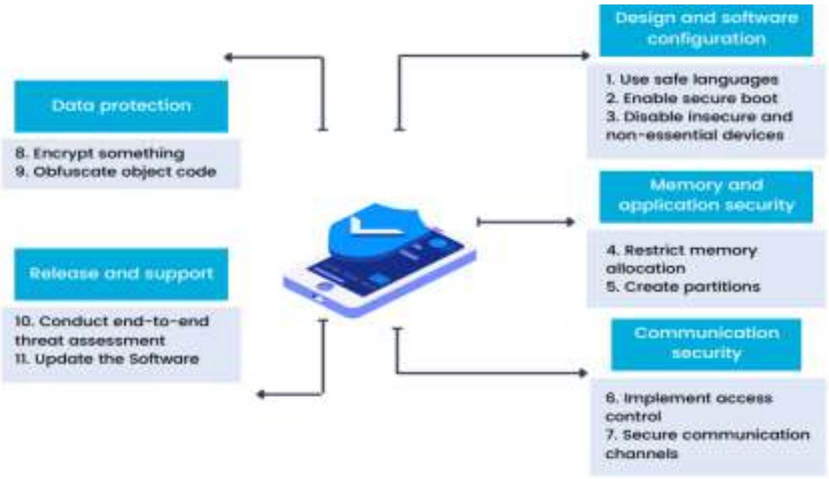
Resource-constrained devices may accomplish RESTful interactions thanks to CoAP, an application layer. CoAP protocol security, however, may be threatened due to DTLS constraints [59]. To encode and decode the data SSL employs asymmetric cryptographic techniques. However, MTM attacks are still possible over SSL [60]. To offer security during data transfer, secure MQTT (SMQTT), an extension of MQTT, was suggested [61]. A private key is given to publishers and subscribers once registered with the broker. This key can be used by publishers and subscribers respectively, to encrypt and decrypt data. Key generation & encryption techniques, however, are not standard.

In the IoT, hackers may take advantage of consumer devices and software flaws. Malicious software can be introduced into an IoT system by an adversary who is impersonating or manipulating legitimate users. Several IoT attacks, including

Bashlite and Mirai assaults, have been caused owing to the absence of user authentication [5].

1.6 Crucial Security Factors for IoT

IoT security requirements divided into three areas is shown in Figure 1.14. Data that IoT devices gather needs to be secured in order to safeguard critical information. To prevent an adversary from influencing data flow, communication of these devices must likewise be encrypted. In certain Internet of Things scenarios, customers can receive cognitive services from physical items that communicate with one another. Therefore, it is essential to protect these devices.



Data protection
8. Encrypt something
9. Obfuscate object code
Release and support
10. Conduct end-to-end threat assessment
11. Update the Software
Design and software configuration
1. Use safe languages
2. Enable secure boot
3. Disable insecure and non-essential devices
Memory and application security
4. Restrict memory allocation
5. Create partitions
Communication security
6. Implement access control
7. Secure communication channels

Figure 1.14 IoT Security Levels

1.6.1 Data security

The Internet of Things (IoT) gadgets constantly monitor environmental settings and send the data they acquire over wireless channels. Yet other security risks, such as eavesdropping and data alteration, might affect the sent data. Data’s integrity, confidentiality, and privacy must all be protected if we are to safeguard it in the IoT setting as can be seen from Figure 1.15.

The technique of keeping sensitive information hidden from unauthorized Internet of Things (IoT) devices [62, 63] also asserted that data privacy is a crucial problem that requires attention is data confidentiality. Given the restricted resources of IoT devices, it is difficult for IoT systems to rely on standard cryptographic algorithms. The authors of [66] recommended the adoption of lightweight cryptographic methods to ensure data safety and secrecy.

A person’s right to privacy includes the right to keep their personal information private and to decide how that information is used [68]. Data integrity guarantees that information has not been changed in transit [62]. It entails preserving the data's consistency, precision, and dependability. To safeguard data integrity, cryptographic hash algorithms like SHA1 and MD5 are frequently utilized. However, these algorithms are frequently unfeasible due to the resource limitations of many IoT devices [70]. Numerous lightweight hash functions have been developed to tackle this difficulty. Additionally, altered data can be found and addressed by error correction methods like checksum functions and Cyclic Redundancy Checks (CRC) [6].

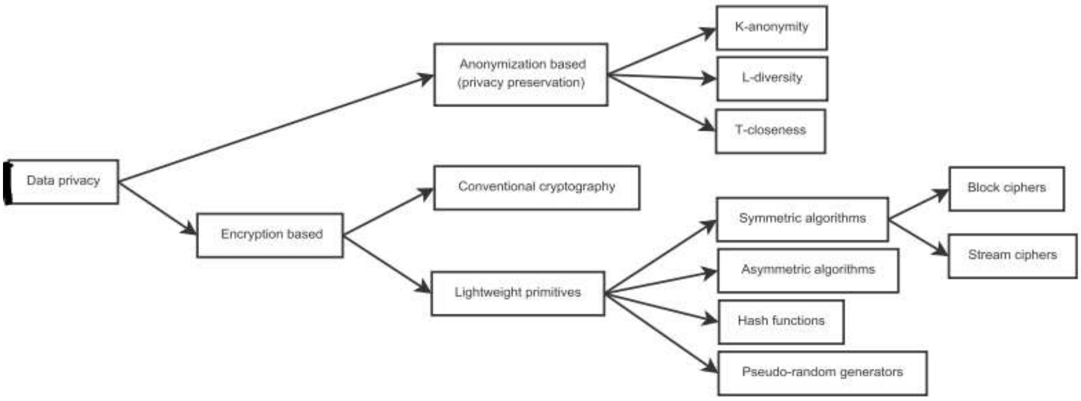


Figure 1.15 Data Privacy Approaches in IoT [38]

1.6.2 Communication Security

An association and message between IoT devices must first go via an authentication method. This means that only approved devices have access to data or systems. Furthermore, the communication also achieves non-repudiation. Verifying an identity with a longing and further information, including a password, PIN, biometrics, and digital certificates, is the process of authentication [69]. In an Internet of Things system, it is required for secure communication between two or more participants. Authentication guarantees that only authorised users can access Internet of Things devices by achieving no repudiation in communications. Before sending data, any new device connecting to the network needs to authenticate itself. Authentication can be confirmed via biometric identity, physical primitives, and low-tech cryptography techniques [73, 74].

A security component called access control ensures that systems and users have the right authorization to access various devices and sources [75]. Non-repudiation is important when it comes to IoT network security [76]. It guarantees that the IoT node cannot retract the message after it is sent, and the recipient cannot retract receiving it [62]. In business contexts, such as digital contracts, non-repudiation is especially crucial since it supports the validation of the legality and veracity of interactions between parties. PKC, or public key cryptography, can be employed to satisfy the non-repudiation security requirements [77].

1.6.3 Device security

Trust and confidence between interacting nodes must be maintained to guarantee security in a critical environment. Also, the availability of IoT devices is crucial. According to [78], trust is essential for IoT consumers. Making choices on how to communicate with unidentified parties is the process of managing trust [79]. Deterministic and non-deterministic trust are the two basic categories into which trust management approaches fall, according to [69]. The non-deterministic trust covers systems based on recommendations, reputation, prediction, and social networks, whereas the deterministic trust includes processes based on policy and certificates. To determine trust, the policy-based procedures employ a set of policies. To define trust, recommendation-based systems make use of historical data. Prediction-based strategies can be utilized if there is no prior knowledge. On one side social network-based systems take into account the entitie’s social reputation, and on the other reputation-based systems use the worldwide reputation of the entities.

As IoT systems may be used in critical sectors like the economy, manufacturing, healthcare, etc. [80], device availability is an essential component of IoT systems [4] States that the availability of the IoT networks must be tested based on both hardware which means availability of the devices constantly and software which means the capability of offering services at any place, anytime.

IoT devices may experience a variety of assaults, including DoS and DDoS, which can impair the availability of the network or interfere with the provision of services.

1.7 IoT Security Solutions

1.7.1 Fog Computing Solution

It was intended to supplement CC's computational capabilities rather than to completely replace them. At the network's edge, it offers networking, communication, computing, and storage [84]. The architecture of fog computing, as depicted in figure

1.16 and explained in [54], is made up of fog nodes that are situated close to IoT devices and are linked to central cloud server.

The quantity of transferred data with cloud infrastructure & IoT devices is decreased thanks to the fog architecture. For real-time or latency-sensitive Internet of Things applications, fog computing is regarded as the perfect solution. Fog nodes meet variety of security requirements, with encryption, privacy protection, & authentication to safeguard resource-constrained IoT devices.

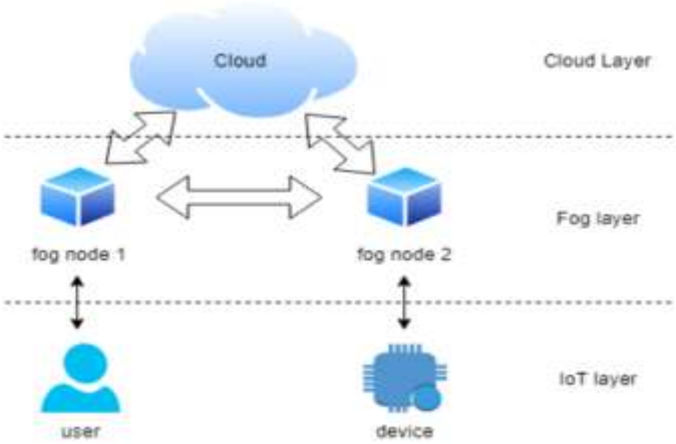


Figure 1.16 Fog Computing Based IoT Environment [54]

1.7.2 Software Networking Solutions

SDN is a unique computer paradigm that divides routing decisions made by network components from the forwarding process, making network administration easier. Figure 1.17 [39] illustrates how the network components govern data forwarding, while a centralised component called the SDN controller handles network administration tasks such forwarding tables and ACL rules.

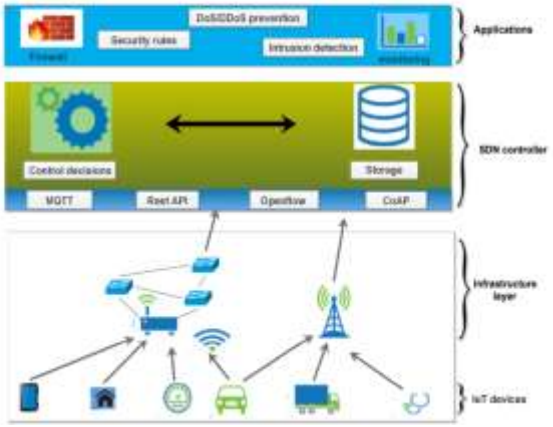


Figure 1.17 SDN Architecture [39]

The SDN can be a useful tool for establishing security, authentication, secrecy, and intrusion detection and mitigation.

1.7.3 Blockchain-based solutions

The revolutionary technology known as blockchain has caused a transformation in the crypto currency business. A distributed ledger or database stores the transactions made by nodes in a p2p network [54].

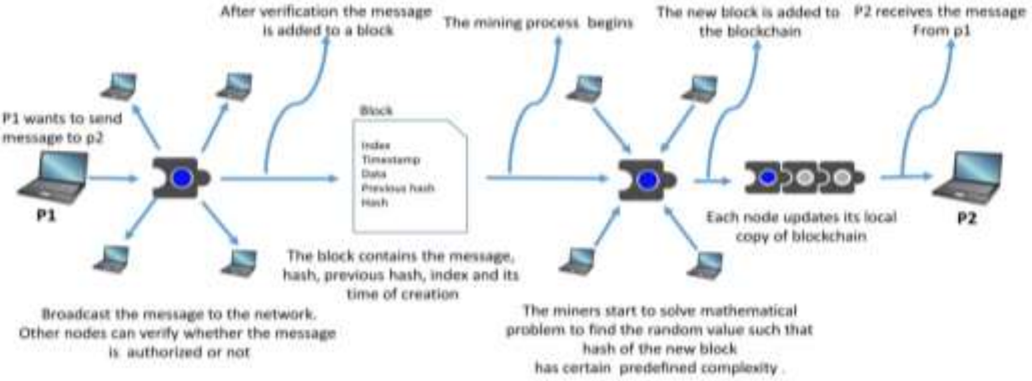

After verification the message is added to a block
The mining process begins
The new block is added to the blockchain
P2 receives the message From p1
P1 wants to send message to p2
P1
Block
Index
Timestamp
Data
Previous hash
Hash
Each node updates its local copy of blockchain
P2
The block contains the message, hash, previous hash, index and its time of creation
Broadcast the message to the network. Other nodes can verify whether the message is authorized or not
The miners start to solve mathematical problem to find the random value such that hash of the new block has certain predefined complexity .

Figure 1.18 Blockchain Working Processes [54]

By combining related transactions into a group, a consensus mechanism is utilised to distribute the validity of a block of transactions. The blocks connected to form a chain of blocks, & their working is given in figure 1.18. Every chunk is separated into parts: validated transactions are in the first part, and block timestamp, nonce value, block hash, and block hash of the previous one are in the second part.

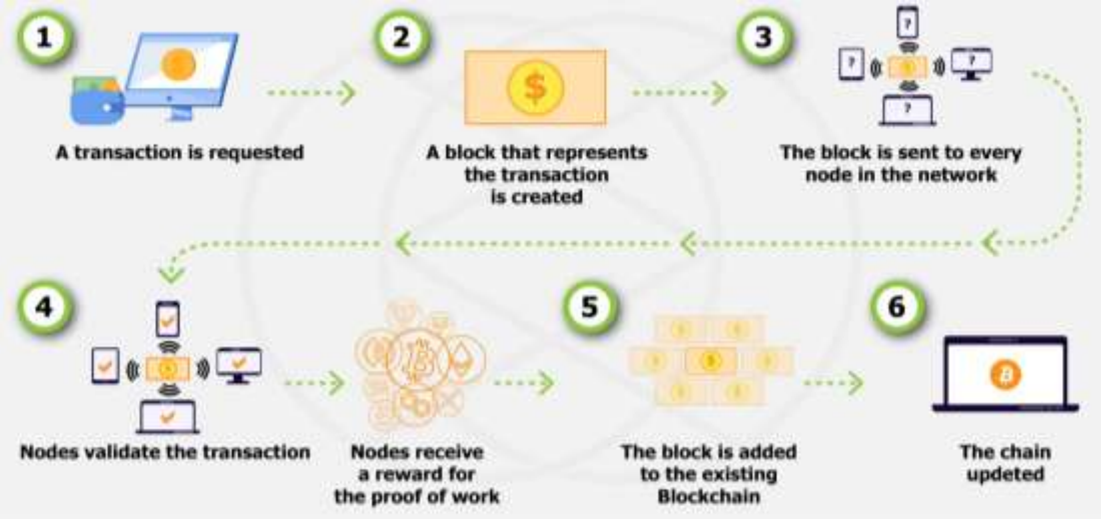

1
A transaction is requested
2
A block that represents the transaction is created
3
The block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the proof of work
5
The block is added to the existing Blockchain
6
The chain updeted

Figure 1.19 Steps of Block chain Validation Process

Nodes in the network carry out the consensus process. PBFT, PoW, & PoS are common consensus methods. With the use of these algorithms, mining nodes can come to an agreement on adding a fresh block to the blockchain. Figure 1.19 depicts the steps involved in validating a transaction using the blockchain.

Public blockchain (permission-less) and private blockchain (permissioned) are the two primary varieties. Only specific nodes are part of the private blockchain whereas any node can join the public network. Popular public blockchain include Ethereum and Bitcoin. The characteristics and needs of an IoT application determine the blockchain type and consensus method that should be used.

1.7.4 Lightweight Cryptography Solution

It is a potent instrument for guaranteeing veracity, privacy, & validity. Unfortunately, complex factors like processor speed, memory size, and battery life are present in most IoT devices. Thus, for low-resource IoT devices, traditional encryption approaches are inadequate. IoT system security has recently been proposed using lightweight cryptographic primitives. The four primary categories of lightweight cryptographic approaches are elliptic curve cryptography, stream ciphers, hash functions, and block ciphers, as illustrated in figure 1.20. By transforming an arbitrary-length message into a fixed-length message, hash functions ensure data integrity.

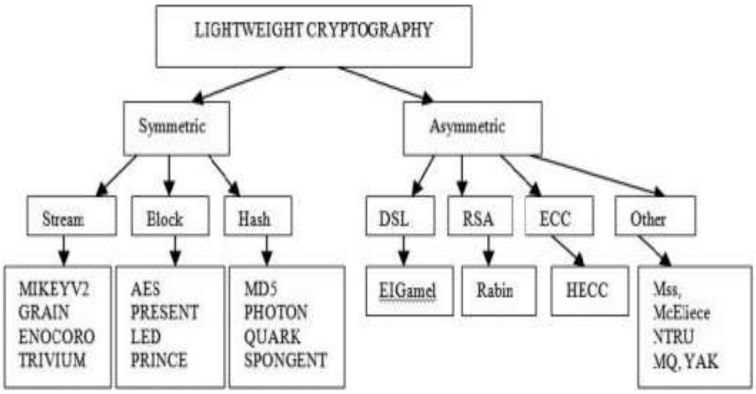


Figure 1.20 Lightweight Cryptography Techniques [92]

1.7.5 Searchable Encryption and Homomorphic Solution

The proliferation of IoT devices is being driven by the wish to enable the development of ever-sophisticated applications. The procedure produces a substantial volume of data, gathered and used for analysis. One application of cloud computing is the processing and storage of data obtained from IoT devices. Safeguarding data from unauthorized access is crucial due to the potential presence of sensitive information inside it. To ensure confidentiality, the gathered data is encrypted before being stored on a public cloud. The fundamental categories of homomorphic encryption are partially & fully homomorphic algorithms. SE enabled secure retrieval of information from encrypted material.

1.7.6 Machine learning-based solutions

IoT devices can now tackle a variety of security risks thanks to a promising method called machine learning (ML). One split of AI used to provide intellectual security solutions with the Internet of Things. A wide range of assaults made against IoT systems can be recognised and countered with ML techniques.

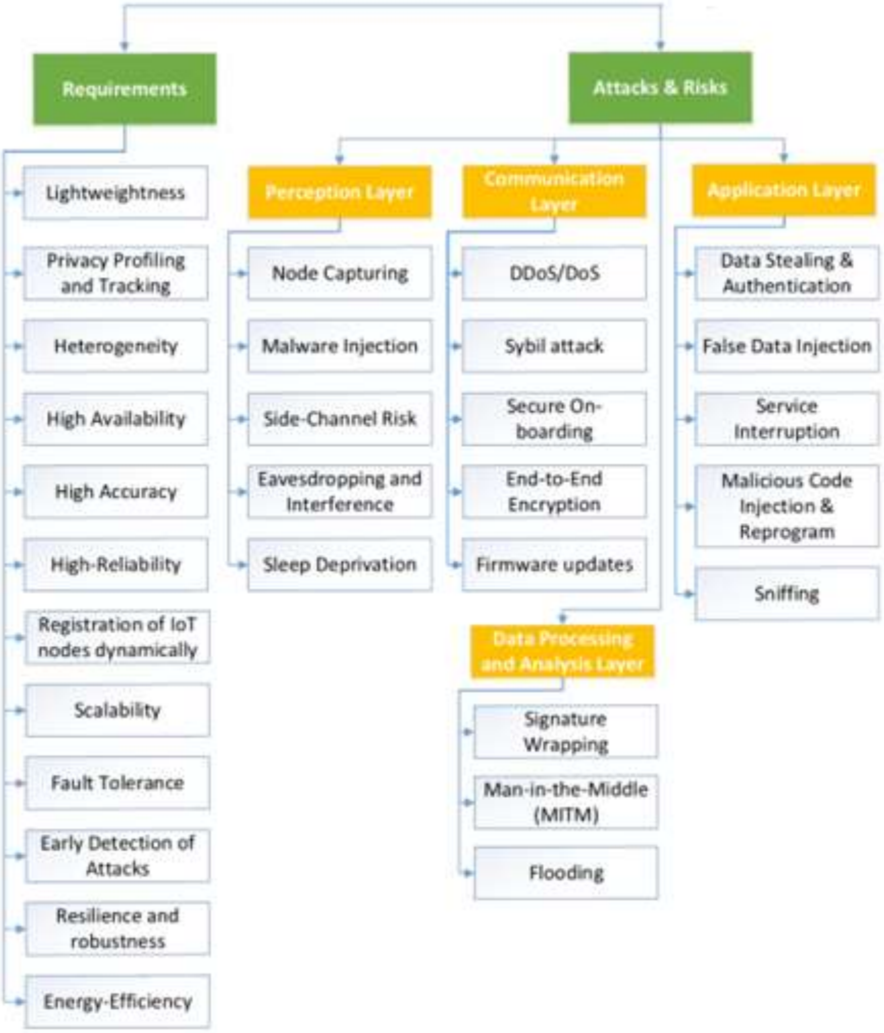


Figure 1.21(a) ML-based approaches for IoT [99]

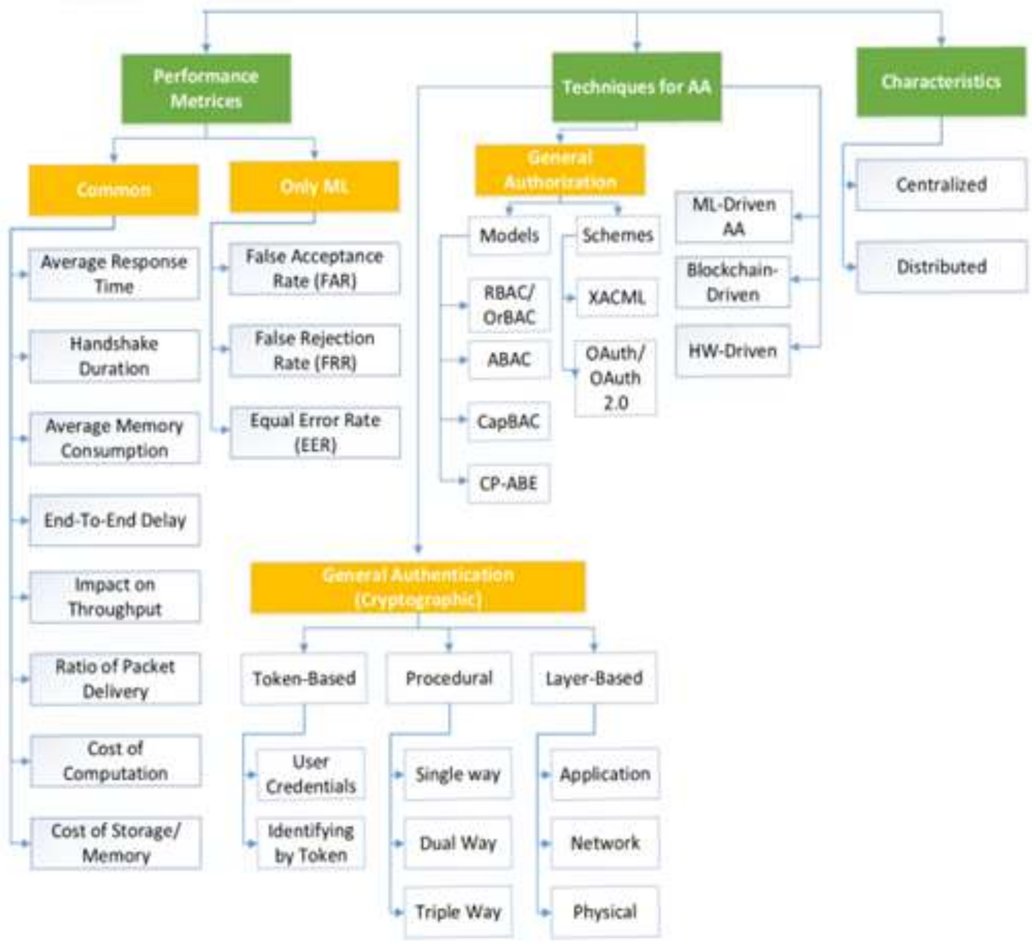


Figure 1.21(b) ML-based approaches for IoT [99]

IoT devices can now tackle a variety of security risks thanks to a promising method called machine learning (ML). One subset of AI is used to provide IS solutions for the Internet of Things networks. A wide range of assaults made against IoT systems can be recognised and countered with ML techniques.

ML-based methods for IoT authentication & authorisation are shown in figure 1.21 [99]. The machine learning algorithms fall into five categories: reinforcement, unsupervised, semi-supervised, supervised, & deep learning. SL techniques like NB,

1.8 IoT Authentication

Safety measures are of utmost necessity in the IoT environment, & authentication is one major concern taking into consideration the damage that can be provided by a malicious unauthenticated object. This section provides a near complete view of the authentication techniques. As seen from figure 1.22 detailed taxonomy for IoT authentication schemes have been explained [55].

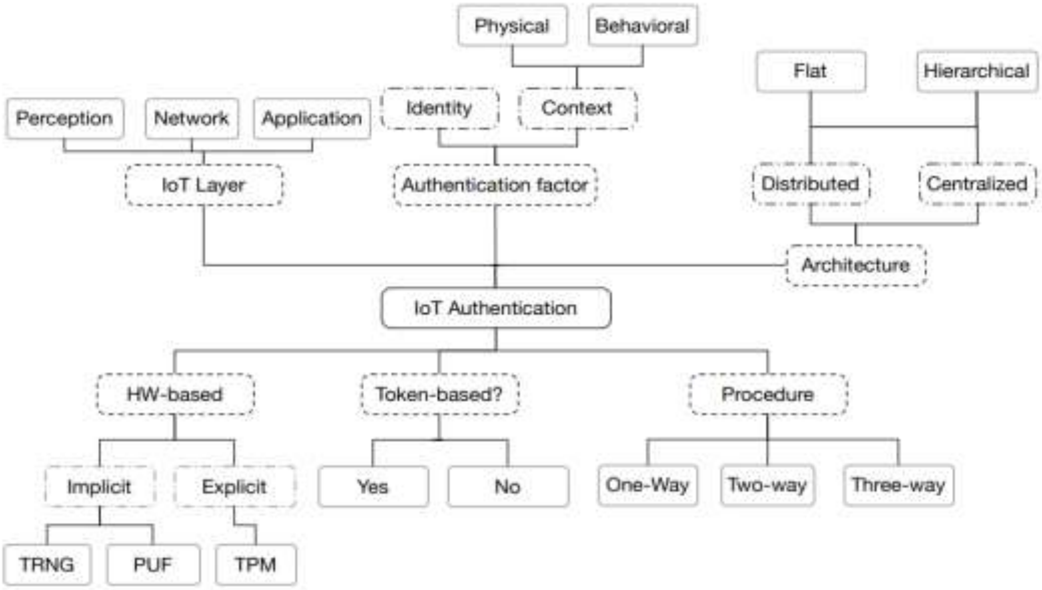


Figure 1.22 IoT Authentication Schemes [55]

A security requirement of IoT depends on the safety needs of the IoT applications. Although, authentication is considered to be the most important requirement of IoT devices as trust between the communicating parties is very important for secure communication. Due to this need for lightweight authentication scheme's emergence took place. A survey of various authentication schemes for IoT has been explained in this section.

1.8.1 Authentication Factor

Authentication factor are credentials provided from one person to another, sometimes combination of more than one parameter validate authenticity of the communicating parties concerned in some kind of communiqué. Various authentication factors include:

i. **Identity:** Identity based techniques uses one of the hash algorithms, symmetric or asymmetric cryptographic algorithms shared between two parties to authenticate themselves.

ii. **Context:** It can be used in two different ways

a. **Physical:** Physical characteristics of an individual like fingerprint, retina scan, hand geometry etc. are provided for ensuring the authenticity of the communicating objects.

b. **Behavioural:** Based on behavioural characteristics of an individual like voice recognition based system, keystroke timing creation when a person types, walking pattern of an individual to represent the biometric characteristics.

1.8.2 Use of Tokens

These are protocols in which encrypted security tokens get generated and help users verify the identity of communicating objects. Finally, receiver side objects provide sender unique value which the sender can use for accessing protected pages and resources for a limited duration of time. Some of the advantages behind using token based authentication include stateless nature, tokens that expire once the session is over, are machine-generated and encrypted, adding a barrier to prevent hacking, etc. Although, all authentication tokens provide users with access to a drive or an application there are several different types of procedures used for the authentication as given below:

i. Authentication on the basis of token: Authentication of a device is done on the basis of a bit of data generated by the server as a third party.

ii. Non-token based authentication: Traditional method of authenticating devices whenever some data to be exchanged with the help of predefined username/password combination which may lead to leakage of the details and the security of the system will be at risk.

1.8.3 Authentication Methods

i. One-Way: In this method one party authenticates oneself to the other party while the second party remains unauthenticated.

ii. Two-way: It is a method where both communicating objects engage in authentication with each other.

iii. Three-way: It is the process in which a third party, known as a centralized one, facilitates the authentication of both communication parties by providing an additional document known as a certificate. This certificate enables the parties to mutually authenticate themselves.

1.8.4 Authentication Frameworks

i. **Distributed Architecture:** Communicating objects are available on different platforms and several objects can cooperate to achieve specific goals or objectives. The communicating parties in this model authenticate each other directly using the distributed structure.

ii. **Centralized Architecture**: Whenever the credentials used for the authentication are distributed and managed by a centralized trusted third party then this framework plays an important role. There are normally two phases of the centralized architecture; one is registration by all the devices to the centralized authority to ensure that all nodes can be uniquely identified. Second is device authentication and communication in which the central authority authenticates the communicating entities with the help of the certificate issued at the time of the device registration and finally once it is verified both parties are allowed to start communicating with each other.

iii. **Hierarchical:**Multi-Level architecture is being used to handle the authentication between the two IoT devices.

iv. **Flat:** Hierarchical architecture has not been used to handle the authentication.

LITERATURE REVIEW

CHAPTER 2

2.1 Introduction

Ensuring security of communication, in IoT devices is crucial given their use and potential access to information. Lightweight authentication protocols play a role in safeguarding communication in devices that have limited resources as traditional cryptographic methods can be too computationally demanding. This review delves into authentication strategies proposed for IoT devices examining their security features, effectiveness, scalability, privacy implications and hardware requirements. By evaluating these aspects we aim to pinpoint avenues for enhancing communication security in resource limited settings.

2.2 Literature Review

In a study conducted by **N. Li et al. [24]** in 2015, a protocol tailored for devices used in smart city applications was introduced. Their protocol strikes a balance with efficiency, communication overheads & security measures. To overcome the shortcomings of protocols on devices they devised an innovative public key encryption system that minimizes computational demands. This system was utilized to develop a mutual authentication protocol with a number of rounds based on security parameters. Through evaluations conducted in software and hardware setups, the protocol exhibited performance enhancements compared to existing RSA and ECC-based protocols at levels of security. Experimental findings underscored the efficiency of the proposed protocol for resource-limited devices and its potential as a solution for communication, in smart city scenarios. In the future, there could be exploration of testing the protocol in a setting, with devices and investigating ways to improve the handling of larger messages.

In a study by **Y. Qiu et. al. [21]** in 2016 an upgraded authentication & key establishment method called EAKES6Lo designed to improve machine-to-machine communications by using cryptography to address resource limitations at 6LoWPAN nodes was introduced. This scheme involved deployment, authentication and key establishment as well as handover phases to verify the authenticity of both stationary and mobile nodes. The security of this approach was confirmed using Protocol

Composition Logic (PCL). MATLAB simulations revealed that EAKES6Lo resulted in transmission overheads compared to existing methods thereby improving efficiency and security during handovers in 6LoWPAN networks.

WSNs components of IoT have become widely used for purposes, like health monitoring, environmental sensing and traffic management. While offering benefits WSNs face security risks that emphasize the importance of user authentication. Recent biometric-based authentication systems have been claimed to withstand types of attacks including dictionary attacks and impersonation attempts. However upon inspection, by **C. Wang [25]** in 2017, it was found that these systems still had vulnerabilities such as dictionary attacks, impersonation risks, lack of user anonymity and no forward secrecy. To overcome these issues an advanced authentication method was suggested. This new approach underwent security validation using BAN logic & heuristic analysis to prove its resilience against threats. A comparison with existing protocols showed that the proposed method offers security & performance. The study stressed the significance of understanding system architecture, adversary models and security needs which are often neglected. This research lays the groundwork for developing authentication protocols in the increasingly interconnected IoT and IoV environments.

In 2017 **S. Challa et. al. [23]** responded to rising security concerns in settings and introduced a signature-based key establishment system to ensure secure user verification. This system focuses on addressing challenges related to user access to device data in application areas like smart homes and transportation systems. Gateways play a role as intermediaries facilitating communication between users and resource-limited IoT devices. The device assumed the adversary of intercepting, altering or deleting messages sent over channels and even physically seizing devices to access sensitive data. Security evaluation confirms that the system adequately defends against threats. Additionally, practicality is a focus of this approach. Researchers conducted simulations using the NS2 simulator to assess system presentation in terms of communication and computational expenses. These simulations illustrate that not only is the system secure but it is also efficient making it suitable for deployment in real-world scenarios within environments with limited resources. When compared to existing authentication methods for devices the proposed signature-based key establishment scheme brings benefits. It achieves a level of security while also being efficient in terms of communication costs. This blend of security measures and practicality positions the scheme as a solution for user authentication, across various IoT applications.

A lightweight authentication scheme was introduced by **F. Wu et. al. [26]** in 2017 to address security issues associated with authentication methods that often do not meet the requirements of wearable device communications. The methodology involves a three-step process; initialization, pairing and authentication. When the wearable device (WD) and the service provider (SP) pair up they establish a connection. During authentication, they create a session key, for future data exchanges. Important identity details are stored in a cloud server (CS) which holds manufacturer-uploaded data and session information from SPs. To ensure communication, separate session keys are used for range (like Bluetooth) and long-range (like WiFi, 4G) connections. The security of this system is confirmed using ProVerif, a tool that checks protocols for their ability to resist attacks and keep session keys secret. Comparisons, with methods, demonstrate that this approach is more practical and efficient. Future plans involve testing the system in real-world settings and exploring group authentication for devices, possibly incorporating public key infrastructure to boost security further.

In 2017 **A. Esfahani et. al. [43]** identified the drawbacks of existing M2M protocols that heavily relied on cryptography and incurred computational costs. They introduced an authentication method specifically designed for resource-constrained devices, in IoT settings. This technique utilized Xor operations to reduce computational, communication and storage burdens. The approach involved two steps; sensor registration with an Authentication Server (AS) and authentication between the sensor and router equipped with TPM.

In 2018, **R. Amin et. al. [35]** tinted the adoption and operation of Internet-connected devices within IoT which emerged as the leading technology in today’s world. The data produced by devices in IoT setups raises significant concerns related to managing and securing vast volumes of information. Cloud computing, also known as CC has become a technology for managing volumes of data efficiently. One of the challenges in this area is ensuring the security of information stored on multiple private cloud servers making it essential. It introduces a model suited for dispersed cloud environments, and presents a smartcard-based authentication protocol that allows registered users to securely retrieve private information from a private cloud server. By utilizing tools like AVISPA and BAN logic for casual cryptanalysis the protocol's strength against security threats is confirmed. It offers an effective method for users to access cloud servers without relying on password verifier tables while allowing for easy password and identity updates.

Research conducted by **M.S. Albela et. al. [33]** in 2018, further supports these findings. In the past, there have been studies on how to secure communications in IoT networks with a focus on dealing with the limitations of IoT nodes. Early research pointed out that traditional security methods were not enough, which led to hardware platforms incorporating hardware-accelerated cryptographic features. Experts looked into using Transport Layer Security (TLS) to boost communication security and compared two common authentication algorithms; ECDSA and RSA. In experiments, researchers downloaded data like a 512-byte JSON file time while tracking energy use and transaction speeds. The results consistently showed that ECDSA performed better than RSA in tests in terms of energy efficiency & processing speed. Notably, improvements in ECC library implementations enabled curves such as secp256r1 to outshine others like secp224r1 at security levels. These discoveries highlighted the potential of ECDSA to meet security needs in setups as RSA key sizes would become less practical with increasing security demands. In the realm of IoT and WSNs, secure data exchange is crucial. To meet this requirement, **S. Jebri et. al. [34]** introduced a lightweight and anonymous mutual authentication algorithm named LTAMA back in 2018. This algorithm was designed to establish trust and ensure data confidentiality, between communicating entities while safeguarding their identities. LTAMA utilizes IBE PKG and ECC to ensure anonymity and secure creation. The protocol has three phases; setup, authentication execution using the LTAMA algorithm and establishing a shared session key. An analysis of its security shows that the selected cryptographic methods along with hashing functions effectively provide anonymity, trustworthiness and data protection. The security of LTAMA was further confirmed through testing with AVISPA tools. This study introduces a secure mutual authentication solution tailored for WSN environments with limited resources.

In 2018 **E. H. Teguig et. al. [31]** delved into the challenges of management and authentication in securing WSNs used in IoT applications. They focused on countering man-in-the-middle attacks while minimizing energy usage and resource consumption, on sensor nodes with capabilities. To tackle these issues they introduced ECC_ASV as a solution leveraging ECC to enhance network security. ECC_ASV emphasizes both security effectiveness and operational efficiency by establishing a secure communication pathway among sensor nodes through network deployment, neighbourhood recognition and an encryption-decryption process accompanied by signature verification. By utilizing ECC, ECC_ASV achieves this level of security while also being efficient in terms of time making it a good fit with Internet of Things (IoT) environments with resources.

S. Dey et. al. [44] in 2019 a new method for establishing session keys was proposed to enhance the security of communication among home devices. This innovative approach addresses the shortcomings found in studies by striving to find stability in safety & efficiency for devices with resources. Unlike methods that required service provider availability or resulted in high communication overhead the proposed method utilizes the DHK swap method for secure key establishment. Additionally, it incorporates Silicon IDs for device authentication removing the necessity for registration with service providers or manufacturer involvement in the authentication process. Formal analysis conducted using AVISPA (SPAN) has confirmed that this method successfully achieves its goals of authentication and confidentiality. Furthermore, performance analysis indicates that this approach maintains a design similar to previous works making it well-suited for deployment, in resource-limited smart home environments. The authors intend to validate their research through simulation or experimental studies in endeavours.

Y. Chen et. al. [46] introduced a mobile payment system in 2019 tailored for IoT emphasizing user isolation & efficient use of device resources. Unlike solutions, this innovative protocol strikes a balance between these two aspects. At its core is a unique one-way certificateless proxy re method that not only enhances mobile payments but also offers additional benefits. By employing this method a trusted Pay Platform can serve as an intermediary for users in transactions with merchants safeguarding user identity. Moreover by offloading tasks to the Pay Platform, which typically has computing power the protocol lessens the burden on resource-limited smart devices. To tackle scalability concerns related to handling a user base the researchers incorporated batch verification techniques for the Pay Platform and Merchant Server. These techniques notably reduce processing time for verifying signatures. Through security assessments based on the Computational Diffie Hellman problem, they've demonstrated the protocol's resilience against attacks. Performance evaluations have also validated its effectiveness in environments with resources. Comparative analyses with existing protocols underscore the practicality and efficacy of their proposed solution offering an avenue for user-friendly mobile payments, within the IoT landscape.

In 2019 **S. Banerjee et. al. [48]** put forward mechanisms for secure user authentication. A new user authentication system was recently introduced, incorporating card, password and personal biometric data verification. Notably, this protocol does not store user information at gateway nodes. Its security was rigorously tested using models and simulation tools showing its effectiveness as per safety, functionality and efficiency. The authentication process involves setup, registration, operation and maintenance stages, with features like dynamic device enrolment and anonymous user login. While simulations have shown promise, real-world implementation and evaluation are research goals.

In the realm of IoT wireless body area networks played a role to collect physiological data from wearable or implantable devices for healthcare purposes. However the openness and mobility of these networks expose them to privacy breaches and information theft by actors. Existing authentication methods relying on asymmetric encryption face challenges due to resource limitations of sensor devices.

In addition, numerous simple authentication methods lacked the feature of secrecy, which raised security concerns. To tackle these issues a safe lightweight verification method was projected by **Z. Xu et. al. [50]** in 2019, for WBANs. The method ensured familiar privacy with no reliance on encryption The design of the scheme involved utilizing parameter PKs to ensure forward secrecy and included three phases, Initialization, registration and authentication. With system administrator (SA) involvement in the two phases and secure information exchange between sensor nodes (SN) and the server during the authentication phase.

To overcome these limitations in 2016 proposed solutions the iLACKA IoT protocol, developed by Choudhari has been suggested as an enhanced approach. This updated method has shown resilience, against threats, backed by formal validation using the ROR model & informal security analyses. Performance assessments have indicated that iLACKA IoT not only boosts security but also improves efficiency cutting down computation and communication costs by around 39.7% and 12% respectively compared to LACKA IoT. The proposed iLACKA IoT protocol has significantly speed up the access control and key establishment phases showcasing its potential for implementation.

In a study by **Y. Chen et. al. [46]** in 2019 it was observed that recent research has introduced methodologies to develop security & isolation in mobile payment systems within the realm. One noteworthy approach involved creating a certificate less proxy re scheme as the basis for a novel mobile payment protocol. The authors put forward a protocol that achieved both anonymity and enforceability while minimizing resource usage on devices effectively. By delegating tasks to the Pay Platform with ample computational resources efficiency was notably enhanced. Moreover, batch verification techniques were utilized to tackle scalability concerns enabling computations.

Protocol security was officially confirmed through a security analysis regarding the CDH problem with performance assessments showcasing its practicality and effectiveness, for IoT devices with limited resources. This comprehensive method guaranteed user privacy and transaction integrity effectively meeting security needs in mobile payment systems.

The realm of sensor networks (WSNs) & their advantages in IoT have seen significant progress. However, ensuring data security in WSNs has emerged as an issue demanding user verification methods. Past authentication protocols for medical sensor networks (WMSNs) often fell short in enabling password changes and forward secrecy while defending against threats like stolen smart card attacks. To address these limitations **X. Li et. al. [79]** proposed ECC-dependent 3-factor verification protocols with privacy for WMSNs in 2020. The protocol's security underwent rigorous assessment, through security techniques the Proverif tool and information analysis. In comparison, to protocols the new solution was found to be strong and reliable successfully safeguarding against threats like losing a device exposing sensor keys and preventing denial of service (DoS) attacks caused by message substitution. By incorporating elliptic curve cryptography (ECC) this protocol achieved forward secrecy marking advancement in security and efficiency, for WMSN systems compared to versions. To meet demand for secure procedures a fresh mutual authentication protocol that merges RC5 & ECC was introduced and put into action on Zolertia RE IoT gadgets. The protocol, devised by **Y. Yilmaz et. al. [51]** in 2019 achieved the transmission of data and mutual authentication through two communication connections Leveraging ECDSA for data validation & ECDH for generating secret keys further bolstered the security and efficiency of the protocol.

W. Liu et. al. [66] 2020 presented a remote multi-feature verification scheme considered for crowd-sourced IoT applications to address shortcomings found in current methodologies where authentication factors solely encrypt a local secret key. The suggested plan utilizes the user’s individuality, password & biometrics to authenticate by the server. These elements also play a role, in establishing a shared key through maps, zero-knowledge proofs and fuzzy extractors. This approach guarantees that confidential user data remains protected during authentication. The security assessment employing the ROR model BAN logic and ProVerif has confirmed the system's resilience against attacks.

In advancement aimed at enhancing user authentication security in settings, **S. Banerjee et. al. [52]** introduced a novel lightweight protocol in 2019 that emphasizes user anonymity and resilience against physical device compromise. This protocol addresses security issues faced by resource-constrained devices by leveraging Physically Unlovable Functions (PUFs) – unique identifiers embedded in each device that are resistant to cloning attempts. This distinctive feature significantly boosts the protocol's security stance, in situations where attackers may try theft of devices or copying credentials. To thoroughly evaluate the protocol's effectiveness in enhancing security measures researchers took an approach. In 2020 researchers conducted a security assessment using the ROR system to assess the strength of protocols. They also used the AVISPA tool, for software-based verification to detect security vulnerabilities. Additionally, they employed security analysis through thought experiments and protocol inspection to further investigate weaknesses.

T. Alladi et. al. [80] presented a lightweight verification and attestation system in 2020 for verifying vehicle Electronic Control Unit (ECU) firmware during transit. The methodology involves a four-phase protocol; initialization, registration, vehicle RSU authentication and attestation. The OBU of the vehicle authenticates with RSUs connected to edge servers for ECU firmware attestation. Security of protocol was established through analysis & ProVerif tool demonstrating its resistance against attacks.

In 2020 **B. Hammi et al. [57]** presented research findings that in the past, researchers have pointed out that IoT has presented safety and privacy challenges in various applications worldwide. To tackle these issues previous studies have investigated authentication methods such as one-time passwords (OTP). However, they discovered that enhancing security involved expanding the OTP concept using curve cryptography (ECC) and isogeny. This new method created keys for each communication exchange between devices and servers enhancing security without relying on counters or timestamps as synchronous OTP approaches do. Additionally, devices with limited resources. A comparison with HMAC-based OTP & time-based one-time passwords further highlighted the superiority of the planned approach. This study shows promise in bolstering security within environments that can be applied across various IoT applications, like smart parking and waste management contributing to the progress of smart city initiatives.

Research conducted by **S.S. Ullah et. al**. **[82]** in 2020 after consideration it has been noted that Named Data Networking (NDN) is seen as an approach for efficiently sharing content in IoT networks especially when addressing data security issues such as content tampering attacks. To address this concern experts have introduced a signature system based on identities that is specifically designed for NDN environments. This system used Hyperelliptic curves to ensure security to well-known cryptographic methods like RSA and ECC but with smaller key sizes. The effectiveness and practicality of this proposed system were confirmed through both informal security assessments. Performance tests illustrated its superiority in security & efficiency compared to existing techniques. By utilizing tools like the AVISPA with models like the Oracle model (ROML) it was demonstrated that this system provides verifiable security against various attack scenarios. Furthermore, actual implementations in smart city applications based on NDN highlighted how this solution can be applied effectively in real-world situations. The rise of devices & IoT has emphasized the significance of data transmission between IoT networks and remote users.

In 2021 a team led by **D. Sadhukhan [93]** introduced a user authentication system based on ECC with three factors. This system was specifically designed for devices emphasizing the protection of privacy and data confidentiality. Comparisons of communication overheads revealed that this scheme is more lightweight compared to existing protocols. Security assessments using the AVISPA simulation tool further validated its ability to withstand security threats. The scheme consists of five phases; registration, login, mutual authentication and session key negotiation. It effectively balances security and resource efficiency in environments by establishing mutual authentication between users and IoT nodes through gateways.

The increasing prevalence of IoT has highlighted the need for data access & communication for both users and sensors. While there are authentication methods many struggle to guarantee the privacy of unattended sensors against potential attacks or tampering incidents due to resource limitations. In response, a recent article, by **Z. Liu [69]** and colleagues in 2020 introduced a security protocol aimed at improving security and efficiency. This protocol utilizes functions (PUF) for physical security and combines three factors, Personal biometrics, smartcard and password. To enhance overall security measures. In their 2020 work**, X. Lu et. al. [81]** pointed out that traditional encryption schemes often relied on devices for data encryption/decryption processes leading to communication and computation challenges. This scheme leverages identity-based broadcast encryption to protect patient privacy while allowing authorized access to shared data. Additionally, it incorporates an integrity verification mechanism to prevent users from accessing corrupted data. The utilization of a trusted Security Mediator (SEM) enabled the creation of data blocks and block tags leading to a decrease in the workload on patients. This strategy not only safeguarded data privacy from trusted parties but also guaranteed that solely authorized individuals could retrieve the raw health information showcasing its usefulness, in real-life IoMT settings.

In 2020 a study, by **M. A. Khan et. al. [76]** introduced a framework that starts with verifying the identity of patients and activating sensors to monitor their vital health signs. This system combined data with user credentials and employed the SHA 512 algorithm. To secure data transmission the framework used both Substitution Caesar cipher and an enhanced Elliptic Curve Cryptography (IECC) approach. The improved ECC method included a key for added security measures beyond the standard public-private key pair setup. The proposed technique exhibited performance with reduced costs and efficient encryption/decryption processes. Statistical analysis indicated a security level with an average correlation coefficient of 0.045.

On a note **S. Zhang et. al. [75]** in 2020 recognized the need for authentication methods for underwater acoustic networks (UANs) due to their unique challenges and the sensitivity of collected data. Current authentication schemes designed for resource-constrained systems fell short in UANs settings leading to the development of an approach. Authors have proposed a scheme for users, on chaotic maps & leveraging the DLP & DHP. The scheme makes use of tools to achieve shared verification and key agreement. Presentation analysis shows the scheme offers efficiency and robustness compared to schemes designed for resource-constrained environments. The authentication process includes an authentication mechanism using smart cards' random number mechanisms for user anonymity as well as timestamp mechanisms for ensuring message freshness. This novel approach does not provide a secure & efficient validation solution for UANs. In 2020 **C. Trinh et. al. [63]** highlighted a growing focus among researchers on enhancing the security of IoT devices in scenarios involving resources like RFID tags and WSNs. They conducted analyses to reveal vulnerabilities in existing lightweight and lightweight protocols such as KSP, SOVNOKP, LBRAPS and LRSAS. The research studies uncovered weaknesses such, as vulnerability to disclosure, resynchronization and traceability attacks. To address these issues a new protocol called LBCbAP was introduced, utilizing the CRAFT block cipher as its primary security component. The protocol underwent security evaluations using approaches to confirm the ability to withstand passive and active attacks. Moreover, performance assessments showed that LBCbAP was more cost-effective compared to protocols offering enhanced security and efficiency.

In today’s world of internet usage and Industrial Internet of Things (IIoT) technologies, safeguarding real-time data transmitted over networks has become increasingly important. To tackle this challenge various user authentication techniques have been developed. One such method introduced by **J. Srinivas [78]** in 2020 involved a user-authenticated agreement scheme that utilized fuzzy extractor technology for verification. This approach incorporated cards, passwords and personal biometrics to heighten security measures. The scheme allowed for device registration password/ updates and smart card deactivation to ensure resilience against diverse threats. Official security evaluations showcased the scheme's ability to resist replay attacks. Furthermore, the NS2 tool was used to compare how the approach performed against other methods showing its effectiveness in terms of speed and delay. Studies found that this approach was better than others in terms of protecting information, communication and costs making it a top choice for efficient user verification in IIoT settings. Remote authentication plays a role in ensuring reliable identity confirmation in the realm of IoT. Conventional methods that rely solely on software-based verification are often weak to cyber-attacks because of the limited capabilities of embedded procedures. To address these weaknesses, a verification protocol utilizing Physical Unclonable Functions (PUFs) was introduced by **B. Zhao et. al**. **[77]** in 2020. This protocol utilized the responses of PUFs as the identity foundation of terminal devices. The objective of this method was to enhance security against attacks and prevent tampering during authentication procedures. Known as ePUF this novel terminal authentication system integrated an identity-based encryption approach to safeguard authentication making it lightweight, adaptable and suitable for environments.

In 2020 **K. Park et. al**. **[68]** presented LAKS NVT, a method for IoT that eliminates the necessity for a vulnerable server verification table. Despite performing to existing schemes LAKS NVT offered security features. NS2 simulations further substantiated its suitability for deployments in world medical IoT scenarios. LAKS NVT emerges as a solution for ensuring communication security in IoT networks.

J. Yu et. al. **[58]** proposed an innovative approach that combines a description of CPABE & KPABS to create an access policy. One key advantage of LH ABSC is its signature size, which helps reduce communication, for IoT devices with limited resources. Additionally, the scheme smartly delegates tasks such as signature generation, verification and decryption to fog nodes. Doing it lessens the load on IoT devices while keeping latency low. Thorough security analysis has shown that LH ABSC provides assurances of message confidentiality, enforceability and verifiable outsourced decryption. In essence, this study presents a solution for ensuring data confidentiality and authenticity in fog-assisted environments by striking a balance between security and efficiency.

In another development in 2020 **M. Nakkar et. al. [72]** projected an authentication protocol tailored for edge-based applications that offer forward secrecy. Designed for the expanding IoT this protocol reduces latency in applications. The protocol makes use of hash chains, authenticated encryption methods and session keys generated from hash functions to enhance resilience against quantum attacks without relying on master keys. The researchers introduced an emergency system scenario where a local application sends out messages to groups of responders. They formally demonstrated the security features in terms of security & performance. The findings indicated that the protocol has complexity, minimal storage needs and little communication.

In 2020 **P. Zhang et. al**. **[61]** introduced a layer (PHY) authentication framework tailored to secure communication among IoT devices within smart city settings. The structure employs a method called tag embedding and verification to achieve authentication. In this process, a designed tag signal is integrated into the signal transmitted by the device separate from the actual message signal. The recipient then extracts this tag signal using detection techniques to verify the sender's authenticity. To safeguard against forgery attempts by adversaries the framework employs two sets of keys; one set encrypts the authentication tag with complexity while another set secures the message signal with potentially higher complexity. This dual key strategy strikes a balance between security and computational efficiency, which is crucial for devices, with limited resources. The researchers expanded their models to evaluate how well their framework performs in verifying identities across a range of tag signal scenarios. Using matrix analysis and composite hypothesis testing theories they were able to determine the chances of alarms (FA), and missed detections (MD), in different situations. To validate their framework they carried out experiments that confirmed the accuracy of the models. These experiments also looked into how the framework responds to impersonation attacks under varying system parameters offering insights for real-world applications.

P. Tedeschi et. al. [60] introduced LiKe, an agreement protocol, without certificates specifically designed for devices with limited resources in the IoT field. The protocol aims to overcome drawbacks of solutions that face issues like message complexity, computational requirements and significant energy usage. LiKe, utilizes public key cryptography (CL PKC) to enhance security against leaks of confidential data stored on TTP. A key feature of this protocol lies in its use of materials enabling functionality even when there is intermittent connection to the TTP. Moreover, it supports easy rekeying processes. Provides protection against impersonation attacks under circumstances where TTP details are compromised. The researchers carefully assessed the security aspects of LiKe using analysis tools. They also put the protocol to test on devices in an 11-node network setup. The outcomes revealed that LiKe can establish session keys on each device within 3.259 seconds while consuming 0.258% of the battery capacity. Showcasing efficiency for energy-constrained IoT environments.

A. Diro et. al. [70] in 2020 introduced a security method for communication in the Internet of Things (IoT) setting. They recognized that standard security protocols such as TLS can be too demanding for devices with resources. Their solution involves delegating tasks and storing security parameters to nearby fog nodes easing the burden on the devices. By merging ECC & AES CCM for message encryption they strike a balance between security and efficiency. This strategy minimizes communication overhead compared to TLS-based methods by requiring handshakes and message transmissions per session (184 bytes versus 332 bytes for TLS). Furthermore, it reduces memory usage on devices by transferring storage responsibilities to fog nodes. Overall this approach ensures end-to-end communication while conserving resources making it ideal for resource-limited applications.

Furthermore in 2020 **G. S. Gaba et. al. [71]** projected an RLMA tailored for securing communications in environments, like smart homes and buildings. This innovative scheme overcomes the challenges posed by methods that often demand computational resources from resource-constrained devices. RLMA utilizes ECC certificates & symmetric encryption to establish efficient authentication. Security assessments conducted using both AVISPA) and methods demonstrate RLMA's ability to withstand a wide array of attacks. Performance evaluations show that RLMA not only ensures security but also consumes energy and computational resources compared to current solutions. These qualities position RLMA as an option for securing communication in smart home environments. The authors intend to expand their research to incorporate user authentication within the Internet of Things in studies.

In 2020 **S. Atiewi et. al. [73]** tackled data security issues in cloud-based IoT architectures by proposing a multi-factor authentication approach employing cryptography. Their proposed system makes use of a hybrid cloud setup that merges public clouds. IoT device data is classified and encrypted using a blend of RC6 and Fiestel algorithms, for security measures. This encrypted information is then safeguarded in the cloud for protection while non-sensitive data is encrypted with AES before being stored in the public cloud. To ensure access control the system incorporates a three-tiered factor authentication process overseen by a Trusted Authority (TA). Users must provide escalating levels of identification for levels of access. Evaluation based on metrics like computation time and encryption/decryption times showed that the projected method responds better than existing solutions. In summary, this study presents an efficient approach to managing security for data in IoT environments integrated with the cloud.

In response to the increasing security concerns in Industry 4.0 settings arising from communication channels among Internet of Things (IoT) devices, **G. S. Gaba et. al**. **[71]** in 2020 introduced a lightweight key exchange protocol called LKE. This protocol tackles the challenge of establishing sessions in environments by using ECQV implicit certificates to build trust and generate keys, among legitimate IoT nodes. It combines symmetric key cryptography keyed hash functions and nonce to secure message exchanges effectively while preventing access, forgery, replay attacks and impersonation attempts. The AVISPA tool analysis shows that LKE can withstand types of attacks such as impersonation, replay and man-in-the-middle attacks. Additionally, the efficiency of the protocol is highlighted by its communication and computation processes based on a set of cryptographic operations. Performance testing indicates that LKE performs better than solutions in terms of efficiency making it a good option for resource-limited industrial IoT networks.

In 2020 **L. Wang et. al. [74]** introduced an authentication system with dynamic key generation to address increasing security challenges in FC communication for future IoT systems. This system overcomes limitations seen in approaches that restrict the devices and communication protocols in FC setups. The new method emphasizes security and scalability by utilizing authentication protocols and layer dynamic key generation to establish secure communication links, across various fog devices. It combines hash functions, encryption and random numbers to enable session key creation and user anonymity. Notably, pseudonyms are updated during each authentication process to enhance device anonymity further. To validate the system's effectiveness researchers conducted an assessment covering security and performance using metrics. The analysis findings indicate that the system offers protection against attacks while keeping computational requirements low. This equilibrium between security and efficient design makes the system ideal for fog computing setups with resources, where both security and resource optimization are crucial. In essence, this study presents a method to enhance communication security in IoT systems using fog technology.

In 2020 **W. C. Wang et. al**. **[83]** devised an authentication method named SLATE to cater to the increasing security. Traditional solutions like functions (PUFs) and lightweight encryption methods often come with high hardware costs or vulnerabilities. SLATE offers a solution by reducing the required space compared to these approaches. By utilizing existing storage techniques from encryption methods and eliminating the necessity for dedicated CRP (challenge-response pair) storage found in typical PUFs SLATE stands out as highly hardware efficient. Implementations have shown a reduction in footprint size ranging from 3.1 to 7.1 times when compared to secure PUFs available on the market. When compared with encryption methods SLATE exhibits a 40% decrease in required space resulting in considerable cost savings. The evaluation of security measures indicates that SLATE has shown resilience, against known attacks targeting Physically Unclonable Functions (PUFs) and logic obfuscation techniques, including model building and Boolean satisfiability attacks. Moreover, SLATE has been proven to offer information security when transmitting challenge response Pairs (CRPs) over unsecured channels.

S. Garg et al. [59] specifically tailored to tackle security issues in resource-limited IoT devices utilized in Industry 4.0 scenarios. This protocol adopts a strategy where a central server manages the majority of the authentication tasks thus reducing the workload on individual IoT nodes. To achieve its nature the protocol incorporates primitives such as ECC, PUFs and hash functions. Additionally, performance evaluations have shown that this proposed protocol exhibits communication overhead compared to existing solutions. The blend of security measures, design and optimal performance positions it as a promising choice for bolstering authentication and key agreement, in resource-constrained IoT environments.

F. Farha et. al. **[91]** 2021 a team introduced a yet method for verifying the identity of devices with limited resources in cloud-connected Internet of Things (IoT) settings. They capitalized on the features of values in static random access memory (SRAM) which share qualities suited for Physically Unclonable Functions (PUFs). SRAM PUFs offer benefits such as unpredictability, reliability and resistance to tampering making them well-suited for identifying devices in scenarios. The proposed method uses challenge-response pairs (CRPs) to authenticate. Challenges are sent as memory addresses & corresponding responses are the values of specific SRAM cells. This strategy reduces load and memory needs aligning with the constraints of devices with resources. A Bose Choudhuri Hocquenghem (BCH) error correction code was applied to improve the reliability of extracted fingerprints. Experimental findings validated the effectiveness of this method in verifying devices with limited resources. Its low computational requirements and small memory usage make it an attractive solution for ensuring secure entity authentication, in resource-constrained setups.

B. H. Taher et. al. **[89]** in 2021 researchers acknowledged the importance of user authentication methods, in settings to safeguard real-time private data accessed through wireless devices. They introduced a lightweight three-factor authentication (3FA) system that combines user biometrics, passwords and smart devices. This system utilizes hash and XOR operations for authentication, session setup and key freshness assurance. Protocol structure Covering registration, precomputation, authentication and key agreement processes as password changes showcased its practicality for IoT WSN applications by ensuring secure, efficient and user-friendly authentication procedures. Responding to the growing security challenges stemming from the adoption of IoT and cloud computing, in cities.

In 2020 enhancements were made to an authentication protocol for devices to tackle counterfeiting attacks. However in 2021 **H. Huang [94]** and colleagues discovered vulnerabilities in the protocol including susceptibility to offline password-guessing attacks. To address these concerns, a pseudonym identity-based authentication and key agreement protocol using cards was introduced. This protocol utilized hash functions and XOR operations to meet the limitations of devices. The security of the protocol was validated using AVISPA and Scyther tools demonstrating its effectiveness against types of attacks such as replay attacks, password guessing attacks, man-in-the-middle attacks and session key disclosure attacks. Additionally, a thorough cryptographic analysis of authentication paths among participants ensured protection against impersonation attempts. Comparative assessments of security features and computational performance indicated that the proposed protocol surpassed existing ones in terms of efficiency and security for deployment, in distributed cloud computing environments within cities.

Industrial control and automation systems play a role in manufacturing processes, where a variety of IoT devices gather large amounts of data for real-time processing. In a study by **J. Xu et. al. [99]** in 2021 they highlighted limitations in data streaming methods, their lack of support for range queries and practicality in real-world scenarios. To address these challenges and enable verifiable range queries in data streaming a new method called the chameleon authentication tree with prefixes (PCAT) was introduced. This innovative approach builds on existing techniques to create a solution that can handle expansion and range queries while being suitable for devices with limited resources. The PCAT process involves stages such as initialization, data appending, querying and verification all designed to meet security standards, for data streaming authentication. Security assessments confirmed that the PCAT fulfils all VDS security requirements while also showcasing efficiency and performance metrics. Compared to existing methods the PCAT excelled in a range of query tasks showcasing its potential to enhance control and automation systems significantly.

In response to the increasing security concerns related to the integration of IoT, edge computing and cloud computing **A. Shahidinejad [92]** introduced Light Edge in 2021. This authentication protocol is tailored for resource-limited devices operating in edge environments. The architecture consists of three layers with a trust centre positioned at the edge layer. The trust centre's key function is to assign a trust value to each device and secure communication channels among devices, the cloud and itself. Through evaluations comparing Light Edge with existing protocols, it was proven that Light Edge excels in resisting attacks, optimizing communication costs and reducing authentication process time. These results indicate that Light Edge shows promise as a secure and efficient authentication solution for networks promoting secure communication within the evolving landscape of edge computing.

In another study by **S. Banerjee et. al. [97]** in 2021 addressed the challenge of ensuring authentication for devices in fog computing environments prone to fog node failures. Their work proposes an authentication mechanism that initiates fast re-authentication with a secondary fog node following an authentication process. This mechanism proves advantageous when an IoT device unexpectedly loses connection, with its primary fog node. The proposed scheme's security underwent comprehensive evaluation using a faceted approach. The researchers first conducted an analysis using the Real or Random (ROR) model. Next, they carried out a security assessment. Finally, they utilized the AVISPA software tool, for security validation. These evaluations aimed to showcase the resilience of the system against known attacks. To evaluate how efficiently the system operates the researchers performed experiments to measure the execution time of cryptographic methods used in the protocol leveraging the MIRACL library. These tests offered insights into whether the system is suitable for devices with limited resources. Additionally, a comparative study was conducted to highlight the benefits of their proposed approach compared to methods. This comparison focused on security features, functionality, communication load and computational load. The findings revealed that their proposed approach provided re-authentication with reduced overhead in comparison to public key authentication schemes positioning it as a strong contender for securing IoT deployments in fog computing environments.

In 2021 **A. Sahu et al. [96]** addressed security issues in E-healthcare communication, by introducing a lightweight multi-party authentication and key agreement (LMPAKA) protocol. In a study, researchers aimed to address the challenges of two-party authentication methods, in IoT-based healthcare settings involving patients, devices, doctors and cloud servers. Their new LMPAKA protocol uses lattice-based cryptography, particularly identity-based encryption (IBE) to establish secure party authentication. The authors thoroughly evaluated the scheme's security, performance and feasibility. They validated its security properties with the Scyther tool. Tested its resilience against various attacks compared to other methods. Practical experiments using IBE confirmed the protocol's applicability in real-world healthcare contexts. The analysis also revealed power consumption compared to existing alternatives. The LMPAKA protocol presents a lightweight and computationally efficient approach for party authentication in e-healthcare environments. Future research could delve into enhancing server-side user data privacy for healthcare system security.

In a development from 2021 by **Z. Zhao et. al. [98]** a novel privacy-preserving data-sharing system for IoMT was introduced to ensure anonymity and controlled access to medical data sharing while maintaining efficiency, on resource-limited IoMT devices. The suggested plan involves employing curve cryptography (ECC) XOR operations and hash functions to enable computations. This strategy enables patients to secure health data while maintaining privacy by generating identities. Furthermore, patients select approved users who can access the encrypted data upon authentication by the cloud server. The plan withstands threats. Provides security features, like privacy, access control and data integrity. Performance testing demonstrated that the plan necessitates computation rather than alternatives making it a viable option for secure and effective data exchange in IoMT.

In 2021 **D. Kwon et. al. [95]** detected security weaknesses in an existing user authentication system for Wireless Medical Sensor Networks (WMSNs) proposed by **Masud et. al.** These weaknesses included vulnerability to offline password guessing, user impersonation, insider attacks from users and lack of user anonymity. To tackle these deficiencies a new three-factor mutual authentication scheme using a function (PUF) was suggested. This scheme utilizes hash functions and XOR operations to support real-time communication; within WMSNs. Additionally, it integrates biometrics and PUFs with extractors to combat attacks, offline password-guessing attempts and unauthorized impersonation.

The security aspects of the plan were thoroughly examined using security analysis Burrows Abadi Needham (BAN) logic, the Real or Random (RoR) model and Automated Verification of Internet Security Protocols and Applications (AVISPA) simulation. These reviews confirmed that the plan is resilient against types of attacks such as password guessing, impersonation, privileged insider attacks, replay attacks and man-in-the-middle attacks. Additionally, it ensures user anonymity, forward secrecy and mutual authentication. The performance assessment indicated that the plan has computation and communication costs making it suitable for resource-limited WMSN environments. In comparison to existing authentication methods, this new solution presents an efficient approach for WMSN applications.

In 2021 **M. Hossain et. al. [90]** introduced P HIP. An authentication scheme aimed at overcoming the limitations of the Host Identity Protocol (HIP) in IoT environments with limited resources. Although HIP enables communication among devices it poses challenges for low-power IoT devices. P HIP addresses this issue by utilizing Elliptic Curve Qu Vanstone (ECQV) cryptography to reduce tasks, like modular exponentiation and signature verification during authentication and key exchange. P HIP also reduces the need for exchanging certificates, which often involves breaking down data packets for transmission over networks. Moreover P HIP allows devices to generate identifiers for each network and session enhancing privacy by safeguarding against location tracking and identity exposure. Security assessments confirm that P HIP can withstand attacks while performance evaluations show decreased computation, communication and energy usage compared to HIP methods. These enhancements position P HIP as an option for efficient authentication in IoT setups with limited resources.

The focus on lightweight security solutions for IoT and IIoT applications is presented in [115-118], each addressing different aspects of authentication, encryption, and countermeasure strategies. In [115], Ahmed et al. suggested an optimized AES design for IoT, with focus on efficiency in FPGA and ASIC, and with resistance to Differential Fault Analysis (DFA). Jin et al. [116] proposed a lightweight authentication scheme based on PUF and Chebyshev Chaotic Maps for secure Power

IoT communications. Villegas-Ch et al. [117] reviewed a blockchain-based authentication and authorization control for IoT networks, which are challenged in terms of resources. At the same time, Tanveer et al. [118] proposed LEAF-IIoT, an authentication framework for Industrial IoT, optimizing security. While Ahmed et al. paid attention to the cryptographic optimization, Jin et al. and Tanveer et al. paid attention to the authentication mechanisms, where the former implemented PUF and chaotic maps, and the latter aimed at industrial applications. Villegas-Ch et al. proposed a decentralized approach with blockchain, which is different from the other approaches.

2.3 Analysis and Summary of Literature Study

Analysis and summary of key trends form research papers; on authentication methods for IoT:

a. Several key trends emerge many papers propose authentication schemes and protocols specifically designed for resource constrained IoT devices. These approaches often utilize tools and strategies to ensure both security and efficiency.

b. The use of Light weight cryptography algorithms is a common thread in these studies. These algorithms are crafted to minimize memory demands catering to devices with limited resources.

c. Multi factor authentication (MFA) is underscored as crucial for IoT security in various papers. MFA integrates authentication factors, such as knowledge based possession based and biometric factors to bolster security during the authentication process.

d. Authentication methods based on Physical Unclonable Functions (PUFs) are gaining popularity. PUFs exploit the characteristics of devices to generate individualized keys enhancing security without necessitating extra storage.

e. Elliptic Curve Cryptography (ECC) stands out in many studies due to its robust security features and efficiency. Numerous papers delve into ECC based solutions for delivering lightweight authentication mechanisms.

f. Privacy preservation also emerges as a focus area, in these research efforts. Privacy is a concern, within environments. Some studies focus on maintaining privacy by suggesting methods that enable authentication while minimizing the exposure of data.

g. The energy consumption of devices is an aspect. Numerous studies concentrate on energy efficient authentication approaches to ensure that authentication procedures do not rapidly deplete the devices batteries.

h. Many studies recognize the challenges presented by environments, such as evolving network structures, device mobility and diverse device capabilities. Solutions often take these challenges into account when devising authentication strategies.

i. Efficient key management is vital for ensuring authentication. Several studies put forward management techniques that are lightweight and well suited for IoT devices.

j. Studies frequently delve into real world applications of the proposed methods across scenarios, including smart homes, industrial IoT, healthcare and smart cities. Real life examples showcase how applicable and effective the authentication methods can be.

k. Authors regularly conduct security assessments to assess the effectiveness of the proposed methods, against cyberattacks and vulnerabilities. This ensures that the suggested solutions are capable of handling threats when applied in real world scenarios.

l. Most studies feature a section dedicated to evaluating performance, where they compare the proposed approaches, with existing ones based on factors like authentication speed communication overhead, memory usage and energy consumption.

m. Some studies align with standardization efforts to promote interoperability and widespread adoption of authentication methods across environments.

n. The scalability aspect is crucial in deployments. Several studies tackle this issue by introducing methods that can manage a number of devices while ensuring security and efficiency.

The research papers provided contribute to the advancement of authentication methods for IoT. They underscore the significance of striking a balance between security, efficiency and practicality when designing authentication solutions for devices with limited resources. As IoT continues to progress, these studies offer insights into overcoming the challenges posed by the interconnected and diverse landscape of IoT.

2.4 Research Gaps

Although the research papers delve into various aspects related to lightweight authentication methods for IoT there remain noticeable gaps in research and areas that could benefit from further exploration;

a. **User Friendliness and User Experience:** While many authentication methods prioritize security and efficiency aspects such, as user experience and usability are often neglected. Creating authentication systems that're both secure and user friendly can significantly increase their acceptance, in IoT applications.

b. **Staying Resilient to Threats**: With the rise of IoT devices as attractive targets attackers are developing advanced techniques. Research should proactively address emerging attack strategies to ensure the durability of authentication methods against evolving risks.

c. **Enhancing Compatibility and Standardization:** Despite authentication approaches being suggested efforts towards standardization are limited. Research focusing on crafting standardized lightweight authentication protocols could establish benchmarks and facilitate integration within IoT environments.

d. **Addressing Resource Limitations:** While many studies acknowledge resource constraints there is still scope for refining authentication methods for devices with resources like those with minimal processing capabilities or memory.

e. **Safeguarding Privacy**: The vast data collection and transmission, in IoT raise privacy issues. Investigating authentication methods that safeguard user privacy and prevent data leakage during the authentication process is a research avenue.

f. **Ensuring Long Term Security:** While numerous methods prioritize security concerns long term security is equally vital. Research could focus on ensuring that authentication methods remain strong and effective throughout the lifespan of devices.

g. **Quantum Authentication:** As quantum computing progresses the security of authentication methods may be, at risk. It is important to research and develop authentication methods that can withstand quantum threats in devices.

h. **Hybrid Solutions:** Combining authentication approaches like biometrics and cryptography could lead to improved security and user friendliness. Exploring solutions customized for environments could be beneficial.

i. **Edge and Fog Computing:** With the increasing popularity of edge and fog computing authentication mechanisms must adapt to these decentralized setups. Research can investigate how lightweight authentication methods can be fine-tuned for edge and fog architectures.

j. **Energy Harvesting and Efficiency:** Some IoT devices rely on energy harvesting techniques for power creating authentication methods that're energy efficient and adaptable to fluctuating energy levels is a research area.

k. **Real World Deployment Challenges:** While new methods are proposed in research it is crucial to address the challenges of implementing these techniques, in world IoT settings, including integration, scalability and management issues.

Research that emphasizes authentication methods integrating elements, like behaviour patterns, biometric markers or context could pave the way, for personalized and secure authentication approaches. Tackling these research gaps may help in crafting authentication methods that're both comprehensive and user friendly designed specifically for the changing realm of IoT applications.

Table 2.1 summarizes the potential drawbacks associated with the mentioned research gaps and highlights the need for further research to enhance IoT authentication methods.

Table 2.1: Drawbacks Associated with Research Gaps in IoT Authentication Methods

Research Gap	Drawbacks
User Friendliness and User Experience	Low usability reduces user engagement and acceptance in IoT applications.
Staying Resilient to Threats	Authentication factors may be made obsolete as attackers design better techniques.
Enhancing Compatibility and Standardization	Lack of standardization poses a challenge to integration across different IoT systems.
Overcoming Resource Constraints	Some authentication mechanisms are not suitable for low-power, resource-restricted IoT devices.

Safeguarding Privacy	Data leakage and unauthorized access may happen due to insufficient privacy measures.
Ensuring Long-Term Security	Methods may deteriorate over time, leading to the need for regular updates or replacement.
Quantum Authentication	Classic cryptographic techniques can be breakable by quantum attacks.
Hybrid Solutions	Using multiple authentication mechanisms may enhance complexity and computational requirements.
Edge and Fog Computing	Authentication models may not be optimized for decentralized architectures, which can be inefficient.
Energy Harvesting and Efficiency	High energy consumption in authentication processes can quickly deplete battery-powered IoT devices.
Real-World Deployment Challenges	Scalability, integration, and management problems limit its adoption in real-world applications.

OBJECTIVES AND RESEARCH METHODOLOGY

CHAPTER 3

3.1 Objectives

On analysing the gaps related IoT security issues, objectives of the proposed work are as following:

i. To study and review the various methods for lightweight authentication.

ii. To propose an enhance lightweight authentication method for IOT.

iii. To verify and validate lightweight authentication for IOT.

iv. To analyse the proposed lightweight authentication for its efficiency.

3.2 Research Phases

To achieve the proposed objectives the research will pass through the following phases:

i) At the outset, the literature will be reviewed for different security aspects prevalent in IoT and authentication. This will help in making the foundation for security needs required in the IoT environment. Further we will compare techniques on the basis of parameters and their optimized values and various security goals and requirements fulfilled by these techniques.

ii) The existing security schemes algorithms will be considered to explore and analyse the fundamentals of existing security proposals being used in IoT. At this stage basic understanding of the thesis will be met.

iii) To start with the second objective, a lightweight authentication approach for IoT will be proposed based on the information acquired and the gaps present therein.

iv) After successfully proposing new techniques for security and authentication, the same will be simulated using standard implementation platforms. This will help in achieving the second objective.

v) After successful completion of the second phase. The third objective will come into focus in which verification and validation of the proposed approach will be done in comparison to existing protocols or approaches.

vi) At last, the newly designed technique will evaluate for efficiency with help of various structure parameters such as computation cost, communication cost, throughput, lambda etc. This phase will help in achieving the final objective.

3.3 Recent Trends in Lightweight Authentication for IoT

In the years there has been a surge in research and advancements focused on creating simpler ways to authenticate devices in the Internet of Things (IoT) realm. This surge is driven by the increase in devices with resources and the growing demand for authentication methods that're both secure and efficient. Researchers and creators have been working diligently to develop authentication solutions that balance security with the computing constraints of devices. They are exploring areas such as incorporating techniques like post quantum cryptography and blockchain to strengthen authentication protocols against potential threats from quantum computing while also improving transparency and trust within IoT networks. Additionally, progress in biometric based authentication, physical unclonable functions (PUFs) and machine learning algorithms has paved the way for creating sturdy authentication systems that leverage unique device characteristics and user behaviors for secure access. The inclusion of edge computing and zero trust security models further boosts the effectiveness and speed of authentication processes. Efforts towards standardization along with privacy preserving methods play a role in ensuring compatibility, scalability and data protection across IoT deployments. As the IoT landscape continues to evolve on-going research into authentication methods holds promise for establishing a foundation of smooth and reliable interactions, among interconnected devices and services.

3.4 Implementation Layers for Proposed Algorithm

A total of three layers will be used during the implementation of the proposed algorithm.

i. **IoT DEVICE LAYER**

It contains the actual producers of the data such as machines in the industry, sensors with patients in the medical system, and sensors in the environment.

ii. **FOG GATEWAY DEVICE LAYER**

It acts as a mediator between the user and the cloud. It is also responsible for the initial registration of the user with the cloud, login process, password recovery help, and re-registration of a particular device and decrypting data received from users and sending encrypted data to the cloud.

iii. **CLOUD SERVER LAYER**

It is responsible for handling user registrations, and receiving and storing complete data received from the sensor devices and the overall administration will be handled at this level.

3.5 Flowchart for Proposed Algorithm

To transmit the data collected at each IoT device, user IoT devices, a fog gateway device, and a cloud server will be built. Certain layers will be taken into consideration, such as the data service layer, which is in charge of transmitting encrypted data, the device access control layer, which is in charge of registering user devices, the gateway layer, which serves as an interface between the device access control layer and the remote layer. Figure 3.1 displays the suggested algorithm's flow chart.

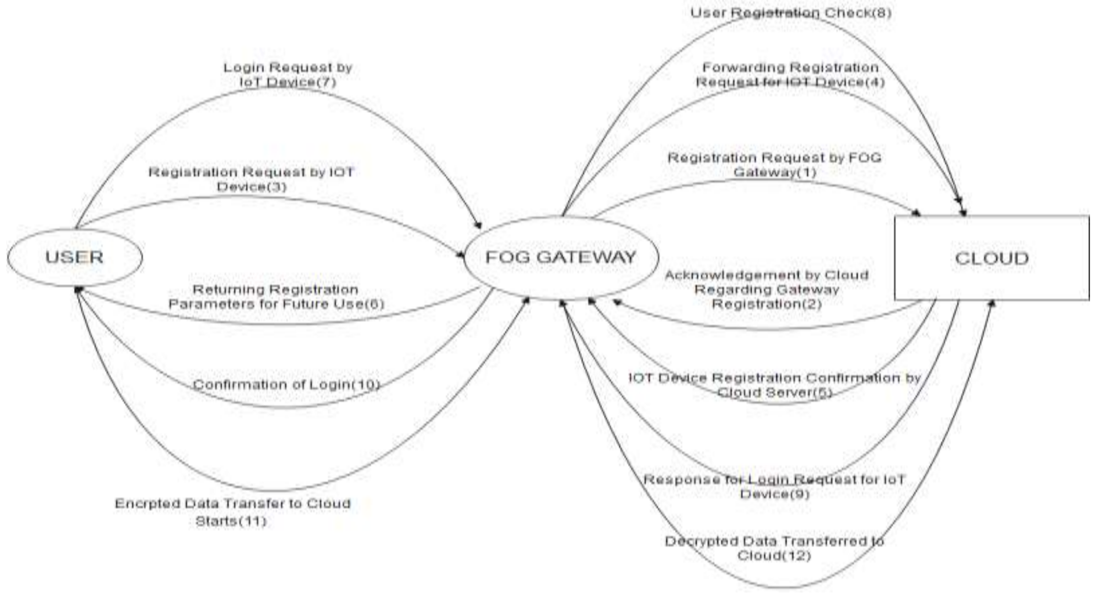

User Registration Check(8)
Login Request by IoT Device(7)
Forwarding Registration Request for IOT Device(4)
Registration Request by IOT Device(3)
Registration Request by FOG Gateway(1)
USER
FOG GATEWAY
CLOUD
Returning Registration Parameters for Future Use(6)
Acknowledgement by Cloud Regarding Gateway Registration(2)
Confirmation of Login(10)
IOT Device Registration Confirmation by Cloud Server(5)
Response for Login Request for IoT Device(9)
Encrpted Data Transfer to Cloud Starts(11)
Decrypted Data Transferred to Cloud(12)

Figure 3.1: Flow Chart for Proposed Algorithm

This flowchart outlines the secure registration process for an Internet of Things (IoT) device on a fog computing network. Fog computing solves the gap between resource-constrained IoT devices at the network edge and the powerful processing capabilities of the cloud.

i. The process begins with the fog gateway sending a registration request to the cloud. This request includes details, about the fog gateway itself such as its identifier and processing capabilities.

ii. Once the cloud receives the registration request it acknowledges it confirming that the fog gateway is recognized and authorized within the network.

iii. To register their device users interact with a designated interface like an app or web portal. During this process they provide information such as a device identifier device type and relevant sensor data.

iv. When the registered IoT device sends a login request to the fog gateway the fog gateway validates it before forwarding it to the cloud. This validation includes checking if the device ID matches a registered device and confirming security credentials.

v. In some system designs the cloud may temporarily hold login requests, for processing or security checks before proceeding.

vi. The cloud sends over parameters or configuration details after the fog gateway registers, in step 1. These details help the fog gateway handle tasks efficiently or improve communication with the cloud.

vii. Next the fog gateway forwards the users IoT device login request to the cloud for verification. The cloud then conducts its verification process, which may involve cross checking the device ID with a registry or performing additional security checks.

viii. After confirming the login request the cloud sends a response containing confirmation messages, access tokens or any necessary configuration data back to the fog gateway. The fog gateway then relays this confirmation back, to the users device to indicate that registration and login are complete.

ix. With everything set up secure data transmission can begin from the device to the fog gateway.

x. Data is usually encrypted for security and protection as it travels to the cloud. Once the fog gateway sends the data to the cloud it decrypts it using methods.

xi. The cloud may also handle data processing tasks before storing or transferring it to a location depending on how the system is set up.

3.6 Proposed Algorithm

3.6.1 Algorithm: Fog Gateway Registration

STEP R1:

Input:

- IP_i: IP address of the fog gateway device.
- FG_i: Unique ID of the fog gateway device.
- RG_i: Random number generated by the fog gateway device.
- TG_i: Timestamp of the fog gateway device.
- n: A large number for generating random numbers.

Output:

- Registration of fog gateway device and IoT devices with the cloud server.
- Generation of a unique authorization entity for each gateway device.

Step R1: Fog Gateway Device and IoT Device Registration

1. Compute Temporary ID (TIDi) for Fog Gateway Device:

$$TID_i = IP_i \parallel FG_i \parallel RG_i \parallel TG_i$$

2. Compute Hash Value of Temporary ID:

$$hash\_TID_i = h\ (TID_i)$$

3. Create Message M1:

$$M1 = TID_i \parallel hash\_TID_i$$

4. Transmit M1 from Gateway to Cloud Server:

- Send message M1 through a secure communication channel:

Gateway → Cloud Server: M1

Step R2: Cloud Server Processing

1. Recalculate Hash Value:

$$recalculated\_hash\_TID_i = h\ (TID_i)$$

- Compare with the received hash value:

- If ($recalculated\_hash\_TID_i == hash\_TID_i$), proceed to the next step.

2. Extract and Validate Timestamp (TG_i):

- Validate the freshness of the message using TG_i

3. Generate Random Numbers RCL1 and RCL2:

$$RCL1, RCL2 \text{ in } \{1, 2, ..., n-1\}$$

4. Create Random Component for Certificate (RCS):

$$RCS = RG_i \parallel RCL1$$

5. Create Message m:

$$m = TID_i \parallel RCS$$

6. Generate Implicit Signature (SIGCS):

$$SIGCS = h\ (m \parallel RCL2)$$

7. Create Authorization Certificate (ACS):

$ACS = V_c\ (FG_i \parallel RCS \parallel m \parallel SIGCS \parallel TSCS \parallel LTCS)$

8. Transmit M3 from Cloud Server to Gateway:

- Send the encrypted authorization certificate ACS:

Cloud Server → Gateway: M3 = ACS

9. Store Authorization Entity in Gateway:

- Store ACS in the fog gateway device's local memory for future communication with the cloud server.

End of Algorithm

This algorithm provides a clear and structured approach to the registration and certification process between fog gateway devices and the cloud server.

3.6.2 Algorithm: IoT Device Registration and Authentication

Input:

- IP_j: IP address of each IoT device.
- ID_j: Unique ID of each IoT device.
- RD_j: Random number generated by each IoT device.
- Tj_0: Current timestamp of each IoT device.
- LT_j: Lifetime of the temporary ID of each IoT device.
- ACS: Authorization Certificate from the cloud server for the fog gateway device.
- n: A large number for generating random numbers.

Output:

- Secure registration and authentication of IoT devices with the cloud server through the fog gateway device.

Step R3: IoT Device Registration

1. Compute Temporary ID (TID_j) for IoT Device:

Text {TID_j} = h (text {IP_j} || text {ID_j} || text {RD_j} || text {Tj_0} || text{LT_j})

2. Compute Hash Value of Temporary ID:

Text {hash_TID_j} = h (text {TID_j})

3. Create Message M4:

Text {M4} = text {TID_j} || text {hash_TID_j}

4. Transmit M4 from IoT Device to Fog Gateway Device:

- Send message M4 to the nearest fog gateway device:

Text {IoT Device} →text {Gateway}: text{M4}

5. Gateway Appends Permanent ID (ACS) to M4:

- Append the authorization certificate (ACS) received from the cloud server:

Text {M5} = text {M4} || text {ACS}

6. Transmit M5 from Fog Gateway Device to Cloud Server:

- Forward the augmented message to the cloud server:

Text {Gateway} → text {Cloud Server}: text {M5}

7. Cloud Server Verifies the Permanent ID of the Gateway Device:

- Confirm the validity of the permanent ID stored in the cloud server's database.

8. Recalculate Hash Value of IoT Device Message:

Text {recalculated_hash_TID_j} = h (text {TID_j})

- Compare with the received hash value:

- If (text {recalculated_hash_TID_j} == text {hash_TID_j}), proceed to the next step.

9. Extract and Validate Timestamp (Tj_0):

- Validate the freshness of the message using Tj_0.

Step R4: IoT Device Authentication

1. Generate Random Numbers RCL3 and RCL4:

Text {RCL3}, text {RCL4} in {1, 2, ..., n-1}

2. Create Random Component for IoT Device Certificate (RCS2):

Text {RCS2} = text {RD_j} || text {RCL3}

3. Create Message m:

m = h (text {TID_j} || text {RCS2})

4. Generate Implicit Signature (SIGCS2):

Text {SIGCS2} = h (m || text {RCL4})

5. Create Authorization Certificate (ACS2) for IoT Device:

Text {ACS2} = V_c (text {TID_j} || text {RCS2} || m || text {SIGCS2} || text {TS2} || text {LT2})

6. Transmit M7 from Cloud Server to Fog Gateway Device:

- Send the encrypted authorization certificate ACS2:

Text {Cloud Server} → text {Gateway}: text {M7} = text {ACS2}

7. Transmit M8 from Fog Gateway Device to IoT Device:

- Relay the message to the IoT device:

Text {Gateway} → text {IoT Device}: text {M8} = text {ACS2}

8. IoT Device Stores Authenticator (ACS2) for Future Communication:

- Store ACS2 in the IoT device's local memory.

9**. Future Communication and Relocation:**

- If the IoT device changes location and connects to a different fog gateway device:
- The IoT device shares the value of the authenticator with the new fog gateway device.
- The new gateway device assists in successfully logging in with the cloud server.

End of Algorithm

This algorithm ensures secure registration and authentication of IoT devices within the network, allowing them to communicate securely with the cloud server through the fog gateway devices.

3.7 Steps for Implementing Lightweight Security Protocol for IoT

The following are some actions that must be taken in order to establish a lightweight security protocol for the Internet of Things:

I. Initialization

During this phase, the cloud server and the fog gateway will establish their nonce values, which will be utilized during information exchange securely. The cloud server will generate and identify its public and private key pairs. These keys will be employed during the transmission of the personal ID to both the fog gateway device and the IoT device. The cloud's private key is denoted as β_c and the public key as V_c, where $1<V_c<n$ and $1< \beta_c< n$. The list of important symbols used is provided in Table 3.1.

Table 3.1: Symbols and Their Description

Symbol	**Explanation**
β_c	Private Key of Cloud Server
V_c	Public Key of Cloud Server
TID_i , TID_j	Temporary ID of Gateway Device, IoT Device
IP_i , IP_j	IP address of Gateway Device, IoT Device
RG_i , R_{CL1} , R_{CL2} , R_{CL3} , R_{CL4} , RD_j	random numbers generated at each gateway device/cloud server/IoT device
TG_i, TS_{CS}, T_j^0, TS_2, $TG1_i$, $TG2_i$, T_j^1	timestamp of the gateway device, cloud server, IoT device
SIG_{CS} , SIG_{CS2}	Implicit Signatures of the cloud server
LT_{CS} , LT_2 , LT_j	Lifetime of the authentication entity generated by the cloud server for the gateway device/IoT device, Lifetime of the temporary ID of IoT device
A_{CS} , A_{CS2}	Authentication certificate generated by cloud server for gateway device/for the IoT device
FG_i , ID_j	Unique ID of the gateway device/IoT device
R_{CS} , R_{CS2}	Concatenated random numbers by cloud server

II. Fog gateway registration over Cloud Server

Step R1: During this phase, each fog gateway device within the network initiates registration with a designated cloud server, as all data transmissions from user IoT devices to the cloud server are routed through these gateway devices. Additionally, IoT devices undergo registration with the cloud server by forwarding a registration request through the fog gateway device. The gateway device transmits its temporary identification, denoted as TID_i, for registration to the cloud server through a secure communication channel. The computation of the temporary ID is given in equation 1 is as follows:

$$TID_i = (IP_i \| FG_i \| RG_i \| TG_i) \qquad (1)$$

where

TID_i = temporary ID for each gateway device for i Ɛ 1, 2, 3 …

IP_i = ip address of each gateway device

FG_i = unique ID of the gateway device

RG_i = random number generated at each gateway device

TG_i = timestamp of the gateway device

The temporary ID is transmitted to the cloud server subsequent to the computation of its hash value, which is derived from concatenating pertinent data. This hash value is then appended to the temporary ID, serving as a means to authenticate and ensure the integrity of the message as given in equation 2.

$$\mathbf{M1} = TID_i \parallel h\ (TID_i)$$
$$\{Gateway \rightarrow Cloud\ Server\} \qquad (2)$$

Step R2: Upon receipt of the listing message from the fog gateway device, the cloud server takings to recalculate the hash value of the message. Subsequently, it conducts an evaluation between the recalculated hash value and the received hash value. Upon verification of their equivalence, the cloud servers proceed to extract specific components of the message to verify the timestamp value as mentioned in equation 3.

$$\mathbf{M2} = h\ (M1) = h\ (TID_i) = h\ (IP_i \parallel FG_i \parallel RG_i \parallel TG_i) \qquad (3)$$

Following decryption, the cloud server proceeds to retrieve the gateway device's credentials, facilitating the validation of the timestamp to ensure message freshness. Subsequently, the server generates two random numbers, RCL_1 and RCL_2, from the set {1, 2, ..., n-1}. Utilizing the temporary ID of the gateway device, the cloud server creates a certificate for said device, intended for future communications. This certificate includes several components: combined random numbers R_{CS}, implicit signature SIG_{CS}, the current server timestamp TS_{CS}, the certificate's lifetime LT_{CS}, and an authorization entity as explained from equations 4 to 7.

$$R_{CS} = (RG_i \parallel R_{CL1}) \qquad (4)$$

$$m = (TID_i \parallel R_{CS}) \qquad (5)$$

$$SIG_{CS} = h\ (m \parallel R_{CL2}) \qquad (6)$$

$$A_{CS} = V_c\ (FG_i \parallel R_{CS} \parallel m \parallel SIG_{CS} \parallel TS_{CS} \parallel LT_{CS}) \qquad (7)$$

The authorization entity remains encrypted, as the private key necessary for decryption is exclusively held by the cloud server. Subsequently, the cloud server shares the pertinent details with the fog gateway device, enabling the device to store the encrypted authorization entity within its local memory. This ensures the device's capability to engage in future communications with the cloud server. Importantly, the value assigned to the authorization entity as given in equation 8, varies uniquely for each gateway device.

$$\mathbf{M3} = A_{CS}$$

$$\{\text{Cloud Server} \rightarrow \text{Gateway}\} \tag{8}$$

The details are then transmitted to the fog gateway device, enabling it to store the authorization entity within its local memory. This allows the device to maintain authorization credentials for future interactions with the cloud server. The authorization entity will be unique for each gateway device.

III. User IoT device registration over Cloud Server via Fog gateway

Step R3: involves an essential phase in the initial network setup, which is pivotal for securely registering every IoT device through the Cloud server. Each IoT device, selected as {Dj | j ε 1, 2, 3, ...}, is capable of with a unique identifier IDj. These devices transmit a temporary ID to the cloud server for registration. This transmission occurs from side to side the nearest fog gateway device, which ensures intermediary processing before the message reaches the cloud server. The computation of the temporary ID for each IoT device is a critical component of this process and is elaborated upon as follows in equation 9:

$$TID_j = (IP_j \parallel ID_j \parallel RD_j \parallel T_j^0 \parallel LT_j) \tag{9}$$

where:

IPj_i = ip address of each IoT device

TID_j = provisional ID of the IoT device

RD_j = casual number generated at each IoT device

T_j^0 = current timestamp of each IoT device

LT_j = Lifetime of the temporary ID of each IoT device

Before transmitting a registration request from the IoT device to the cloud server, the temporary ID combined with its corresponding hash value is first sent to the fog gateway device for processing is given in equation 10.

$$\mathbf{M4} = TID_j \parallel h\,(TID_j) \tag{10}$$

$$\{\text{IoT Device} \rightarrow \text{Gateway}\}$$

Upon receiving the listing message from the IoT gateway device, the fog device appends its permanent ID, acquired from the cloud server, to the message received from the IoT device is given in equation 11. Subsequently, it forwards the augmented message to the cloud server.

$$\mathbf{M5} = M4 \,||\, A_{CS} \tag{11}$$

{Gateway→Cloud Server}

Upon receipt of the message, the cloud server verifies the permanent ID of the fog gateway device stored in its database. After confirming the validity of the permanent ID, the cloud server recalculates the hash value of the message sent by the IoT device to verify its integrity. It then compares the recalculated hash value with the received hash value. Upon confirmation of their equivalence, the cloud server proceeds to extract specific components of the message to validate the timestamp value as given in equation 12.

$$\mathbf{M6} = h\,(TID_j) = h\,(IP_j \,||\, ID_j \,||\, RD_j \,||\, T_j^0 \,||\, LT_j) \tag{12}$$

After decryption, the cloud server accesses the gateway device's credentials, enabling the validation of the timestamp to ensure the freshness of the message.

Step R4:

After all verifications have been completed by the cloud server will generate random numbers R_{CL3} and R_{CL4} followed by the authenticator for each individual IoT device that approached the cloud server for registration is given in equation 13 to 16.

$$R_{CS2} = (RD_j \,||\, R_{CL3}) \tag{13}$$

$$m = h\,(TID_j \,||R_{CS2}) \tag{14}$$

$$SIG_{CS2} = h\,(m \,||\, R_{CL4}) \tag{15}$$

$$A_{CS2} = V_c\,(ID_j \,||\, R_{CS2} \,||\, m \,||\, SIG_{CS2} \,||\, TS_2 \,||\, LT_2) \tag{16}$$

As previously noted, the authenticator remains encrypted as the private key is exclusively held by the cloud server. Following verification, the pertinent details are communicated to the fog gateway device, which subsequently relays them to the IoT device. The IoT device stores the authenticator in its local memory for subsequent communications with the cloud server is given in equation 17 & 18. Notably, the authenticator value varies uniquely for each IoT device.

$$\mathbf{M7} = A_{CS2}$$

{Cloud Server→Gateway} (17)

$$\mathbf{M8} = \mathbf{M7} \tag{18}$$

{Gateway→IoT Device}

Once it is verified the value of A_{CS2} is forwarded by the gateway device to the IoT device for future communication along with a timestamp to maintain the freshness of the message. Next time any device changes its location and gets attached to some other fog gateway device depending on the shortest distance, in that case only the value of the authenticator is required to be shared for the cloud server so that the gateway device shall help the IoT device for successful login with the cloud server.

IV. Login Request by the Device

After successful registration IoT device can communicate with the cloud server. But for the same, every IoT device needs to successfully log into the cloud server and when authentication is required, the IoT device Dj executes the following steps to log in to the cloud server. The IoT device generates the timestamp $T_j^{\ 1}$, selects a random number r_i Ɛ Z_p^*, and finally transmits a message to the gateway device is given in equation 19.

$$\mathbf{M9} = < TID_j \,||\, A_{CS2}|| \, T_j^{\ 1} \,||\, r_j \,||\, A_{CS}> \tag{19}$$

Upon receiving the message firstly, the gateway device will check the timestamp $TS_G - T_j^{\ 1} <= \Delta TD$ where ΔTD represents the maximum allowable delay, if the delay falls within the validity period, the message is transmitted to the cloud server for authentication. Otherwise, if the delay exceeds the threshold, the received message is either discarded or the connection is terminated. This preventive measure mitigates the potential for replay attacks within the proposed scheme. Subsequently, the gateway device forwards the received message to the cloud server in its original state, as received from the IoT device, ensuring the cloud server's authentication of the IoT device's authenticity.

At the cloud server level, upon receiving the message, the validity of the timestamp and the random number provided by the IoT device within the message are scrutinized to ascertain the message's freshness. Upon successful validation, the cloud server proceeds to decrypt the values of ACS and ACS2. This decryption process serves to authenticate both the gateway device and the IoT device as authentication entities. Notably, the authenticator generated by the cloud server for the communicating devices is also decrypted and validated as part of this process. Finally, the cloud server sends an acknowledgment message to the IoT device, prompting it to commence transmitting the sensed data through the gateway device. Upon receiving this acknowledgment from the cloud server, the IoT device initiates the transmission of encrypted sensed data. This encryption utilizes the public-private key pairs associated with both the gateway device and the cloud server.

V. Expired authenticator request by the gateway device/IoT device

Each authenticator is associated with a timeline. After the lapse of the authenticator lifetime, the communication session gets terminated between the IoT device and the cloud server or the gateway device and the cloud server. Thus, the gateway devices as well as the IoT devices need to initiate an authenticator renewal process. A new authenticator will be negotiated between the communicating entities. The information related to the expiry of the authenticators will be shared by the cloud server as the details can only be decrypted by the cloud server and once informed the IoT device as well as the gateway device will follow the procedure for renewal:

$RD1_j = 1,2,3\ldots$

{Fresh random number generated at the IoT Device}

$$\mathbf{M10} = h(TID_j \,||\, RD1_j \,||\, A_{CS2})$$

$$\{\text{IoT Device} \rightarrow \text{Gateway}\} \qquad (20)$$

Once the message will be received by the gateway device, the value of the random number will be validated to check the freshness of the message as given in equation 20. Afterward, the gateway device will evaluate the integrity of the message by calculating a new hash function h' and will compare h' == h once found accurate then it will share the authentication entity A_{CS} along with the original message received from the IoT device to the cloud server. A timestamp value will be attached by the gateway device to ensure the freshness of the message is given in equation 21.

$$\mathbf{M11} = h(TID_j \,||\, TID_i \,||\, TSG_i \,||A_{CS2} \,||\, A_{CS}\,) \qquad (21)$$

Where TSG_i = current time status of the gateway device

The cloud server will respond back either by sharing a fresh authenticator for the IoT device or by updating the lifetime of the authenticator shared with the IoT device at the time of the initial registration.

In case the authentication entity of the gateway device gets expired then the gateway device must contact the cloud server for renewal. During the communication gateway device will use its current timings of the system along with other details to be shared with the cloud server for renewal is given in equation 22.

$$\textbf{M12} = h(TID_i \parallel TSG_i \parallel A_{CS})$$

$$\{\text{Gateway Device} \rightarrow \text{Cloud Server}\} \qquad (22)$$

Once the message will be received by the cloud server, it will decrypt the message and check the timestamp TSG_i with the current timings of the local server and if found under the valid limits it will accept the message otherwise it will drop the communication. If the message will be accepted by the cloud server then either a fresh authentication entity will be shared with the gateway device or the value of the lifetime variable used at the time of generation of the authentication entity during the initial registration of the gateway device will be increased.

Conclusion: The proposed technique is a lightweight authentication for the security of IoT, which is based on a three layer architecture namely IoT Device Layer, Fog Gateway Device Layer and Cloud Server Layer. The process starts with an analysis of the current security approaches and gaps between them. Then a new authentication method is simulated and evaluated with respect to the computational cost, communication cost and efficiency. The authentication process starts with the secure registration of the IoT devices to the fog gateways to the cloud using cryptographic methods like hash functions and random number generation. The protocol provides secure device authentication, encrypted data transmission and periodic update of authentication credentials to sustain the security and prevent replay attack. The integration of post-quantum cryptography, block chain, biometric authentication, and machine learning improves the security without compromising on the efficiency in the resource constrained IoT networks.

RESULTS AND DISCUSSION

CHAPTER-4

4.1 Introduction

The primary focus of this chapter is the development of a lightweight authentication mechanism designed for devices. In the past, IoT devices had to register with services, on servers or third party platforms to access and share important data with cloud servers. However, relying on third party authentication introduces complexity and security risks. There is concern that external authentication services may not adhere to the security standards required for environments potentially exposing devices to security breaches and compromising private data.

Additionally incorporating third party authentication can lead to interoperability challenges. IoT devices from manufacturers may struggle to authenticate across different third party services resulting in compatibility issues and inconsistent user experiences. Moreover, depending on services exposes devices to reliability issues such as service disruptions or changes in authentication methods that could disrupt device functionality and restrict user access.

Furthermore this approach highlights the challenges faced by energy constrained devices in terms of time consumption and energy depletion. The size of the certificates is actually bigger than the transmission unit (MTU) used by devices on networks like 6LowPAN, CAN, KNX, Z Wave and ZigBee. These networks have limited bandwidth ranging from 16 to 250 kb/s. Due to this disparity in size and network capabilities the certificates are broken down into fragments before being sent over these networks. Consequently, both sender and receiver IoT devices face challenges in processing these fragments, ensuring delivery efficiently. This leads to increased communication complexities and energy consumption, on the devices affecting their ability to respond promptly to real time requests and reducing their battery life.

This procedure ensures that a robust authentication system is in place to address these challenges. By utilizing fog gateways positioned between devices and cloud servers, the proposed protocol enhances registration efficiency which overcomes distance related limitations and improves the overall responsiveness and reliability of the system.

In this section, it is assessed how well the proposed protocol performs in both software and hardware settings. When compared to existing RSA and ECC protocols at the security level, the proposed protocol demonstrates superior performance. Initially, some enhancements to the key encryption scheme, for increased security and efficiency, were proposed. Subsequently, the setup, implementation approaches and performance comparisons will be outlined.

4.2 Analysis of Performance Parameters

Using NS3 simulations, the impact on throughput, average departure rate (lambda), end to end delay, and number of packets transmitted/received, computation cost and the communication cost is demonstrated in this work. A more detailed and comprehensive security analysis is presented below:

4.2.1 Study and Review of Lightweight Authentication Methods

During this stage a thorough examination was carried out on the lightweight authentication techniques commonly used in Internet of Things (IoT) settings. Lightweight authentication plays a role, for devices given their limited resources and the importance of effective security measures. Various methods including Elliptic Curve Cryptography (ECC) Hash based Message Authentication Codes (HMAC) and lightweight symmetric key algorithms were analyzed. Each method was evaluated based on factors like complexity, communication efficiency, and energy usage and security strength. This assessment laid groundwork for improving existing practices.

4.2.2 Proposal and Enhancement of a Lightweight Authentication Method for IoT

After analyzing the findings, an authentication approach designed specifically for IoT settings is introduced. This method merges the advantages of SHA256 to strike a balance between security and effectiveness. Improvements encompassed management procedures and simplified authentication steps to lessen the burden on computational resources and communication channels.

4.2.3 Verification and Validation of the Lightweight Authentication Method for IoT

To confirm and authenticate the suggested approach, it was put into action, within the NS3 simulation platform. The confirmation procedure entailed testing across network scenarios and instances of attacks. Threats like man-in-the-middle attacks, replay attacks and denial of service attacks were replicated to guarantee the method's strength. Evaluation criteria consisted of the rate of authentication acceptance rate and false rejections rate all indicating the methods durability and trustworthiness.

4.2.4 Analysis of the Proposed Lightweight Authentication Method

- **End-to-End Delay**

The end-to-end delay to evaluate the impact of the authentication method on network latency is measured. It is calculated as the relation between the time and total packet send, is given in equation 1.

$$E_d = \sum_{i=1}^{Vpacket} \frac{(T_{RECEIVE}) - (T_{SEND})}{Vpacket} \tag{23}$$

$T_{RECEIVE}$ is the total time to receive a packet and T_{SEND} is the total time to send a packet. $Vpacket$ Is the total number of the packets sent over the channel and it is measured in seconds. Table 4.1 given below shows the end to end delay calculated in respect of the number of nodes for the proposed approach.

Table 4.1: End to End Delay for Proposed Protocol

Number of Nodes	End to End Delay(sec)
10	0.437305
15	0.517
20	0.528
25	0.6592
30	0.7247
35	0.795
40	0.845

The proposed method showed a minimal increase in end-to-end delay compared to traditional methods, ensuring that data packets were transmitted with negligible latency, which is critical for real-time IoT applications such as smart healthcare and industrial automation. The relation between numbers of nodes with E_d is presented in figure 4.1.

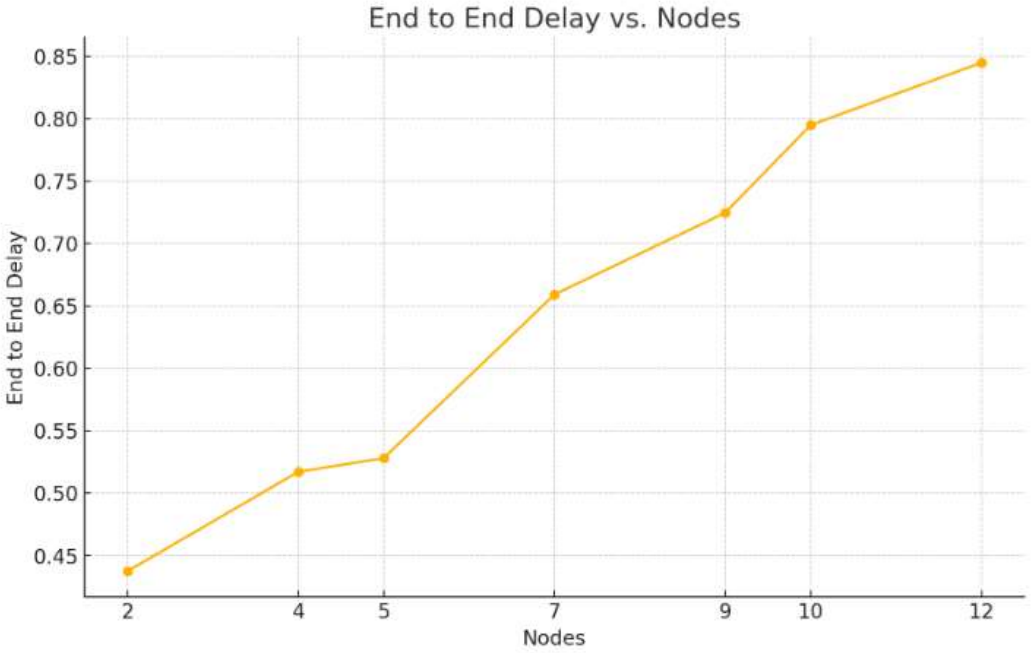


Figure 4.1 Relation between Number of Nodes & End to End Delay

The line graph depicts how the number of nodes, in a network influences the end to end delay within that network. On the x axis you can see the range of nodes from 2 to 12 representing devices or points in the network for sending, receiving or relaying information. The plotted data points are at 2, 4 5 7 9 10 and 12 nodes. The y axis shows the end to end delay in seconds as data packets travel from source to destination node. The delay values span from around 0.44 to 0.85 seconds.

By moving from 2 to 4 nodes the end to end delay increases slightly from about 0.44 seconds to 0.52 seconds indicating a rise with added nodes. Progressing from 4 to 5 nodes sees an increase to 0.528 seconds. Showing a marginal uptick in delay, a noticeable jump occurs as it goes from 5 to7 nodes with the delay spiking to around.6592 seconds, highlighting a significant impact on delay, with these additional nodes.

The pattern persists with 9 nodes experiencing a delay of 0.7247 and 10 nodes encountering a delay of 0.795 indicating an increase, in delay with the addition of nodes.

The highest delay is observed at 12 nodes registering a delay of 0.845. This indicates that as the network expands the overall end to end delay escalates significantly. The escalation in end to end delay with an increase in the number of nodes could be attributed to network congestion, where additional nodes result in heightened data traffic and subsequent delays. With an expanding number of nodes, the intricacy of routing data packets also rises, potentially contributing to prolonged delays. Networks face limitations in processing capabilities; therefore as the number of nodes grows these resources are utilized intensively leading to amplified delays.

The graph unmistakably illustrates that as the number of nodes within a network raises so does the end to end delay. This correlation underscores the significance of network design and management to minimize delays within larger networks. It underscores that while augmenting nodes can enhance network coverage and capacity it can also introduce delays that necessitate careful management, through network protocols and infrastructure enhancements.

- **Computation Cost**

The expense of computation measured by the number of CPU cycles needed for verification saw a decrease. The proposed approach utilizes basics and refined algorithmic executions to cut down on processing time. This decrease, in computation expense renders the approach viable for energy gadgets with restricted processing abilities. Table 4.2 given below represents the computation cost calculated in respect of the number of nodes for the proposed approach.

Table 4.2:Computation Cost for Proposed Protocol

Number of Nodes	Computation Cost (Seconds)
10	0.009335
15	0.010116
20	0.014435
25	0.014507
30	0.014767
35	0.014861
40	0.016453

The chart enclosed here illustrates how the processing time, in a network changes based on the number of nodes. On the axis we have the range of nodes from 10 to 40 while the vertical axis shows the processing time.

Here's a breakdown of what the graph shows;

In the starting Phase (10 to 15 Nodes), the processing time begins at about 0.009 seconds for 10 nodes. It gradually increases to around 0.010 seconds as it reach 15 nodes. This initial phase demonstrates a rise in processing time with each node. In the noteworthy Surge (15 to 20 Nodes) Between 15 and 20 nodes there is a spike in processing time jumping from 0.010 seconds to about 0.015 seconds. This spike highlights an increase, in demand as the network expands to include 20 nodes.

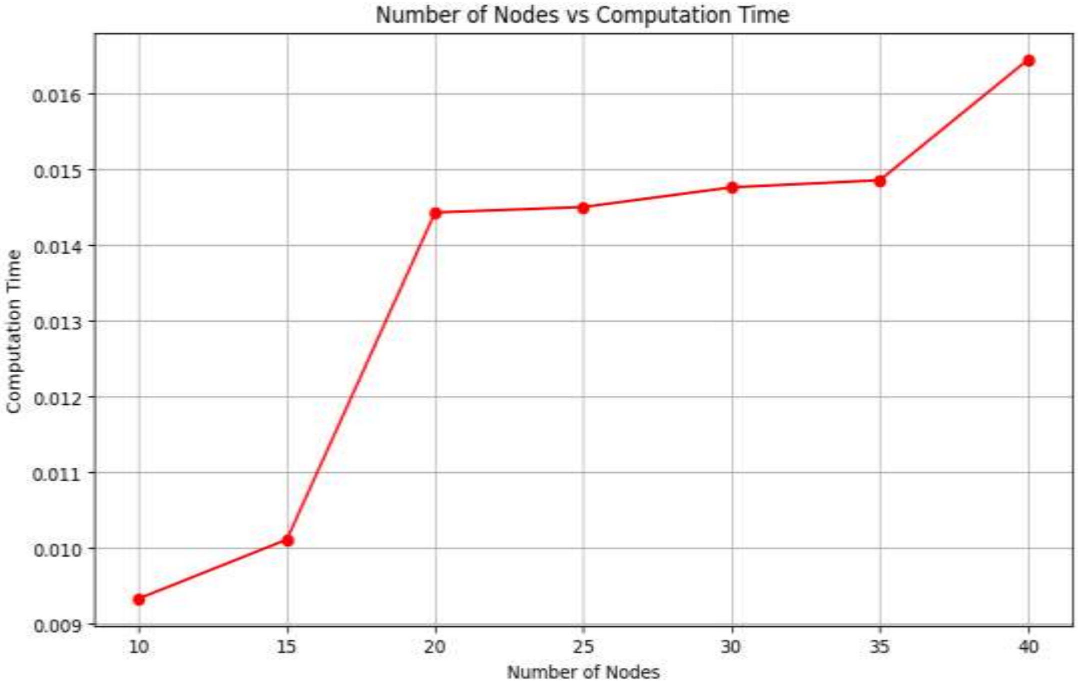


Figure 4.2 Relation between Number of Nodes & Computation Time (Seconds)

During the Plateau Phase, which spans from 20 to 35 nodes the computation time remains quite steady at around 0.015 seconds with fluctuations. This phase indicates that the networks computational capacity can accommodate nodes without causing an increase, in computation time. Subsequently as it moves into the further Increase phase from 35 to 40 nodes there is an uptick in computation time peaking at 0.016 seconds when reaching 40 nodes. This uptrend suggests that with network expansion the computational load starts to rise as shown in figure 4.2.

To summarize the graphs findings it is evident that as the number of nodes increases so does the computation time. Notably there is a spike between 15 and 20 nodes. Following this surge the computation time stabilizes until reaching, around 35 nodes before showing another increase. This pattern underscores how network size impacts efficiency and emphasizes the importance of scaling for optimal performance.

- **Communication Cost**

The expense of communication as determined by the volume of data shared during the verification process was lessened by cutting down on the number of message swaps and refining the payload size. This effectiveness aids in saving bandwidth lessening network traffic and enhancing network performance, as a whole.

On the basis of equation 1 and 2 given in chapter 3, the computation cost for step R1 can be calculated by adding the bits used at the time of the concatenation of ip address of the device, unique ID of the gateway which MAC address has been considered in the algorithm, the size of the random number generated by the device in bits and the bit size of the timestamp i.e. the current time of the device which varies from 7 bytes to 13 bytes and finally the size of the hash value generated by the SHA256 hash algorithm used before delivering the details of the gateway device to the cloud server.

M1= $TID_i \| h(TID_i) = (IP_i \|FG_i \| RG_i \| TG_i) + h(IP_i \|FG_i \| RG_i \| TG_i)$

from equation 1

CCost1 = size of IP address of gateway device + MAC address of gateway device + size of random number generated at the gateway device in bits + timestamp of the gateway device + SHA256 value of the $(IP_i \|FG_i \| RG_i \| TG_i)$

CCost1 = 128 bits + 48 bits + 48 bits + 56 bits + 256 bits = 536 bits (24)

Similarly, second computation calculated on the basis of the response given by the cloud server to the gateway device and on the basis of the equation 4-7 under step R2 can be calculated as given below:

$A_{CS} = V_c (FG_i \| R_{CS} \| m \| SIG_{CS} \| TS_{CS} \| LT_{CS})$ from equation 7

CCost2 = MAC address of gateway device + size of combined random numbers R_{CS} in bits + size of implicit signature SIG_{CS} in bits + the current cloud server timestamp TS_{CS} in bits + the certificate's lifetime LT_{CS} size of random numbers generated at the cloud server in bits

CCost2 = 48 bits + 96 bits + 152 bits + 256 bits + 56 bits + 64 bits = 672 bits (25)

Adding more, the third computation cost related to step R3 on the basis of equation 9 and 10 can be calculated as:

$TID_j = (IP_j \| ID_j \| RD_j \| T_j^0 \| LT_j)$ from equation 9

M4= $TID_j \| h(TID_j)$ from equation 10

CCost3 = IP address of the IoT device + MAC address of the IoT device + size of random number generated at the IoT device in bits + the current timestamp of each IoT device + Lifetime of the temporary ID of each IoT device in bits + SHA256 value of the (IP_j || ID_j || RD_j || T_j^0 || LT_j)

CCost3 = 128 bits + 48 bits + 48 bits + 56 bits + 64 bits + 256 bits = 600 bits (26)

In addition to this, another computation cost value will be calculated on the basis of the equation number 11 as mentioned below:

M5= M4 || A_{CS} from equation 11

CCost4 = CCost3 + CCost2 = 600 + 672 = 1272 bits (27)

Finally, the cloud server replying back to the IoT device via the gateway device as explained with step R4 and equation 16 using 672 bits.

$A_{CS2} = V_c\,(ID_j \,||\, R_{CS2} \,||\, m \,||\, SIG_{CS2} \,||\, TS_2 \,||\, LT_2)$ from equation 16

CCost5 = MAC address of the IoT device + size of combined random numbers R_{CS2} in bits + size of implicit signature SIG_{CS2} in bits + the current cloud server timestamp TS_2 in bits + the certificate's lifetime LT_2 size of random numbers generated at the cloud server in bits

At last, the total computation cost used for one successful authentication using the proposed approach by adding all the values calculated using equations 24-27 is

CCost1 + CCost2 + CCost3 + CCost4 + CCost5= 536 + 672 + 600 + 1272 + 672 = 3752 bits. (28)

- **Average Departure Rate (λ)**

The average departure rates indicate how many packets each node sends, per second on average helping us evaluate the scalability of proposed approach. The proposed method performed well under request volumes showing its capability to handle large scale IoT deployments with multiple devices transmitting packets simultaneously. The values obtained for average departure rate by varying the number of nodes can be seen in table 4.3.

Table 4.3: Average Departure Rate for Proposed Protocol

Number of Nodes	1024/10	1024/20	1024/30	1024/40	1024/50
10	1.7742	1.7809	1.7876	1.7943	1.801
15	1.8533	1.8619	1.8705	1.8791	1.8877
20	1.8492	1.8503	1.8514	1.8525	1.8536

25	1.9127	1.9217	1.9307	1.9397	1.9487
30	1.9271	1.9313	1.9355	1.9397	1.9439
35	1.9372	1.9412	1.9452	1.9492	1.9532
40	1.9447	1.9493	1.9539	1.9585	1.9631

The relation of average departure Rate with number of nodes is given in figure 4.3. The graph attached depicts the correlation between the number of nodes and the average departure rate (λ) in a network. The x axis displays the node count ranging from 10 to 40 while the y axis shows the departure rate (λ). There are five datasets represented by lines; 1024/10, 1024/20, 1024/30, 1024/40 and 1024/50.

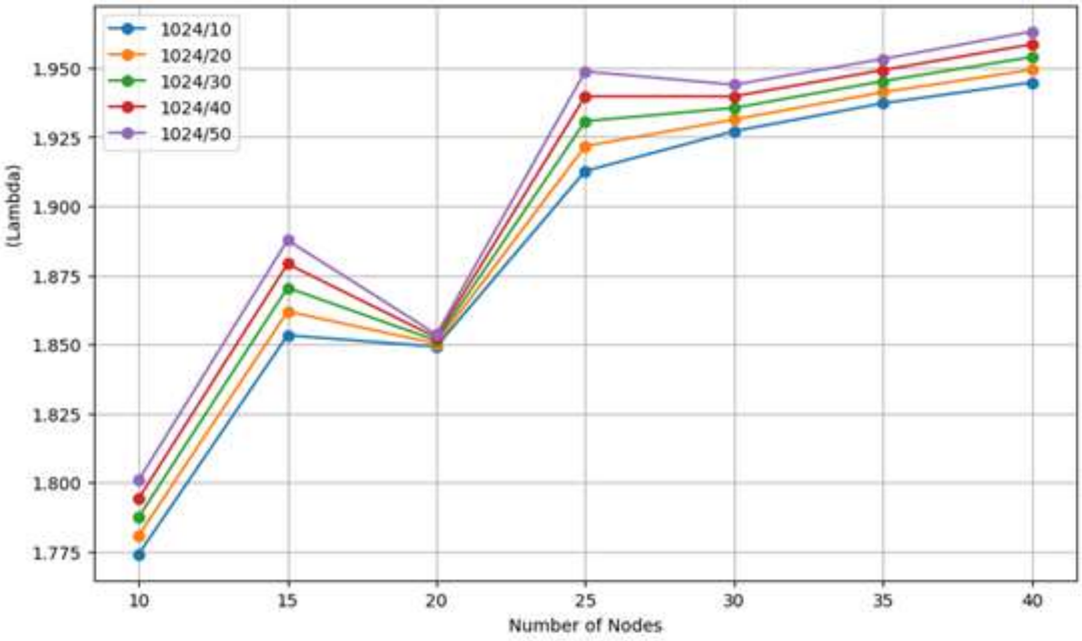


Figure 4.3: Relation between Average Departure Rate & number of nodes

Initial Increase across all datasets there is a rise in the departure rate as the number of nodes increases from 10 to 15. This suggests that adding nodes initially enhances the departure rate.

Fluctuation at 20 nodes some datasets show a plateau or slight decrease in departure rate. This plateau indicates that adding nodes reaches equilibrium where it has minimal impact, on the departure rate. After reaching a point the rate at which nodes leave continues to go up when the number of nodes goes from 20 to 40. This suggests that the network can manage nodes without compromising on or even improving departure rates.

When looking at datasets each line represents a dataset, with different parameters likely related to message size or frequency. Across all datasets there is a trend of an increase in the departure rate as the number of nodes increases with slight variations based on specific parameters. This pattern illustrates that the network can expand to support nodes while maintaining a departure rate.

In summary the graph illustrates that as the number of network nodes increases so does the average departure rate, with fluctuations at points. While different datasets with parameters show different performances the overall trend suggests effective scalability and efficiency, in managing additional nodes.

- **Throughput**

Evaluating the efficiency of communication networks involves considering network throughput, which measures the rate of data transmission, between points over a time period. It is commonly expressed in bits per second (bps) or packets per second (pps). It is calculated as (Total received packets * size of individual packet) / total time in seconds as given in equation 4.2.

$$\text{Throughput} = \frac{Total\ received\ packets*siz\ \text{泠}\ of\ indiv\ \text{峢}dual\ packet}{total\ time\ in\ sec\ \text{獉}\ \text{潲}ds} \tag{29}$$

Represented as $(a_r * P)/T$ where a_r are the total received packets, P is the packet size and Tis the total time in seconds to receive the packet successfully. The values obtained for throughput by varying the number of nodes can be seen in table 4.4.

Table 4.4: Throughput for Proposed Protocol

Number of Nodes	1024/10	1024/20	1024/30	1024/40	1024/50
10	60.3202	60.5432	60.7662	60.9892	61.2122
15	63.0132	63.3401	63.667	63.9939	64.3208
20	64.2892	64.3222	64.3552	64.3882	64.4212
25	65.0333	65.0561	65.0789	65.1017	65.1245
30	65.5208	65.5509	65.581	65.6111	65.6412
35	65.8649	65.8761	65.8873	65.8985	65.9097
40	66.1208	66.1298	66.1388	66.1478	66.1568

A high network throughput signifies data transfer for supporting bandwidth heavy activities like streaming, online gaming and real time communication. Network bandwidth, latency, packet loss and protocol efficiency are factors influencing network throughput. In this study, a NS3 to assess the throughput of proposed authentication protocol is assessed. The findings demonstrated that proposed protocol maintained a level of throughput ensuring reliable data transmission even under varying network conditions. This validates its suitability, for applications requiring rapid data transfer. The relation between the throughputs with number of nodes is described in figure 4.4.

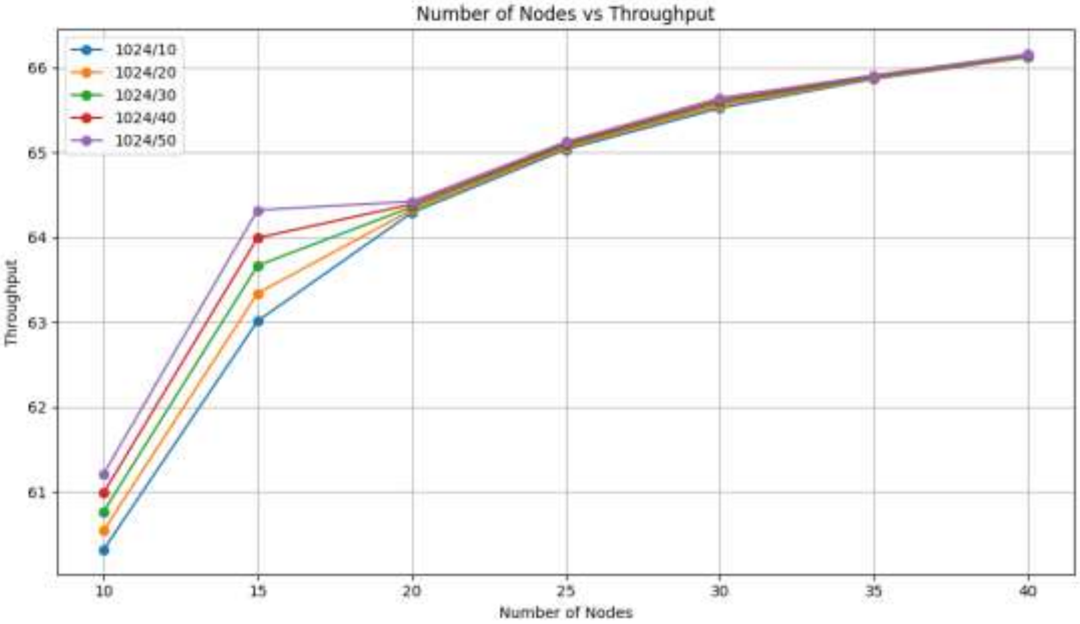


Figure 4.4: Relation between Throughput & number of nodes

The graph illustrates how the throughput changes with varying numbers of nodes, in setups, labelled as 1024/10, 1024/20, 1024/30, 1024/40 and 1024/50. The x axis represents the number of nodes from 10 to 40. The y axis indicates the throughput, which measures data processing capacity or performance. Each line corresponds to a configuration (1024/10, 1024/20, 1024/30, 1024/40, 1024/50) likely reflecting settings like block sizes or bandwidth limits. With an increase in nodes the throughput also rises across all configurations. This suggests that more nodes generally improve system throughput. There is a surge in throughput when moving from 10 to 20 nodes. This implies a benefit in increasing nodes up, to this point. When the number of nodes exceeds to 20, the increase in throughput indicates that adding nodes does not significantly improve throughput.

Initially there are variations in throughput among configurations. As the number of nodes increases the throughput levels for various setups become similar.

The configuration denoted as 1024/50 achieves throughput compared to others especially with a larger number of nodes. The graph illustrates that while increasing the node count generally enhances throughput the rate of improvement slows down after a threshold. Moreover different configurations have effects on throughput. These distinctions diminish as more nodes are added. It is noted that an increase in message exchanges corresponds to network throughput. Our systems throughput may be lower than systems due to using messages during login and authentication phases.

The thorough analysis validates that the proposed lightweight authentication method is highly efficient and suitable for environments. It ensures security, without impacting performance or resource usage. By balancing communication expenses while improving energy efficiency and maintaining latency this method effectively addresses IoT security challenges.

In the tasks the main focus will be, on applying these ideas in real life scenarios and making improvements to keep up with the latest IoT advancements. This thorough examination gives a view of the research carried out the techniques. The criteria employed to assess their efficiency. It is specifically designed for research purposes providing an understanding of both the practical sides of lightweight authentication, for IoT systems.

4.3 Simulation Analysis

NS3 is well known as an adaptable network simulator that offers simulation features and flexibility. It is capable of supporting network protocols and technologies allowing researchers to develop realistic network models. A key feature of NS3 is its design, which makes it easy for users to customize and expand by adding protocols and simulation scenarios. This flexibility is backed by simulation results ensuring performance evaluations of network systems. NS3 also provides documentation and a helpful community making it user friendly, for researchers at all levels of expertise. With its ability to simulate network structures and offer control over factors like traffic patterns and node movement NS3 stands out as a valuable tool, for driving networking research forward.

4.3.1 Performance Metrics

The simulation is set up using NS3 version 3.29 on a 64 bit Linux system. Initially during the simulation setup users and sensors are randomly placed within a 150x200 square meter area. Figure 4.5(a) and (b) presents NS3's visualization tool depicts a scenario where 3 gateways and 36 sensors are spread across the 150x200 square meter area. The message length is set at 1024 bytes and varying numbers of packets (10, 20 30 40 and 50) can be transmitted across the network. Each user sends messages every two milliseconds.

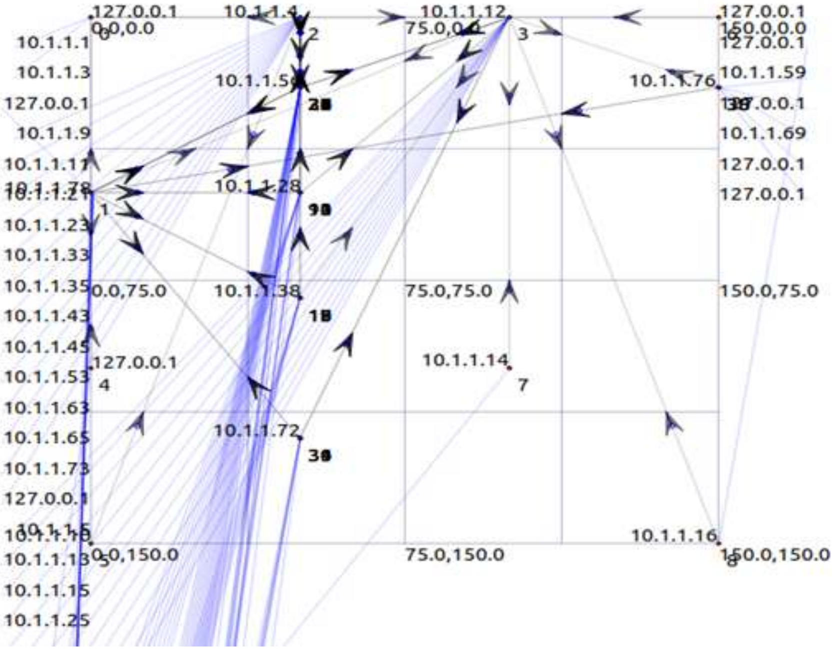
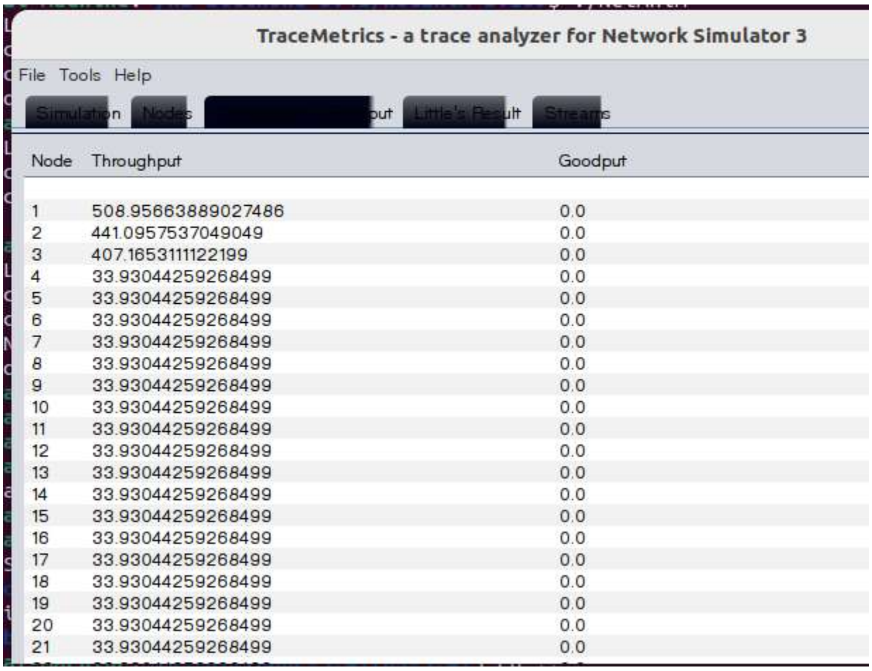


Figure 4.5(a) NS3 NetAnim Environment



Node	Throughput	Goodput
1	508.95663889027486	0.0
2	441.0957537049049	0.0
3	407.1653111122199	0.0
4	33.93044259268499	0.0
5	33.93044259268499	0.0
6	33.93044259268499	0.0
7	33.93044259268499	0.0
8	33.93044259268499	0.0
9	33.93044259268499	0.0
10	33.93044259268499	0.0
11	33.93044259268499	0.0
12	33.93044259268499	0.0
13	33.93044259268499	0.0
14	33.93044259268499	0.0
15	33.93044259268499	0.0
16	33.93044259268499	0.0
17	33.93044259268499	0.0
18	33.93044259268499	0.0
19	33.93044259268499	0.0
20	33.93044259268499	0.0
21	33.93044259268499	0.0

Figure 4.5(b) NS3 Tracemetrics Environment

The figure 4.5(b) shows a TraceMetrics window, which is a trace analyzer for Network Simulator 3 (NS-3), which displays node-wise throughput values. The values are explained in the following analysis: High Throughput Nodes (1-3) Node 1: 508.95 Mbps Node 2: 441.09 Mbps Node 3: 407.16 Mbps These nodes have a relatively high throughput, which indicates that they are the primary data sources, or hubs, or high bandwidth nodes in the network. Low Throughput Nodes (4-21) Node 4-21: 33.93 Mbps each. These nodes have a uniform and much lower throughput as opposed to nodes 1-3 which could be normal network nodes with lesser data throughput. All nodes have Goodput = 0.0. Goodput is the effective throughput (which considers no retransmissions, overhead etc.). The value of zero suggests that there are packet losses, no data is being delivered successfully or that there is an problem with the protocol. The nodes 1-3 could be the primary data sources with a high traffic load. Nodes 4-21 are secondary nodes that have limited data sharing. The absence of Good put could be due to network congestion, retransmission, or packet loss.

NS3 played a role in this research by providing an adaptable simulation platform that allowed achieving goals of examining, proposing, validating and analyzing lightweight authentication methods for IoT applications. Initially NS3 is enabled to investigate and assess lightweight authentication methods through detailed simulations that highlighted their performance metrics such, as throughput, end to end delay, computational costs, communication costs, lambda (authentication request arrival rate) and energy efficiency.

During the proposal phase of the research project, NS3's structure made it easier for us to incorporate and enhance the lightweight authentication approach. This method within the NS3 environment while optimizing it for IoT environments in analysed.

The testing environment allowed to try out this method in situations making sure it could handle the challenges faced by IoT devices, like limited processing power and battery life.

During the verification and validation phase, NS3's ability to mimic network conditions was incredibly helpful. Being able to adjust parameters helped us tune the authentication process keeping delays minimal for real time communication cutting down on costs for computation and communication to save device resources and optimizing energy usage for longer device life.

The functionality of simulating networks, in NS3 was evaluated to test how well it could handle a number of authentication requests without compromising performance. The analysis revealed that the straightforward authentication method managed to maintain a balance between security and efficiency for deployments. The extensive simulation features of NS3 were instrumental in demonstrating the practicality and effectiveness of the research findings. Specific instructions for implementing the proposed approach are available in Table 4.5.

Table 4.5: Parameters for Proposed Protocol

Name of Parameter	Values Assigned
Tool Used	ns3
Number of Nodes	10,15,20,25,30,35,40
Packet Length	1024 bytes
Number of Packets	10,20,30,40,50
Time Interval	2.0 seconds
Data Rate	5 Mbps
Delay	2 ms
Processor	11th Gen Intel(R) Core(TM) i5-11300H @ 3.10GHz
RAM	2 GB
OS	ubuntu-22.04.1
Virtual Environment	VMware-workstation-full-17.0.0-20800274

4.3.2 Implementation and Performance Evaluation

The mutual authentication protocol was created with a focus, on devices. Specific parameter values used in proposed protocol are outlined in Table 4.1. The performance of proposed implementation using the NS3 simulator selecting parameters for the experiment based on security requirements is assessed. The values obtained for communication cost by varying the number of nodes for the proposed approach and for the various researchers can be seen in table 4.6.

Table 4.6: Communication Cost Comparison

Authors	**bits used**
Ullah et. al.	340
L. Wang et. al.	720
M A Khan et. al.	1440
SadhuKhan	1600
Taher et. al.	1664
S. Garg	1792
J. Srinivas et. al.	1856
Esfahami et. al.	1920
A. Shahidinejad et. al.	1954
R. Amin	2048
D. Kwon et. al.	2080
S. Banerjee	2304
Liu et. al.	2490
Z. Zhao et. al.	2496
Zhang et. al.	2560
H Lee et. al.	2592
X. Li et. al.	2720
Chaudhary et. al.	2944
K. Park et. al.	3008
Proposed	3752
Z. Xu et. al.	3904
Wu. Et. al.	4800
G. Gaba et. al.	7400

A bar chart compares data usage and computational complexity among authors or research works as presented in figure 4.6. On the x axis are the bits used while author names are listed on the y axis. The bars are ordered from lowest to bits used. Ullah et al. and L. Wang et al. utilized, around 500 and 1000 bits. Following them M A Khan et al., SadhuKhan, Taher et al. and S. Garg used 1500 to 2000 bits. Some authors like J. Srinivas and team Esfahami and colleagues A. Shahidinejad et al. and R. Amin utilized between 2000 to 2500 bits in their work. On the hand researchers such as D. Kwon et al., S. Banerjee, Liu and team Z. Zhaos group, Zhangs collaborators and H

Lees associates exhibited an increase in bit usage with numbers hovering around 2500 to 3000 bits.

Moving on to higher bit consumption individuals like X. Li and co-authors, Chaudhary's team and K. Park et al. showcased a range of bit usage varying from about 3000 to 3500 bits. Additionally the proposed method possibly denoting a novel or recommended strategy employed over 4000 bits, placing it among the higher bit users without reaching the peak. Finally, in terms of the highest bit utilization observed in studies conducted by Z. Xu et al. they approached 5000 bits while Wu et. al. research surged close to the 6000 bit mark. Notably missing from this analysis is any data, on G. Gaba and associates bit utilization levels. The author group, at the top of the list uses over 7000 bits, which is much higher than any group mentioned. The chart shows a variation in the usage of bits among studies or approaches indicating differences in data complexity, encryption strength or computational needs, in their research.

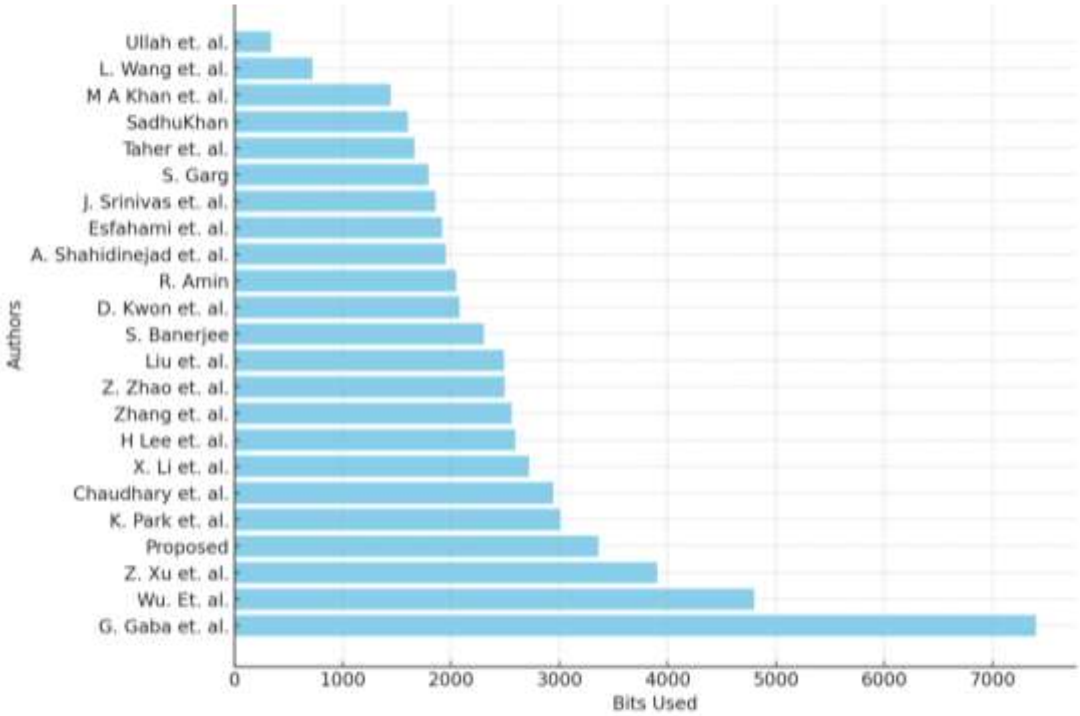


Figure 4.6: Comparison of Communication Cost of Proposed Approach

The chart in figure 4.7 illustrates a comparison of expenses, among researcher's methodologies with the horizontal axis showing the number of nodes and the vertical axis indicating the researchers involved. The horizontal Axis gauges the expenses based on the quantity of nodes. The farther to the right the greater the computational cost. Vertical Axis names the researchers who introduced approaches for computing tasks. Y. Qius technique incurs the expense surpassing 6 in value. Following closely are Ullah et al. and D. Kwon et al., whose methods demand computational resources, approaches by Hammi et al., Z. Liu, S. Banerjee, J. Srinivas et al., SadhuKhan, Z. Xu et al., Esfahami et al., Chaudhary et al., Alladi et al. And A. Shahidinejad et al. exhibiting computational costs. Table 4.7 highlights the values of computation cost for the proposed approach and the literature.

Table 4.7: Computation Cost Comparison

Author Name	**Configuration Used**	**Approach Used**	**Tool Used**	**Cost (sec)**
S. Garg	-	-	AVISPA	0.008
K. Park et. al.	Ubuntu 18.04 LTS	ROR/BAN LOGIC	NS2, AVISPA	0.01
Proposed	i5-11300H @ 3.10GHz, Ubuntu22.04, 2GB	SHA256	NS3	0.01349
A. Shahidinejad et. al.	-	-	AVISPA,MATLAB	0.016
Alladi et. al.	-	ECC	Proverif	0.022
S. A. Chaudhary et. al.	dual PC (E2200) with 2 GB RAM and 2.20 processor speed over Ubuntu OS	ECC	-	0.0224
Esfahami et. al.	-	ECC	AVISPA	0.052
Z. Xu et. al.	i7, 2.5 GHz, 8 GB, Win8	Hash + XOR	Proverif	0.0624
SadhuKhan	i7, 2.5 GHz, 4 GB, Win7	ECC	AVISPA	0.0806
J. Srinivas et. al.	Ubuntu 14.04 LTS	ECC	NS2, AVISPA	0.09542

S. Banerjee	Ubuntu 16.04, 2.4-GHz Wi-Fi	CBC AES-128	AVISPA	0.159
Z. Liu	-	PUF	NS3	0.2903
Hammi et. al.	2600/3100 MHz, 8 GB	SHA256/ECC	Java	0.57
D. Kwon et. al.	-	PUF/HASH/XOR	AVISPA	0.717
S. S. Ullah et. al.	i7, 2.5 GHz, 8 GB, Win7	ECC	AVISPA	1.92
Y. Qiu	i5, 1.7 GHz, 8 GB, Win7	MATLAB	Protocol Composition Logic (PCL), AVISPA	6.24

Proposed approach stands out for its computation, with one of the costs incurred, among all compared methods K. Park et al. And S. Garg require resources. This comparison shows how various computational techniques differ in their efficiency based on the number of nodes utilized reflecting the computing resources needed for each method.

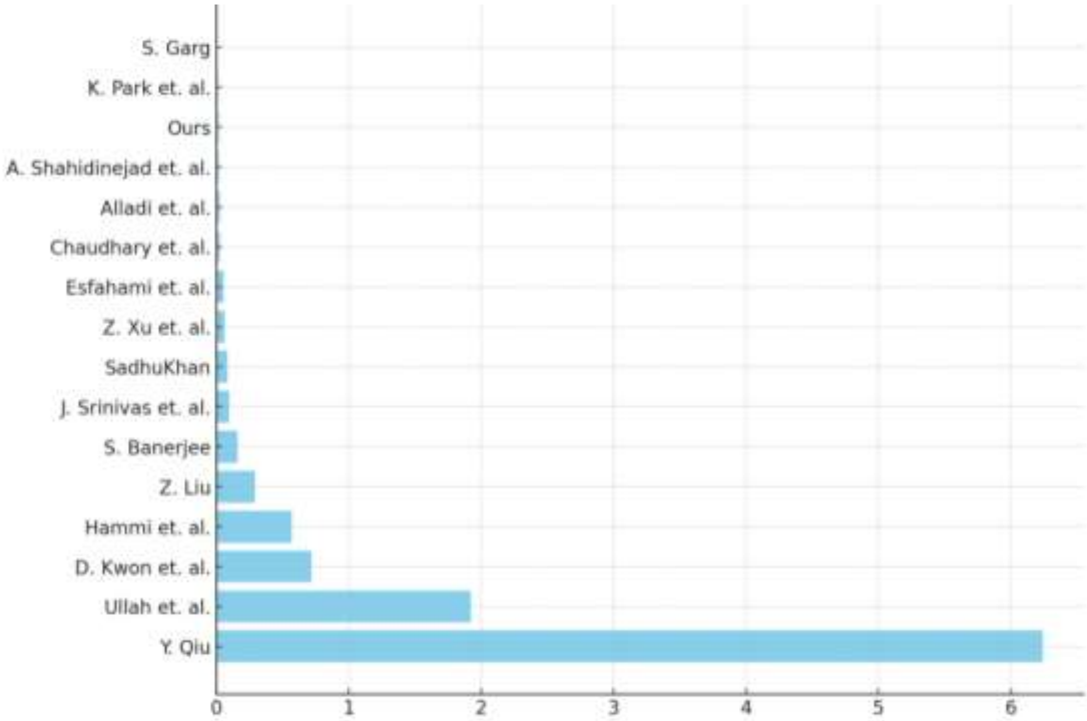


Figure 4.7: Comparison of Computation cost of Proposed Approach

Figure 4.8 given below displays the comparison of end to end delay with numbers of nodes as documented by various authors. On the X axis you can see the node counts where the end to end delay was measured, ranging from 5 to 600. The analysis of end to end delivery includes;

1. End to End Delay by Author Z. Liu et al.; This section displays the end to end delay times provided by Author Z. Liu and their team for node counts of 100, 200 300, 400 and 600. The delays range from 0.1191 to 0.2251 seconds.

2. End to End Delay by Author M.S. Albela et al.; Here the end to end delay times reported by Author M.S. Albela and colleagues for node counts of 100, 120, 160, 175, 200, 280, 350 and 400.The delays range from 0.09 to 0.6 seconds.

3. End to End Delay by Author K.Park et al.; This part lists the end to end delay times shared by Author K. Park and associates. Table 4.8 highlights the value of end to end delay for the proposed approach along with other researchers.

Table 4.8: End to End Delay Comparison

Z. Liu et. al.		M. S. Albela et. al.		K. Park et. al.		S. Banerjee et. al.		A K Das et. al.		S. Challa et. al.		Proposed	
N	**E2E Delay**	**N**	**E2E Delay**	**N**	**E2E Delay**	**N**	**E2E Delay**	**N**	**E2E Delay**	**N**	**E2E Delay**	**N**	**E2E Delay**
100	0.119	100	0.09										
		160	0.15			160	1.24						
200	0.141					200	1.44						
				25	0.769							25	0.6592
				30	0.101							30	0.7247
		350	0.46			350	1.6						
400	0.164	400	0.6			400	1.66			400	0.369		
								11	0.991			10	0.4373
								17	0.282			15	0.517
300	0.133	175	0.22			280	1.56	5	0.118	250	0.345		
		120	0.1			500	1.7			150	0.286		
600	0.225	280	0.35										
												20	0.528
												35	0.795
												40	0.845

Data is reported for node counts of 25 and 30 with delays of 0.77 and 0.10 seconds. The end, to end delay times from authors are as follows;

S. Banerjee et al.; Data is given for node counts of 160, 200 280, 350, 400 and 500 with delay times ranging from about 1.24 to 1.7 seconds.

A K Das et al.; Data is available for node counts of 5, 11 17 and 40 with delays ranging from around 0.12 to a second.

S. Challa et al.; End to end delay times are provided for node counts of 150,250 and400 with delays ranging from approximately0.29to0.37seconds.

The "Proposed" column displays suggested end to end delay times, for node counts.

The expected wait times are provided for numbers of nodes; 10, 15, 20, 25, 30, 35, and 40. The wait times range from, around half a second to under a second. The table shows how end to end delays vary based on authors reports and highlights the suggested values for comparison. The proposed approach seems to result in delays, at node counts particularly for larger numbers (150 nodes and beyond) indicating a more effective network performance.

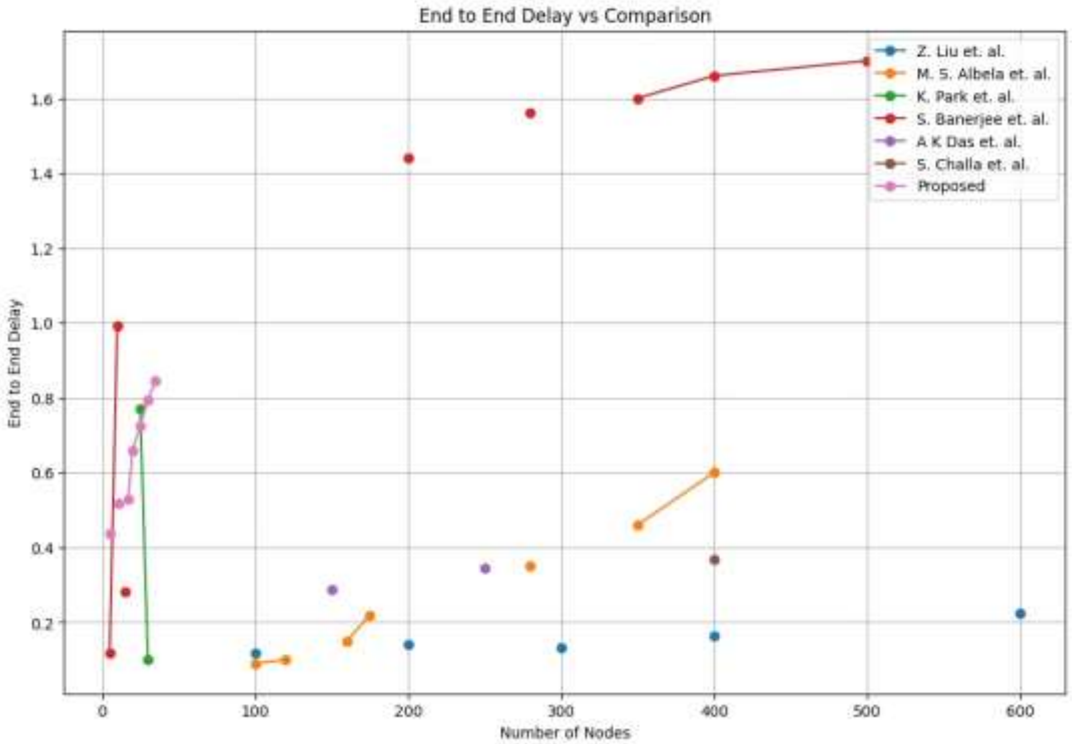


Figure 4.8: Comparison of End to End Delay of Proposed Approach

Figure 4.9 is designed to show how well author’s methods perform in terms of data transmission efficiency across network sizes. Let’s dive into a breakdown of the elements, in the chart and the insights it offers. On the axis you'll find the number of nodes in the network ranging from 5 to 600 nodes indicating how scalable each approach is. The vertical axis represents the amount of data successfully transmitted, known as throughput for each method. Table 4.9 is presenting the throughput comparison with other authors.

Table 4.9: Throughput Comparison

Z. Liu et. al.		M. S. Albela et. al.		K. Park et. al.		S. Banerjee et. al.		A K Das et. al.		S. Challa et. al.		Proposed	
N	**Th**	**N**	**Th**	**N**	**Th**	**N**	**Th**	**N**	**Th**	**N**	**Th**	**N**	**Th**
100	262.7	100	21			160	36	5	9.49	150	286.84	10	60.7662
200	276.1	120	24			200	42	11	16.07	250	489.51	15	63.667
300	280.4	160	30			280	58	17	22.54			20	64.3552
				25	46.8							25	65.0789
				30	55.9							30	65.581
		175	38			500	110					35	65.8873
600	544.4					350	78					40	66.1388
		280	50										
		350	60										
400	530.2	400	70			400	86			400	733.49		

For node counts ranging from 5 to 20 only data for authors S. Banerjee and S. Challa are available, with S. Challa demonstrating throughput performance. For a node count range of 25 40 the data, from M. S. Albela and S. Challa suggests that S. Challa consistently achieves throughput compared to M. S. Albela. In scenarios with a node count ranging from 100 to 600; Data provided by Z. Liu, M. S. Albela, A K Das and S. Challa is considered. Notably as the number of nodes increases S. Challa demonstrates an increase in throughput showcasing scalability. While Z. Liu and A K Das also exhibit throughput levels they do not reach the heights as S. Challa. Scalability wise it is evident that S. Challas approach exhibits superior scalability with the highest throughput values observed, especially at larger node counts. When comparing performance at node counts; At 100 nodes Z. Lius method outshines others significantly. At 400 nodes A K Das showcases a level of throughput ranking second to S. Challa. The graphical representation aids in illustrating which methods prove effective, across scales facilitating the selection of an optimal approach based on network size.

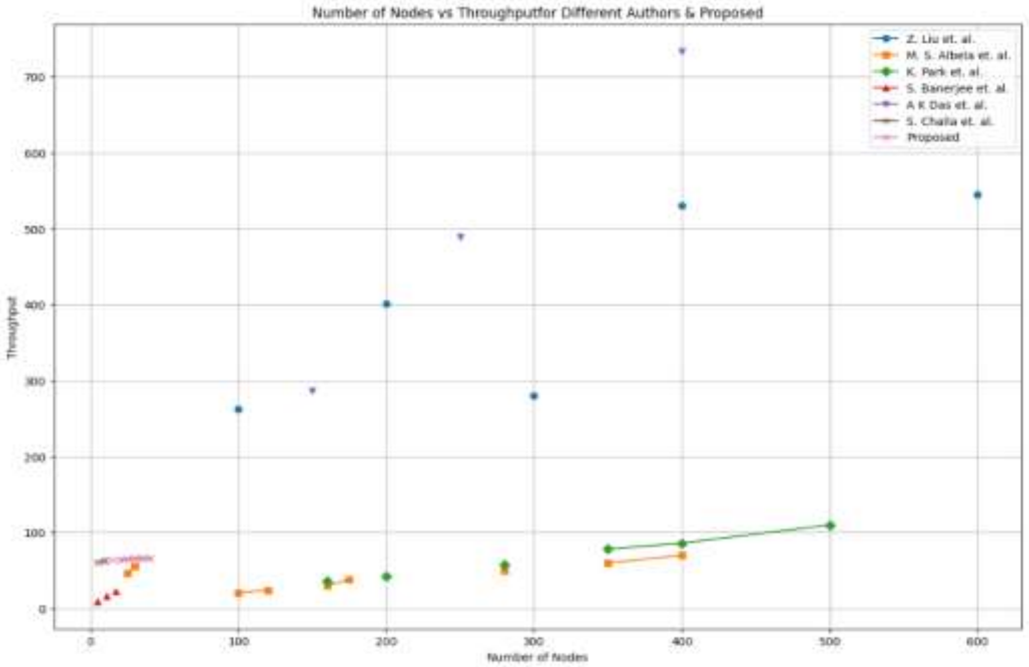


Figure 4.9: Comparison of Throughput of Proposed Approach

CONCLUSION AND FUTURE SCOPE

CHAPTER-5

5.1 Conclusion

The study described here introduces an authentication system specifically tailored for Internet of Things (IoT) devices. The inspiration, behind this research arises from the shortcomings and weaknesses of authentication approaches, which frequently depend on third party servers. These standard methods are not susceptible to security breaches and single points of failure. Also bring about significant computational and communication burdens that are not suitable for the limited resources of most IoT devices. As a result the study seeks to create an authentication protocol that addresses these issues while ensuring effective and scalable communication within environments.

The proposed technique makes use of fog gateways positioned strategically between devices and cloud servers to handle authentication tasks. By leveraging fog computing the protocol can shift computations from devices to the cloud layer conserving the resources of these devices. This design decision is particularly advantageous in lessening the load on devices with restricted processing power and battery life while enhancing the overall system efficiency.

A key aspect of this research is the comparison, between the proposed authentication protocol and existing methods utilizing RSA and ECC algorithms.

The study compares performance measures, such, as the time taken from start to finish, computational expenses, and communication expenses and data transfer rate. The results show that the new approach significantly lowers both the workload and communication burden compared to methods. This improvement is achieved by optimizing encryption processes and reducing the number of message exchanges needed during authentication. The decrease in complexity of computations and communication costs not boosts the systems effectiveness. Also prolongs the operational life of IoT devices by conserving power.

Regarding network performance the suggested protocol exhibits scalability and reliability. The NS3 simulation environment was used to test the protocol under network conditions and security threats like man in the middle attacks and replay attacks. The simulation outcomes demonstrate that the protocol maintains an end to end delay and high data transfer rate with an increasing number of devices in the network. These attributes are crucial for time applications where prompt and dependable data transmission is essential. Furthermore the protocols resistance to network attacks highlights its potential to establish a communication framework, for IoT systems.

In summary the study has successfully devised a effective and secure authentication mechanism for devices by leveraging the benefits of fog computing. The proposed protocol tackles the shortcomings of authentication methods by providing a decentralized resource efficient solution. Its capacity to uphold communication costs while ensuring strong security measures and scalability positions it as a viable choice for various IoT applications. This research not enriches the landscape of IoT security but also holds practical implications, for bolstering the security and efficiency of IoT systems across different industries.

5.2 Future Scope

The potential future of this study involves improving the suggested verification method to adjust to the movement of IoT gadgets connect with fog devices and cooperate with cloud settings. With IoT gadgets turning mobile in scenarios, like vehicles, wearables and drones there is a rising requirement to modify authentication procedures to manage the changing movements of devices and diverse connectivity options.

Let’s improve the suggested simple authentication method to better suit the movement of gadgets.

- Connect it with fog devices. Guarantee compatibility, with cloud environments.
- Adjust authentication protocols to handle the changing nature of device motion and different connectivity for IoT applications such as smart vehicles, wearable tech and drones.
- Include location based authentication methods using the Euclidean distance formula;

- Determine the distance between IoT gadgets and fog nodes or other reference points.
- Confirm the closeness of devices as a part of the verification process.

This approach works well for situations that need details to ensure that devices are within a physical range to access certain services or resources. Use real time location information to set up geo fencing and location aware services boosting security and offering context functionalities.

Incorporate fog computing into the verification system for advantages;

- Fog devices placed nearer to the network edge offer localized data processing, storage and analysis.
- Decrease latency and bandwidth consumption linked with communication with servers.
- Enable management of mobile IoT gadgets particularly in scenarios where low latency and quick responses are crucial. Look into enhancing the handover procedure, between fog nodes as devices shift positions ensuring secure connectivity without compromising user satisfaction.
- Maintain the ability for systems to work together smoothly and grow in size in cloud settings;
- Manage a number of gadgets and changing network situations as the implementation of IoT expands.
- Look into combined structures that make use of both fog and cloud resources to distribute work evenly and make the use of the resources available.
- Research advanced ways of encoding information and technologies, like blockchain spread across network levels to boost the reliability and credibility of the authentication process.
- Concentrate on creating adaptive and secure authentication answers that take into account how IoT gadgets move what fog computing can. How scalable cloud environments are;
- Integrate location verification using the Euclidean distance formula.
- Fine tune resource sharing between fog and cloud layers.
- Ensure transitions for devices.

- Enhance the safety and effectiveness of setups catering to the increasing variety and complexity of applications, in different sectors.

In conclusion, future research should focus on developing more adaptive and secure authentication solutions that consider the mobility of IoT devices, the capabilities of fog computing, and the scalability of cloud environments. By incorporating the Euclidean distance formula for location verification, optimizing resource allocation between fog and cloud layers, and ensuring seamless device handovers, utilizing hyper elliptical curve algorithm the proposed system can be made more robust and efficient. These advancements will not only improve the security and efficiency of IoT systems but also support the growing diversity and complexity of IoT applications in various industries.

BIBLIOGRAPHY

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, vol. 40, no. 8, pp. 102–114, Aug. 2002, doi: 10.1109/MCOM.2002.1024422.

[2] I. F. Akyildiz and I. H. Kasimoglu, “Wireless sensor and actor networks: research challenges”, vol. 2, no. 4, pp. 351–367, Aug. 2004, doi: https://doi.org/10.1016/j.adhoc.2004.04.003.

[3] D. Mpitziopoulos, C. Gavalas, Konstantopoulos and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs”, vol. 11, no. 4, pp. 42–56, Oct. 2009, doi: 10.1109/SURV.2009.090404.

[4] G. Codeluppi, A. Cilfone, L. Davoliand G. Ferrari, “LoRaFarM: A LoRaWAN-Based Smart Farming Modular IoT Architecture”, vol. 20, no. 7, p. 2028, Aug. 2020, doi: 10.3390/s20072028.

[5] F. Li and P. Xiong, “Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things”, vol. 13, no. 10, pp. 3677–3684, Oct. 2013, doi: 10.1109/JSEN.2013.2262271.

[6] K. Zhao and L. Ge, “A Survey on the Internet of Things Security”, pp. 663–667, Aug. 2013, doi: 10.1109/CIS.2013.145.

[7] J. Granjal, E. Monteiro and J. S. Silva, “End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication”, pp. 1–9, Aug. 2013.

[8] S. Guicheng and Y. Zhen, “Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things”, in *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Beijing, China, Aug. 2013. doi: 10.1109/IIH-MSP.2013.118.

[9] B. S. Adiga, M. A. Rajan, R. Shastry, V. L. Shivraj and P. Balamuralidhar, “Lightweight IBE scheme for Wireless Sensor nodes”, in *2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Kattankulathur, India, Aug. 2013. doi: 10.1109/ANTS.2013.6802866.

[10] M. Ryan, “Bluetooth: with low energy comes low security”, in *7th USENIX conference on Offensive Technologies (WOOT'13),* USA: USENIX Association, Aug. 2013.

[11] T. Rosa, “Bypassing Passkey Authentication in Bluetooth Low Energy”, in *IACR Cryptol. ePrint Arch.,* Aug. 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:16694199.

[12] L. Wei, Z. Luo, Q. Qu, Q. He and J. Xu, “A Low-Cost PKC-based RFID Authentication Protocol and its Implementation”, in *2014 Tenth International Conference on Computational Intelligence and Security,* Aug. 2014. doi: 10.1109/CIS.2014.134.

[13] B. A. A. Nunes, M. Mendonca, X. -N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014, doi: 10.1109/SURV.2014.012214.00180.

[14] H. Ning, H. Liu and L. T. Yang, “Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things”, in *IEEE Transactions on Parallel and Distributed Systems,* Mar. 2015. doi: 10.1109/TPDS.2014.2311791.

[15] T. D. P. Bai and S. A. Rabara, “Design and Development of Integrated, Secured and Intelligent Architecture for Internet of Things and Cloud Computing”, in *3rd International Conference on Future Internet of Things and Cloud*, Rome, Italy, Aug. 2015. doi: 10.1109/FiCloud.2015.23.

[16] L. Feng and X. Yao, “RFID System Mutual Authentication Protocols Based on ECC”, in *2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom),* Beijing, China, Aug. 2015. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.299.

[17] M. M. Hossain, M. Fotouhi and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things”, in *IEEE*

World Congress on Services, New York, NY, USA, Aug. 2015. doi: 10.1109/SERVICES.2015.12.

[18] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", in *IEEE Communications Surveys & Tutorials,* Aug. 2015. doi: 10.1109/COMST.2015.2388550.

[19] V. Vijayalakshmi, R. Sharmila and R. Shalini, "Hierarchical key management scheme using Hyper Elliptic Curve Cryptography in Wireless Sensor Networks", in *3rd International Conference on Signal Processing, Communication and Networking (ICSCN),* Chennai, India, Aug. 2015. doi: 10.1109/ICSCN.2015.7219840.

[20] L. Coppolino, V. D'Alessandro, S. D'Antonio, L. Levy and L. Romano, "My Smart Home is Under Attack", in *IEEE 18th International Conference on Computational Science and Engineering*, Porto, Portugal, Aug. 2015. doi: 10.1109/CSE.2015.28.

[21] Y. Qiu and M. Ma, "A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks", in *IEEE Transactions on Industrial Informatics*, Dec. 2016. doi: 10.1109/TII.2016.2604681.

[22] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks", IEEE Internet of Things Journal , vol. 3, no. 5, pp. 816–829, Oct. 2016, doi: 10.1109/JIOT.2016.2516102.

[23] S. Challa, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications", in *IEEE Access*, Aug. 2017. doi: 10.1109/ACCESS.2017.2676119.

[24] N. Li, D. Liu and S. Nepal, "Lightweight Mutual Authentication for IoT and Its Applications", IEEE Transactions on Sustainable Computing, vol. 2, no. 4, pp. 359–370, Oct. 2017, doi: 10.1109/TSUSC.2017.2716953.

[25] C. Wang, G. Xu and J. Sun, "An Enhanced Three-Factor User Authentication Scheme Using Elliptic Curve Cryptosystem for Wireless Sensor Networks", Sensors, vol. 17, no. 12, p. 2946, Aug. 2017, doi: https://doi.org/10.3390/s17122946.

[26] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah and J. Shen, “A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server”, in *Computers & Electrical Engineering*, Aug. 2017. doi: https://doi.org/10.1016/j.compeleceng.2017.04.012.

[27] P. Morgner, S. Mattejat, Z. Benenson, C. Müller and F. Armknecht, “Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning”, in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '17),* New York, NY, USA: Association for Computing Machinery, Aug. 2017. [Online]. Available: https://doi.org/10.1145/3098243.3098254.

[28] M. Ye, N. Jiang, H. Yang and Q. Yan, “Security analysis of Internet-of-Things: A case study of august smart lock”, in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* Aug. 2017. doi: 10.1109/INFCOMW.2017.8116427.

[29] M. Ge, J. B. Hong, W. Guttmann and D. S. Kim, “A framework for automating security analysis of the internet of things”, in Journal of Network and Computer Applications, Volume 83, 2017, Pages 12-27, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2017.01.033.

[30] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things”, in IEEE Internet of Things Journal vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[31] E. H. Teguig and Y. Touati, "Security in Wireless Sensor Network and IoT: An Elliptic Curves Cryptosystem based Approach," in *9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),* New York, NY, USA, Aug. 2018. doi: 10.1109/UEMCON.2018.8796578.

[32] V. Choudhary, D. S. Taruna and L. B. Purbey, “A Comparative Analysis of Cryptographic Keys and Security”, in *3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE),* Jaipur, India, Aug. 2018. doi: 10.1109/ICRAIE.2018.8710431.

[33] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas and L. Castedo, “A Practical Performance Comparison of ECC and RSA for Resource-

Constrained IoT Devices”, in *Global Internet of Things Summit (GIoTS)*, Aug. 2018. doi: 10.1109/GIOTS.2018.8534575.

[34] S. Jebri, M. Abid and A. Bouallegue, “LTAMA-Algorithm: Light and Trust Anonymous Mutual Authentication Algorithm for IoT”, in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, Porto, Portugal, Aug. 2018. doi: 10.1109/VTCSpring.2018.8417686.

[35] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal and V. Chang, “A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment”, in *Future Generation Computer Systems*, Volume 78, Part 3, Pages 1005-1019, Aug. 2018. doi: 10.1016/j.future.2016.12.028.

[36] D. Santhadevi and B. Janet, “Security Challenges in Computing System, Communication Technology and Protocols in IoT system”, in *International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, Kottayam, India, Aug. 2018. doi: 10.1109/ICCSDET.2018.8821074.

[37] H. A. Abdul-Ghani, D. Konstantas and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model”, International Journal of Advanced Computer Science and Applications(IJACSA), vol. 9, no. 3, Aug. 2018, [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2018.090349

[38] A. R. Sfar, E. Natalizio, Y. Challal and Z. Chtourou, “A roadmap for security challenges in the Internet of Things”, in *Digital Communications and Networks*, Volume 4, Issue 2, Pages 118-137, Aug. 2018. doi: https://doi.org/10.1016/j.dcan.2017.04.003.

[39] D. E. Kouicem, A. Bouabdallahand H. Lakhlef, “Internet of things security: A top-down survey”, in *Computer Networks*, Aug. 2018. doi: 10.1016/j.comnet.2018.03.012.

[40] D. V. Jose and A. Vijyalakshmi, “An Overview of Security in Internet of Things”, in *Procedia Computer Science*, Aug. 2018. doi: 10.1016/j.procs.2018.10.439.

[41] P. P. Ray, “A survey on Internet of Things architectures”, in Journal of King Saud University - Computer and Information Sciences, Volume 30, Issue 3,

2018, Pages 291-319, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2016.10.003.

[42] M. Ammar, G. Russello and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks”, in *Journal of Information Security and Applications*, Volume 38, Pages 8-27, Aug. 2018. doi: 10.1016/j.jisa.2017.11.002.

[43] A. Esfahani et. al. “A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment”, in *IEEE Internet of Things Journal*, Feb. 2019. doi: 10.1109/JIOT.2017.2737630.

[44] S. Dey and A. Hossain, “Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography”, in *IEEE Sensors Letters*, Apr. 2019. doi: 10.1109/LSENS.2019.2905020.

[45] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, “Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment”, in *IEEE Access*, vol. 7, pp. 55382-55397, Aug. 2019. doi: 10.1109/ACCESS.2019.2912998.

[46] Y. Chen, W. Xu, L. Peng and H. Zhang, “Light-Weight and Privacy-Preserving Authentication Protocol for Mobile Payments in the Context of IoT”, in *IEEE Access*, Aug. 2019. doi: 10.1109/ACCESS.2019.2894062.

[47] T. A. Ahanger and A. Aljumah, “Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms”, in *IEEE Access*, Aug. 2019. doi: 10.1109/ACCESS.2018.2876939.

[48] S. Banerjee, “A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment”, in *IEEE Internet of Things Journal*, Oct. 2019. doi: 10.1109/JIOT.2019.2923373.

[50] Z. Xu, C. Xu, W. Liang, J. Xu and H. Chen, “A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things”, in *IEEE Access*, Aug. 2019. doi: 10.1109/ACCESS.2019.2912870.

[51] Y. Yilmaz and B. Halak, “A Two-Flights Mutual Authentication for Energy-Constrained IoT Devices”, in *IEEE 4th International Verification and Security Workshop (IVSW)*, Aug. 2019. doi: 10.1109/IVSW.2019.8854438.

[52] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, “Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions”, in *IEEE Access*, Aug. 2019. doi: 10.1109/ACCESS.2019.2926578.

[53] A. Thantharate, C. Beard and P. Kankariya, “CoAP and MQTT Based Models to Deliver Software and Security Updates to IoT Devices over the Air”, in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* Atlanta, GA, USA, Aug. 2019. doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00183.

[54] Y. Harbi, Z. Aliouat and S. Harous, “A Review of Security in Internet of Things”, in *Wireless Pers Communication*, Aug. 2019. doi: https://doi.org/10.1007/s11277-019-06405-y.

[55] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures”, in *IEEE Access*, Aug. 2019. doi: 10.1109/ACCESS.2019.2924045.

[56] M. El-hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni, “A Survey of Internet of Things (IoT) Authentication Schemes”, in *Sensors*, May 2019. doi: https://doi.org/10.3390/s19051141.

[57] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, “A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)”, in *IEEE Systems Journal*, Sep. 2020. doi: 10.1109/JSYST.2020.2970167.

[58] J. Yu, S. Liu, S. Wang, Y. Xiao and B. Yan, “LH-ABSC: A Lightweight Hybrid Attribute-Based Signcryption Scheme for Cloud-Fog-Assisted IoT”, IEEE Internet of Things Journal , vol. 7, no. 9, pp. 7949–7966, Sep. 2020, doi: 10.1109/JIOT.2020.2992288.

[59] S. Garg, K. Kaur, G. Kaddoum and K. K. R. Choo, “Toward Secure and Provable Authentication for Internet of Things: Realizing Industry 4.0”, in *IEEE Internet of Things Journal*, May 2020. doi: 10.1109/JIOT.2019.2942271.

[60] P. Tedeschi, S. Sciancalepore, A. Eliyan and R. Di Pietro, “LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications”, in *IEEE Internet of Things Journal*, Jan. 2020. doi: 10.1109/JIOT.2019.2953549.

[61] P. Zhang, J. Liu, Y. Shen, H. Li and X. Jiang, “Lightweight Tag-Based PHY-Layer Authentication for IoT Devices in Smart Cities”, in *IEEE Internet of Things Journal*, May 2020. doi: 10.1109/JIOT.2019.2958079.

[62] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim and Y. Lee, “A three-factor anonymous user authentication scheme for Internet of Things environments”, in *Journal of Information Security and Applications,* Volume 52, Aug. 2020. doi: 10.1016/j.jisa.2020.102494.

[63] C. Trinh et. al., “A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments”, in *IEEE Access*, Aug. 2020. doi: 10.1109/ACCESS.2020.3021701.

[64] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, “A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)”, in *IEEE Systems Journal*, Sep. 2020. doi: 10.1109/JSYST.2020.2970167.

[65] S. A. Chaudhry, K. Yahya, F. Al-Turjman and M. H. Yang, “A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems”, in *IEEE Access*, Aug. 2020. doi: 10.1109/ACCESS.2020.3012121.

[66] W. Liu, X. Wang and W. Peng, “Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things”, in *IEEE Access*, Aug. 2020. doi: 10.1109/ACCESS.2019.2962912.

[67] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim, M. Liyanage and P. Kumar, “Robust and Lightweight Key Exchange (LKE) Protocol for Industry 4.0”, in *IEEE Access*, Aug. 2020. doi: 10.1109/ACCESS.2020.3010302.

[68] K. Park et. al., “LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification Table in Medical Internet of Things”, in *IEEE Access*, vol. 8, pp. 119387-119404, Aug. 2020. doi: 10.1109/ACCESS.2020.3005592.

[69] Z. Liu, C. Guo and B. Wang, “A Physically Secure, Lightweight Three-Factor and Anonymous User Authentication Protocol for IoT”, in *IEEE Access*, vol. 8, pp. 195914-195928, Aug. 2020. doi: 10.1109/ACCESS.2020.3034219.

[70] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, “Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication”, in IEEE Access, vol. 8, pp. 60539–60551, Aug. 2020, doi: 10.1109/ACCESS.2020.2983117.

[71] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim and P. Kumar, “Robust and Lightweight Mutual Authentication Scheme in Distributed Smart Environments”, in *IEEE Access*, vol. 8, pp. 69722–69733, Aug. 2020, doi: 10.1109/ACCESS.2020.2986480.

[72] M. Nakkar, R. Altawy and A. Youssef, “Lightweight Broadcast Authentication Protocol for Edge-Based Applications”, in *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11766-11777, Dec. 2020. doi: 10.1109/JIOT.2020.3002221.

[73] S. Atiewi et. al., “Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography”, in *IEEE Access*, vol. 8, pp. 113498-113511, Aug. 2020. doi: 10.1109/ACCESS.2020.3002815.

[74] L. Wang, H. An and Z. Chang, “Security Enhancement on a Lightweight Authentication Scheme With Anonymity Fog Computing Architecture”, in *IEEE Access*, vol. 8, pp. 97267-97278, Aug. 2020. doi: 10.1109/ACCESS.2020.2996264.

[75] S. Zhang, X. Du and X. Liu, “A Secure Remote Mutual Authentication Scheme Based on Chaotic Map for Underwater Acoustic Networks”, in *IEEE Access*, vol. 8, pp. 48285-48298, Aug. 2020. doi: 10.1109/ACCESS.2020.2979906.

[76] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, “A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data”, in *IEEE Access*, vol. 8, pp. 52018-52027, Aug. 2020. doi: 10.1109/ACCESS.2020.2980739.

[77] B. Zhao, P. Zhao and P. Fan, “ePUF: A lightweight double identity verification in IoT”, in *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 625-635, Oct. 2020. doi: 10.26599/TST.2019.9010072.

[78] J. Srinivas, A. K. Das, M. Wazid and N. Kumar, “Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things”, in *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133-1146, Nov. 2020. doi: 10.1109/TDSC.2018.2857811.

[79] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan and C. Chen, “A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems”, in *IEEE Systems Journal*, vol. 14, no. 1, pp. 39-50, Mar. 2020. doi: 10.1109/JSYST.2019.2899580.

[80] T. Alladi, S. Chakravarty, V. Chamola and M. Guizani, “A Lightweight Authentication and Attestation Scheme for In-Transit Vehicles in IoV Scenario”, in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14188-14197, Dec. 2020. doi: 10.1109/TVT.2020.3038834.

[81] X. Lu and X. Cheng, “A Secure and Lightweight Data Sharing Scheme for Internet of Medical Things”, in *IEEE Access*, vol. 8, pp. 5022-5030, Aug. 2020. doi: 10.1109/ACCESS.2019.2962729.

[82] S. S. Ullah et. al., “A Lightweight Identity-Based Signature Scheme for Mitigation of Content Poisoning Attack in Named Data Networking With Internet of Things”, in *IEEE Access*, vol. 8, pp. 98910-98928, Aug. 2020. doi: 10.1109/ACCESS.2020.2995080.

[83] W. C. Wang, Y. Yona, Y. Wu, S. N. Diggavi and P. Gupta, “SLATE: A Secure Lightweight Entity Authentication Hardware Primitive”, in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 276-285, Aug. 2020. doi: 10.1109/TIFS.2019.2919393.

[84] H. Mrabet, S. Belguith, A. Alhomoud and A. Jemai, “A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis”, in *Sensors*, no. 13: 3625, Jul. 2020. doi: 10.3390/s20133625.

[85] S. Jadhav, “Towards Light Weight Cryptography Schemes for Resource Constraint Devices in IoT”, in *Journal of Mobile Multimedia*, Aug. 2020. doi: 10.13052/jmm1550-4646.1521.

[86] K. Sha, T. A. Yang, W. Wei and S. Davari, “A survey of edge computing-based designs for IoT security”, in *Digital Communications and Networks*,

Volume 6, Issue 2, Pages 195-202, Aug. 2020. doi: 10.1016/j.dcan.2019.08.006.

[87] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues”, in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191-1221, April 2020. doi: 10.1109/COMST.2019.2962586.

[88] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi and K.-K. R. Choo, “A systematic literature review of blockchain cyber security”, in *Digital Communications and Networks*, Volume 6, Issue 2, 2020, Pages 147-156, Aug. 2020. doi: 10.1016/j.dcan.2019.01.005.

[89] B. Hussein Taher, H. Liu, F. Abedi, H. Lu, A. A. Yassin and A. J. Mohammed, “A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications”, in *Journal of Sensors*, vol. 2021, Article ID 8871204, 18 pages, Aug. 2021. doi: https://doi.org/10.1155/2021/8871204.

[90] M. Hossain and R. Hasan, “P-HIP: A Lightweight and Privacy-Aware Host Identity Protocol for Internet of Things”, in *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 555-571, Jan. 2021. doi: 10.1109/JIOT.2020.3009024.

[91] F. Farha, H. Ning, K. Ali, L. Chen and C. Nugent, “SRAM-PUF-Based Entities Authentication Scheme for Resource-Constrained IoT Devices”, in *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5904-5913, Apr. 2021. doi: 10.1109/JIOT.2020.3032518.

[92] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar and S. Kumari, “Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment”, in *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 57-63, Mar. 2022. doi: 10.1109/MCE.2021.3053543.

[93] D. Sadhukhan, S. Ray and G. P. Biswas, “A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography”, in *Journal of Supercomputers*, pp. 1114–1151, Aug. 2021. doi: https://doi.org/10.1007/s11227-020-03318-7.

[94] H. Huang, S. Lu and Z. Wu, “An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture”,

in *Journal of Wireless Communication Network*, August 2021. doi: https://doi.org/10.1186/s13638-021-02022-1.

[95] D. Kwon, Y. Park and Y. Park, "Provably Secure Three-Factor-Based Mutual Authentication Scheme with PUF for Wireless Medical Sensor Networks", in *Sensors,* no. 18: 6039, Aug. 2021. doi: 10.3390/s21186039.

[96] A. K. Sahu, S. Sharma and D. Puthal, "Lightweight Multi-party Authentication and Key Agreement Protocol in IoT-based E-Healthcare Service", in *ACM Trans. Multimedia Comput. Communication Application*, Jun. 2021. doi: 10.1145/3398039.

[97] S. Banerjee, A. K. Das, S. Chattopadhyay, S. S. Jamal, J. J. P. C. Rodrigues and Y. Park, "Lightweight Failover Authentication Mechanism for IoT-Based Fog Computing Environment", in *Electronics,* no. 12: 1417, Aug. 2021. doi: 10.3390/electronics10121417.

[98] Z. Zhao, C. Hsu, L. Harn, Q. Yangand L. Ke, "Lightweight Privacy-Preserving Data Sharing Scheme for Internet of Medical Things", in *Wireless Communications and Mobile Computing*, vol. 2021, August 2021. [Article ID 8402138, 13 pages]. Available: https://doi.org/10.1155/2021/8402138

[99] J. Xu, Q. Meng, J. Wu, J. X. Zheng, X. Zhang and S. Sharma, "Efficient and Lightweight Data Streaming Authentication in Industrial Control and Automation Systems", in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4279-4287, Jun. 2021. doi: 10.1109/TII.2020.3008012.

[100] I. A. Kazi, M. Tahir, M. H. Habaebi, S. L. Lau and A. Ahad, "Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction", in *Sensors*, no. 15: 5122, Aug. 2021. doi: 10.3390/s21155122.

[101] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends", in *Journal of Network and Computer Applications,* Aug. 2021. doi: 10.1016/j.jnca.2021.103164.

[102] B. Pradhan, S. Bhattacharyyaand K. Pal, "IoT-Based Applications in Healthcare Devices", in *Journal of Healthcare Engineering,* Article ID 6632599, 18 pages, Aug. 2021. doi: https://doi.org/10.1155/2021/6632599.

[103] S. S. Ullah, S. Hussain, A. Gumaei, M. S. Alhilal and B. F. Alkhamees, “A cost-effective approach for NDN-based internet of medical things deployment”, in *Computers, Materials & Continua,* vol. 70, no.1, pp. 233–249, Aug. 2022.

[104] S. K. Das, F. Benkhelifa, Y. Sun, H. Abumarshoud, Q. H. Abbasi and M. A. Imran, “Comprehensive Review on ML-based RIS-enhanced IoT Systems: Basics, Research Progress and Future Challenges”, in *TechRxiv,* Aug. 2022. [Preprint]. Available: https://doi.org/10.36227/techrxiv.19417283.v2.

[105] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen and B. Stiller, “Landscape of IoT security”, in *Computer Science Review,* Volume 44, 100467, Aug. 2022. doi: 10.1016/j.cosrev.2022.100467.

[106] J. Xu, B. Guand G. Tian, “Review of agricultural IoT technology”, in *Artificial Intelligence in Agriculture*, Volume 6, Pages 10-22, Aug. 2022. doi: https://doi.org/10.1016/j.aiia.2022.01.001.

[107] K. Lakshmanna, “A Review on Deep Learning Techniques for IoT Data”, in *Electronics* 11, no. 10: 1604, Aug. 2022. doi: 10.3390/electronics11101604.

[108] A. Koohang, C. Sargent, J. Nordand J. Paliszkiewicz, “Internet of Things (IoT): From awareness to continued use”, in *International Journal of Information Management*, Aug. 2022. doi: 10.1016/j.ijinfomgt.2021.102442.

[109] A. A. Laghari, K. Wu, R. A. Laghari et. al., “RETRACTED ARTICLE: A Review and State of Art of Internet of Things (IoT)”, in *Arch Computat Methods Eng*ineering 29, 1395–1413 Aug. 2022. doi: https://doi.org/10.1007/s11831-021-09622-6.

[110] S. Krishnamoorthy, A. Dua and S. Gupta, “Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions”, in *J Ambient Intelligence Human Comput* 14, 361–407, Aug. 2023. doi: https://doi.org/10.1007/s12652-021-03302-w.

[111] M. O. Qays, I. Ahmad, A. Abu-Siada, M. L. Hossainand F. Yasmin, “Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review”, in *Energy Reports*, Volume 9, Pages 2440-2452, Aug. 2023. doi: 10.1016/j.egyr.2023.01.085.

[112] H. Alrikabi, J. Kadhim and I. Aljazaery, “Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT”, in *International Journal of Emerging Technologies in Learning (iJET),* Aug. 2023. doi: 10.3991/ijet.v18i01.35987.

[113] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang and L. Shu, “Authentication Protocols for Internet of Things: A Comprehensive Survey”, in *Security and Communication Networks,* Aug. 2017. doi: https://doi.org/10.1155/2017/6562953.

[114] A. A. Fadele, M. Othman, I. A. Targio Hashemand F. Alotaibi, “Internet of Things security: A survey”, in *Journal of Network and Computer Applications,* Volume 88, Pages 10-28, Aug. 2017. doi: https://doi.org/10.1016/j.jnca.2017.04.002.

[115] S. Ahmed et al., "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC With DFA Countermeasure Strategies," in IEEE Access, vol. 13, pp. 22489-22509, 2025, doi: 10.1109/ACCESS.2025.3533611.

[116] X. Jin, N. Lin, Z. Li, W. Jiang, Y. Jia and Q. Li, "A Lightweight Authentication Scheme for Power IoT Based on PUF and Chebyshev Chaotic Map," in IEEE Access, vol. 12, pp. 83692-83706, 2024, doi: 10.1109/ACCESS.2024.3413853.

[117] W. Villegas-Ch, R. Gutierrez, A. M. Navarro and A. Mera-Navarrete, "Lightweight Blockchain for Authentication and Authorization in Resource-Constrained IoT Networks," in IEEE Access, doi: 10.1109/ACCESS.2025.3551261.

[118] M. Tanveer, A. A. A. El-Latif, A. U. Khan, M. Ahmad and A. A. Ateya, "LEAF-IIoT: Lightweight and Efficient Authentication Framework for the Industrial Internet of Things," in IEEE Access, vol. 12, pp. 31771-31787, 2024, doi: 10.1109/ACCESS.2024.3357090.

LIST OF PUBLICATIONS

S.No	Type of Paper (Journal Paper /Conference proceeding /Book Chapter)	Name of the Journal/ Conference/Book	Journal indexing (Scopus/UGC/Web of Science)	Title of the Paper	Published Date	Volume & Issue Number	ISSN/ ISBN Number	Impact Factor/ SJR	Type of paper (Research/ Review)	Weather this is thesis work or not (Yes/ No)	Web link of journal indexing
1	Journal Paper	Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology	SCI	Lightweight Security for IoT	04-Oct-23	Volume 45, Issue No 4	DOI: 10.3233/JIFS-232388	1.7	Research	Yes	Lightweight Security for IoT - IOS Press
2	Journal Paper	Kexue Tongbao /Chinese Science Bulletin	Scopus	Mutual Authentication based Lightweight Security for IoT	25-May-24	Volume - 69, Issue - 04	ISSN: 0023-074X	NA	Research	Yes	Mutual Authentication based Lightweight Security for IoT (kex

											uetongbao-csb.com)
3	Conference Proceeding	2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)	IEEE	Study and Analysis of IOT Security	09-Mar-22	NA	978-1-6654-3811-7	NA	Review	Yes	Study and Analysis of IOT Security | IEEE Conference Publication | IEEE Xplore
4	Conference Proceeding	1st International Conference on Artificial Intelligence and its Applications	Springer	A Survey on Blockchain Based Secure Transactions in IoT	18-19 Dec 23	NA	NA	NA	Review	Yes	NOT AVAILABLE YET

5	Journal Paper	Journal of Advances in Nonlinear Variational Inequalities		Security Enhancement for IoT using Mutual Authentication based Lightweight Algorithm	November 24	Vol 28 No. 1s (2025)	1092-910X	0.1	Research	Yes	Security Enhancement for IoT using Mutual Authentication Based Lightweight Algorithm | Advances in Nonlinear Variational Inequalities

LIST OF WORKSHOPS

S. N.	Title	Dates	Organized By
1	FDP On Research Essentials	31st Jan'22- 5 Feb'22	Chandigarh University Mohali
2	FDP On The Internet Of Things & Everything – IOT/IOE	2021-07-26 to 2021-07-30	University Institute Of Engineering, Chandigarh University, Mohali
3	FDP On Research Trends In Data Analytics, Information Security And Its Applications	9th March to 13th March, 2022	Chandigarh University, Mohali
4	ATAL FDP on Artificial Intelligence	25-05-2020 to 29-05-2020	NITTTR, CHANDIGARH
5	ATAL FDP on Internet Of Things(IoT)	25-11-2019 to 29-11-2019	NITTTR, CHANDIGARH
6	FDP On Cloud, Fog And Edge Computing	14/04/2020 to 18/04/2020	NITTTR, CHANDIGARH
7	ATAL FDP on Augmented Reality (AR) / Virtual Reality (VR)	11-05-2020 to 15-05-2020	NITTTR, CHANDIGARH
8	FDP On Java	17 May, 2020 to 22 May, 2020	Spoken Tutorial, IIT Bombay AISSMS Polytechnic
9	FDP On Cyber Security	08/06/2020 to 19/06/2020	NITTTR, CHANDIGARH
10	FDP On Linux	5th April 2021 to 10th April 2021	E & ICT Academy, IIT Kanpur
11	FDP On Cyber Security	12th April 2021 to 17th April 2021	E & ICT Academy, IIT Kanpur
12	FDP On Data Science	15th Feb 2021 to 27th Feb 2021	E & ICT Academy, IIT Kanpur

13	FDP On Cloud Computing	26th April 2021 to 1st May 2021	E & ICT Academy, IIT Kanpur
14	FDP On Advanced Excel With Data Visualization	20th July 21 to 25th July 21	E & ICT Academy, IIT Kanpur
15	ATAL FDP on "Internet Of Things (IoT)	2021-03-15 to 2021-03-19	GOVERNMENT COLLEGE OF ENGINEERING
16	FDP On Python	19th April 2021 to 24th April 2021	E & ICT Academy, IIT Kanpur
17	ATAL FDP On "Digital Forensics And Anti-Forensics"	2022-12-05 to 2022-12-10 and 2022-12-12 to 2022-12-16	Indian Institute of Information Technology, Pune
18	ATAL FDP On Data Science And Cyber Security	08/01/2024 to 13/01/2024	JSPM'S BHIVARABAI SAWANT INSTITUTE OF TECHNOLOGY & RESEARCH
19	One Week Online Short Term Course On Machine Learning And Its Applications In Iot, Computer Vision And Cloud Computing	July 10-14 2023	Department of Computer Science and Engineering, National Institute of Technology Jamshedpur
20	FDP On RESEARCH METHODOLOGY	12th December - 19th December, 2022	Department of Commerce, PPG College of Arts and Science, Coimbatore
21	FDP On Recent Trends In Computational Approaches	2nd January to 6th January 2024	Department of Information Technology, Narula Institute of Technology, Kolkata
22	IBM FDP On Computational Thinking And Cyber	26th to 30th December 2023	JSPM University, Pune

	Security		
23	FDP On Teaching And Research Essentials	26th June 23 to 1st July 23	Chandigarh University Mohali
24	Microsoft, SAP And AICTE FDP On AI Evolution: From Foundations To Generative AI	22nd Jan 24 to 27th Jan 24	JSPM University, Pune
25	MM-TTP On NEP 2020 Orientation & Sensitization Programme	11th Mar 24 to 20th Mar 24	Dr. Babasaheb Ambedkar Marathwada University, Sambhaji Nagar
26	One Week International Workshop On Technical Writing Using Latex	30th Mar 24 to 5th Apr 24	VIT-AP University, Amravati
27	CSI Sponsored FDP On Cyber Intelligence And Awareness On Social Media Security V2.0	27th Nov 23 to 1st Dec 23	Institute of Engineering and Management, Saltlake
28	STTP In Machine Learning & Data Science Marvels	12th Mar 24 to 16th Mar 24	Bengal College of Engineering and Technology