ENHANCING DATA SECURITY IN CLOUD USING INTEGRATED CRYPTOGRAPHIC TRANSFORMATIONS

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

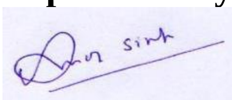
(Computer Applications)

By

Sartaj Singh

Registration number: 41800009

Supervised By



Prof. (Dr.) Amar Singh (23318)

School of Computer Applications

Lovely Professional University, Phagwara.

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

2024

DECLARATION

The work embodied in the thesis entitled, **"Enhancing Data Security in Cloud Using Integrated Cryptographic Transformations",** has been done by me and not submitted elsewhere for the award of any other degree. All the ideas and references have been duly acknowledged.

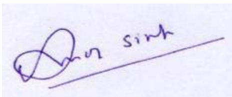
Dated: **Sartaj Singh**

CERTIFICATE

The work included in the thesis entitled, **"Enhancing Data Security in Cloud Using Integrated Cryptographic Transformations"** submitted to the **School of Computer Applications, Lovely Professional University, Phagwara,** for the degree of Doctor of Philosophy, was carried out by **Sartaj Singh** at the **School of Computer Applications, Phagwara** under my supervision. This is an original work and has not been submitted in part or full for any other degree/diploma at this or any other university/ institute. This thesis is fit to be considered for evaluation for the award of degree of Ph.D.

Dated:

Supervisor



Dr. Amar Singh
Professor
School of Computer Applications,
Lovely Professional University, Phagwara

ABSTRACT

In this thesis, we proposed a novel framework to secure data in the cloud. The proposed framework consists of data encryption and data security modules. We proposed an integrated BBBC (Big Bang – Big Crunch) and chaotic map-based approach in the data encryption module. In the proposed data encryption approach, we used the BBBC algorithm to evolve the optimal parameters of chaotic maps. From comparison results, we observed that the proposed approach outperformed the existing chaotic map-based data encryption technique.

Further, we proposed two approaches in the data security module of the proposed data security framework. The first approach is based upon two factors for data security. The second approach is based on multifactor. The multiple factors we considered for the authentication mechanism are passwords, smart cards, and biometric.

The thesis is divided into six chapters, summarized as follows:

Chapter 1 motivates the work, along with the problem formulation and thesis objectives.

Chapter 2 presents a state-of-the-art survey of the associated literature. This chapter is divided into two parts. Part I discusses various encryption and decryption approaches, specifically assessing their suitability for 2D chaotic maps encryption and decryption. Part II focuses on data security approaches for the cloud environment.

Chapter 3 presents a meta heuristic-based 2D Chaotic map approach for data encryption. We evolved the chaotic maps initial parameters with the BBBC algorithm in the proposed approach. BBBC algorithm helps to produce the complex and unpredictable key. For performance analysis purposes, We evaluated the performance proposed approach and compared it with existing genetic algorithm-based 2D Chaotic map approach. For comparison purposes, we tested it on different

character-sized text. From comparison results, we observed from the results that the proposed approach outperformed the existing one on all-sized text.

Chapter 4 proposes a novel approach to secure the data in the cloud environment. The proposed approach consists of multiple factors for user authentication. In the proposed approach, we considered multiple factors in the authentication mechanism, namely passwords, smart cards and biometric. The multiple factors for user authentication schemes ensure more data security on the cloud. We compare the proposed approach with the existing 7 available approaches for comparison purposes. The performance results show that the proposed user authentication scheme outperforms all existing approaches.

Chapter 5 proposes a lightweight data security approach for a cloud environment. The proposed approach is the two-factor-based user authentication scheme for data security on the cloud. The proposed scheme is lightweight as it uses a hash function and is thus suitable for practical applications. From the simulation results, we observed that the proposed scheme outperforms existing data security schemes.

Chapter 6 concludes the research work and outlines future avenues for further exploration.

ACKNOWLEDGEMENTS

I am deeply grateful to my research advisor **Dr. Amar Singh** for his motivating guidance throughout this research work. He provided me great freedom to choose a research topic of my interest and directed and critiqued me just in time. Without his inspiration, untiring efforts, enthusiastic attitude, and personal care, the accomplishment of this dissertation would have been impossible. I benefited enormously from her valuable feedback, logical analysis, and comments. His input was vital in shaping this work. He has been a great source of inspiration to me, and I would like to thank her from the core of my heart.

I would like to gratefully acknowledge the School of Computer Applications, Lovely Professional University (Punjab), India, for offering this doctorate program. The University and the department were always very cooperative in extending all the resource and infrastructure facilities during my research span. I am thankful to all the reviewers of my research manuscripts for providing valuable feedback and comments that helped me raise the standard of this research work. I also extend my special thanks to all the cited authors in my thesis whose research findings provide me a battleground to choose upon the research directions.

Words are inadequate to express my gratitude to my loving wife, **Sandeep Kaur,** for always being there for me. She never failed to give me great encouragement and confidence to finish my thesis. I am highly grateful to her for all the cooperation, affection, motivation, understanding, patience, and sincere advice. Her support and care helped me overcome setbacks and stay focused on my thesis. I greatly value her friendship and sincerely appreciate her belief in me.

I am also grateful to my father, **Sardar Kuldip Singh Deep,** and my mother, **Mrs. Ranjit Kaur,** for their best wishes and words of encouragement. They cheer me up during the walk through the journey towards attaining the Doctorate Degree. Also, I express my thanks to my other family members for always being with me at any stage during this work.

Above all, I firmly believe that everything in the world is happening as per the plan and will of the Almighty. So, I thank him for planning this and allowing me to do this thesis. I pray that he continues showering his grace and blessings onto me and all others.

Sartaj Singh

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

||	Concatenation Operation
AKE	Authentication and Key Exchange
AVISPA	Automatic Validation of Internet Security Protocols and Applications
AWS	Amazon Web Services
CL-AtSe	Constraint Logic based Attack Searcher
CNOT	Controlled-NOT operation
C2G	Citizen-to-Government (C2G)
DCT	Discrete Cosine Transform
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECG	Electrocardiogram
GHZ	Greenberger–Horne–Zeilinger
HMAC	Hashing Message Authentication Code
HLPSL	High Level Protocol Specification Language
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IF	Intermediate Format
IIoT	Industrial Internet of Things
IoT	Internet-of-Things
LAN	Local Area Network

MEC	Multipurpose Electronic Card
OF	Output Format
OFMC	On-the-fly Model-Checker
OOAD	Object Oriented Analysis and Design
PaaS	Platform-as-a-Service
PCA	Principal Component Analysis
PDS	Public Distribution System
QIA	Quantum Identity Authentication
QKD	Quantum Key Distribution
RFID	Radio Frequency Identification
RSA	Rivest Shamir Adleman
SaaS	Software-as-a-Service
SeDaSC	Secure Data Sharing in Clouds
T_E	Time Complexity for Exponential Operation
T_H	Time Complexity for Hash Function
T_S	Time Complexity for Symmetric Encryption
UML	Unified Modelling Language
WBAN	Wireless Body Area Networks
WSN	Wireless Sensor Networks
XOR	Bit-wise Exclusive OR Operation

Chapter – 1

INTRODUCTION

In the digital age, IT infrastructure is vital for data and apps. Cloud computing is on the rise, changing data center norms. Traditional centers yield to modern, agile methods. Cloud's scalability optimizes resources, while software-defined tech reshapes data centers. This evolution ensures efficient data management and dynamic adaptability. Different customers use the same basic hardware to execute the applications and data. There are high-security threats in the cloud environment due to high dependency on the multi-tendency cloud computing model. Cloud environments consist of security layers on both the server and customer side. Data Security is the primary issue of the cloud service providers. There is a high dependency of different organizations on cloud applications. It is a significant problem for cloud service providers to ensure data security on cloud servers and keep data secure and safe during transit.

The data on cloud servers is always at high risk because different clients ask for data stored on a shared server. We can use a data encryption and decryption algorithm for data security and transit. Another concern related to the cloud data store is the risk of losing data stored on the server’s memory. In a cloud environment, you are not having direct control over the storage media of the cloud server. Due to this lack of control, any external unauthenticated person can access confidential data while the system is executing.

Even if the unauthenticated person does not have direct control of the server, it can compromise the system security in different ways. The attacker can misuse the data, even if it is encrypted then he can delete the confidential data. During the data propagation there could be unauthorized access of data.

With cloud storage, you don't have complete control over the network and server infrastructure, which increases the risk of data interception by unauthorized individuals. These concerns highlight the importance of robust security measures and encryption protocols to safeguard data in cloud environments. A framework is required to prevent, harden, and avoid attacks. We aim to overcome the restriction of focusing on security borders with external and internal threats for the data and applications.

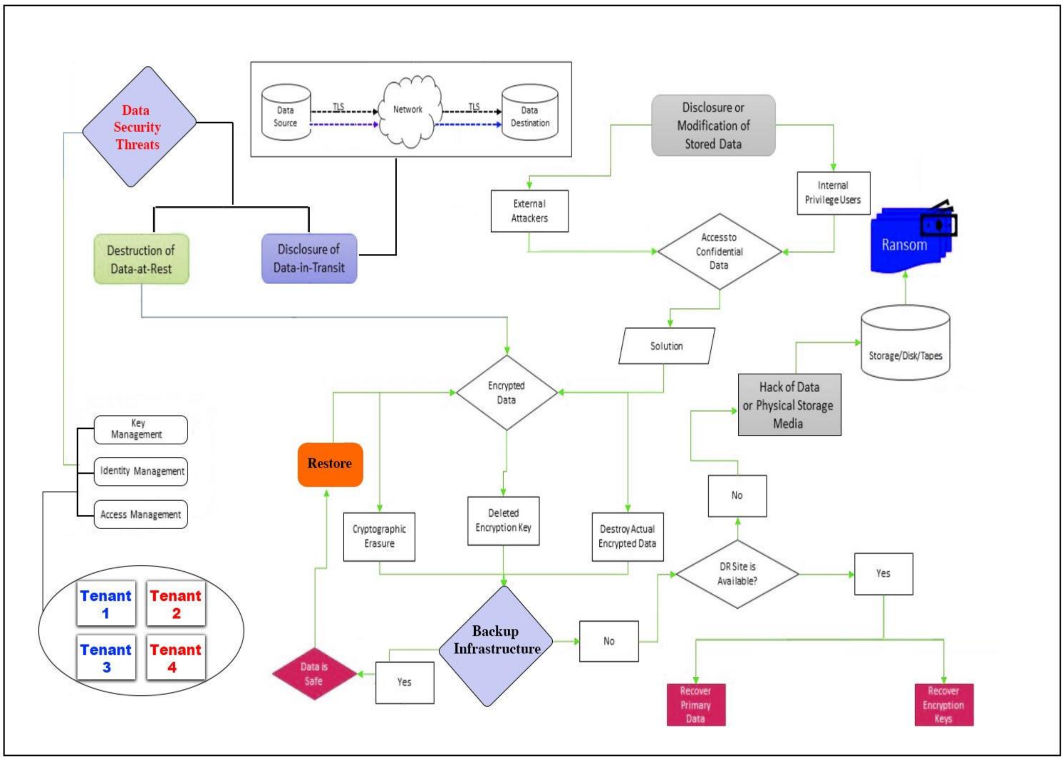


Figure 1.1: Architecture of emerging security threats.

In today's world, businesses are expanding rapidly, reaching global markets. Whether it's a small or large enterprise, IT infrastructure has become a crucial foundation for every aspect of the industry. Digitalization is now integral to every business model, driving the need for reliable IT systems.

As businesses grow larger, the scope of IT infrastructure also widens. Each day brings new challenges and requirements that demand the support of robust IT infrastructure to achieve business objectives efficiently and effectively. Embracing technological advancements helps accelerate business goals and stay competitive in the ever-changing market landscape. Hence, existing setups require both security and scalability. Each business model relies on hardware and software structures to sustain application needs in the given context. In order to host any application, the data centre must have some hardware and software. Assume you wish to expand your company abroad. In that situation, you must not rely on only your application, which can only be accessed with certain restrictions. Now, the query arises: Can our conventional data centers effectively handle and endure the challenges posed by the digital era and the interconnected global landscape?

1.1 CRYPTOGRAPHY

- **Symmetric-Key Algorithms**

Symmetric key algorithms employ a single secret key for both encrypting and decrypting data. This implies that both the sender (Samar) and the recipient (Binwant) must possess the identical key in order to communicate confidentially and securely. It ensures that only the intended recipient with the correct key can decrypt and understand the encrypted message. However, the main drawback of symmetric key algorithms is the need to share the secret key securely. Suppose an attacker gets hold of the shared key. In that case, they can easily decrypt the messages sent between Samar and Binwant, compromising the confidentiality of their communication.

Moreover, the attacker can impersonate Samar by encrypting a fake message with the shared key and sending it to Binwant, who couldn't detect the deception. To prevent such security risks, Samar and Binwant must take extra precautions to protect their shared key. It can include using secure communication channels, regularly changing the key, and implementing additional security measures like using digital signatures to ensure the authenticity of the messages.

- **Asymmetric-Key Algorithms**

Asymmetric encryption, also known as public-key encryption, is another fundamental type of data encryption. In this system, both parties, let's say, Alice and Bob, possess a pair of keys: a public key and a private key. The public key can be openly shared with anyone. In contrast, the private key must be kept confidential and only known to the owner. When Alice wants to send a message to Bob, she uses

Bob's public key to encrypt the message. Only Bob, who possesses the corresponding private key, can decrypt and read the message. This makes asymmetric encryption a powerful cryptographic method used in various technologies, including Bitcoin and secure communication systems. However, there are some drawbacks to consider. The keys used in asymmetric encryption tend to be longer than those in symmetric encryption, making encryption and decryption processes more time-consuming and computationally intensive. Moreover, associating a single encryption key with a single individual can have security weaknesses, significantly if the keys are compromised or not appropriately managed. Despite these challenges, asymmetric encryption remains a crucial tool for secure communication and digital signatures, providing a powerful way to protect sensitive information and enable secure transactions.

- **RSA (Rivest-Shamir-Adleman)**

Initially introduced to the public in 1978, RSA has emerged as the most widely used public-key cryptography algorithm. Its security lies in the ease of multiplying two large prime numbers while making it complex to factor the resulting product back into the original numbers.

It is challenging to determine a clear winner when comparing encryption methods, such as symmetric and asymmetric Encryption. Each method offers its advantages, and it is not feasible to exclusively choose one.

In the realm of security, asymmetric encryption gains an advantage by ensuring authentication and preventing repudiation. Nonetheless, the performance factor remains pivotal, leading to the ongoing use of symmetric encryption.

Table 1.1: Difference between Symmetric and Asymmetric Encryption

Sr. No.	Symmetric Key Encryption	Asymmetric key Encryption
1	A single key is used to encrypt and decode data.	A key pair is used for encryption and decryption. These keys are known as public and private keys.
2	It employs a single key and is a more straightforward encryption method.	It is a more complicated procedure.
3	Encryption is the primary use for Symmetric Encryption.	Encryption, authentication, and non-repudiation are all guaranteed by asymmetric encryption.
4	It has faster performance and uses less processing power.	Because of its complexity, it is slower than symmetric encryption and necessitates more computer resources.
5	Encryption keys with shorter lengths (128-256 bits) are employed.	Asymmetric encryption algorithms use longer keys (for example, 1024-4096 bits).
6	Ideal for applications requiring the encryption of massive amounts of data.	Ideal for applications that just need a small quantity of data secured.
7	The most often used symmetric encryption algorithms are RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC, EI Gamal, and DSA are examples of standard symmetric encryption algorithms.

1.2 SECURITY ISSUES OF DATA IN CLOUD ENVIRONMENT

According to the CSA research, data breach is the most serious threat to cloud computing. According to the CSA report, one of the top risks in cloud computing is data breach; data breach costs billions of dollars each year. In 2018, IBM Security and Ponemon Institute conducted a study that evaluated the cost of data breaches throughout the worldwide IT market [1]. It cost the organisation a lot of money, costing an average of $3.86 million, a 6.4 percent increase over 2017, and $148 each lost record1.

Data breaches is a serious issue and can happen from any layer of the cloud computing environment. Data breaches can cause financial loss and reputational damage. It can happen either from external or internal sources. Data breaches can occur due to human error, application vulnerability or poor security protocols. Data breach can be avoided by providing end-to-end control to cloud service providers and customers.

1.2.1 Data-at-Rest

Data-at-rest means the data is stored physically on the cloud computing infrastructure's storage media while not in active use. The data may be of any format, like text, data, or video files. The data could be encrypted on storage media so unauthenticated people could not read it. For encryption purposes, any data encryption algorithm could be used.

1.2.2 Data in Transit

Data in transit means the data could be moved from one location to another location in the cloud environment. The data is actively in transit from any node in the cloud to another node. For example, the data can be moved from server to user, user to server or server to server. Cloud service providers must ensure the data in transit privacy and security from unauthorized access and data tempering. Data can be secured by implementing data encryption, authentication, and other security measures.

1.2.3 Data Security Components in Cloud Envrionment

The different data security key components are shown in figure 1.2. CIA (Confidentiality, Integrity, Availability) is a framework to secure data in cloud envrionment [2]. For data security, It guides design, implementation and security measures.

1.2.3.1 Protection of Data: Data protection means to make data safe from varous security threats and unauthorized users.

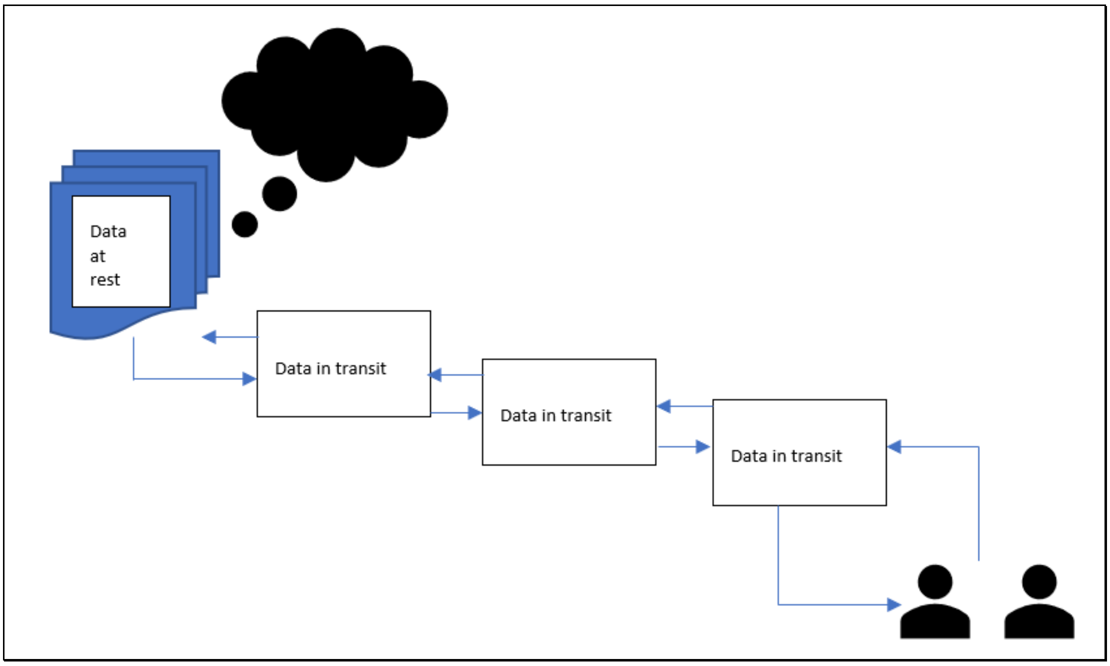


Fig. 1.2 : Data-at-Rest and Data-in-Transit.

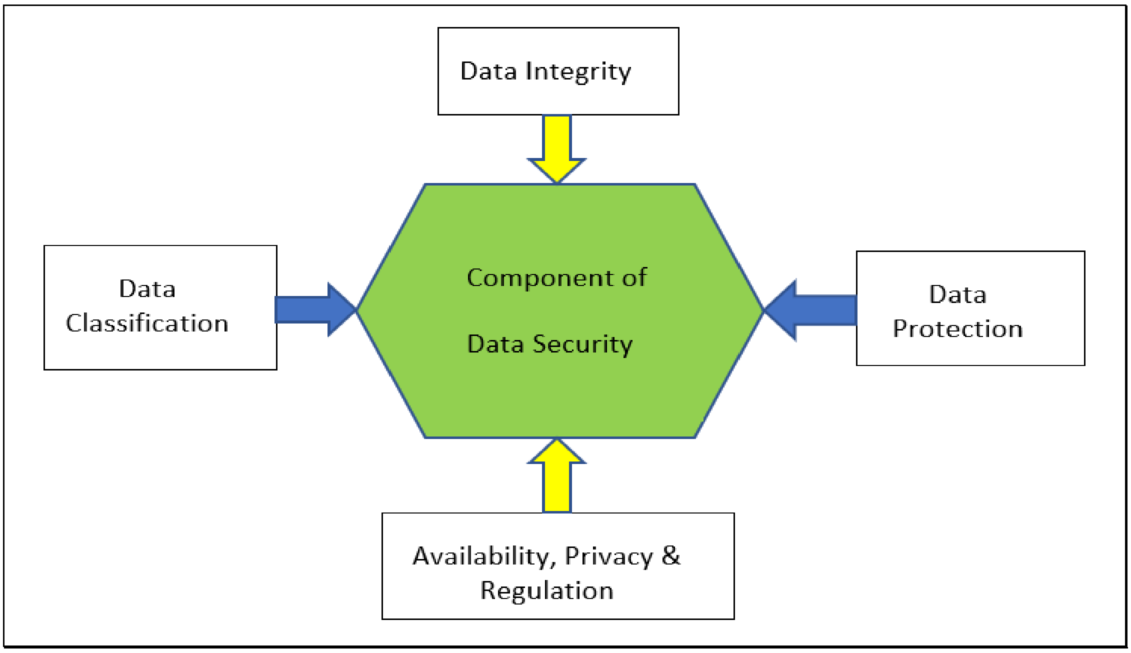


Fig. 1.3: Component of Data Security.

1.2.3.2 Classification of Data : The data could be categorized or classified according to its sensitivity, usage requirements and importance to users [3]. Data classification helps to the cloud environment to make decisions regarding how to handle and secure the data. The data classification component in the cloud environment can automatically discover and classify the data. For data classification purposes, we can use different types of tools like IBM and security guardian.

1.2.3.3 Data Integrity in Cloud Computing : Data integrity in cloud computing deals with maintaining accuracy, consistency and reliability of stored data. The data integrity ensures that the data on cloud secured from outsite tempring. Data integrity focuses to provide security on stored as well as transit data.

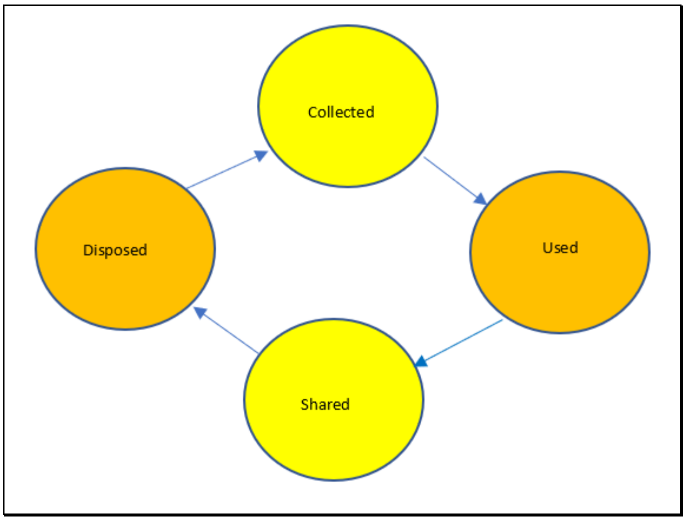


Fig. 1.4 : Data controlling mechanism.

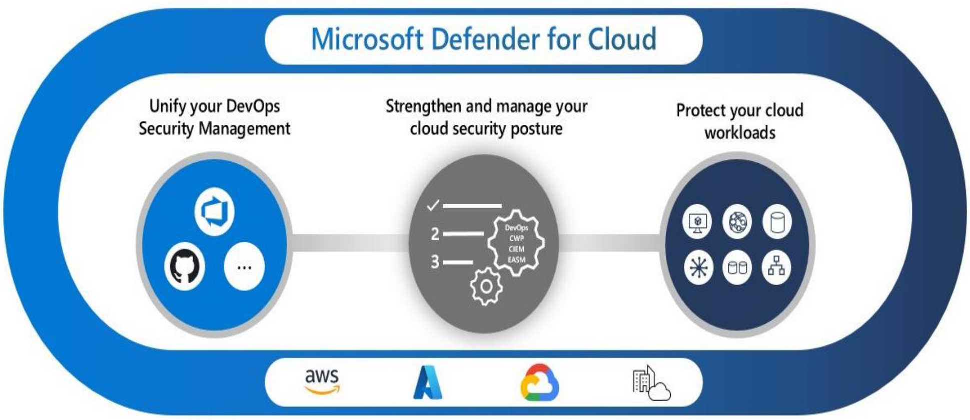


Fig. 1.5 : Data Protection Methods in Cloud (Source: Microsoft).

1.2.3.4 Data Availability, Privacy, and Regulation: Data availability, privacy and Regulation are essential terms in cloud computing. Using these terms, we determine how the data is stored, managed and accessed, deleted and shared in the cloud environment, as shown in Fig. 1.4 [4].

1.3 VARIOUS SOLUTIONS FOR DATA PROTECTION CLOUD ENVIRONMENT

Data protection is the primary objective of cloud service providers. In cloud infrastructure, we can use different types of data protection solutions. Fig. 1.5 shows various categories of protection solutions. Controls, processes, and rules for implementing each data protection solution choice must be defined.

1.3.1 Data Encryption

Data encryption is a technique to convert into code so that the unauthorised users cannot use it. The primary objective of data encryption is to ensure that the user should not access the data without a decryption key. In the cloud environment, the data move from one location to another. Thus there is a need for any technique which ensures that if an unauthorized person hacks the data, he cannot decrypt it. SSL and HTTPS are the most popular security protocols used to encrypt data during movement [5].

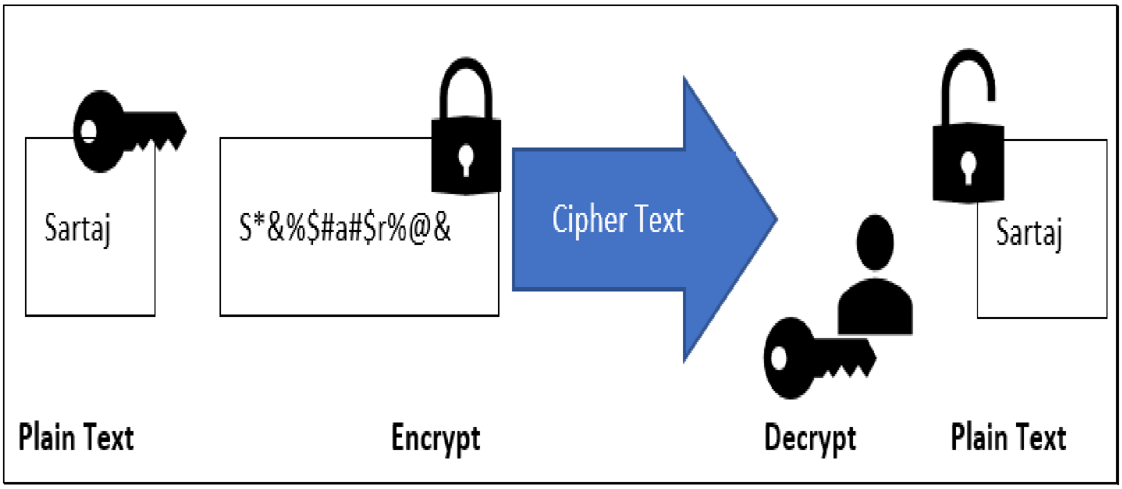


Fig. 1.6 : Cryptography Process.

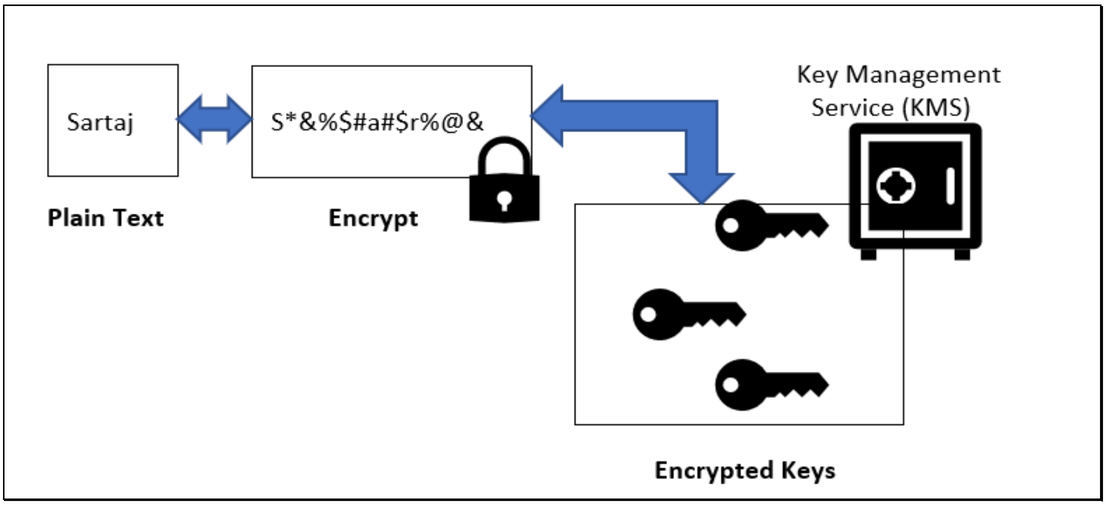


Fig. 1.7 : Key Management Service.

1.3.2 Management of Keys

Keys in data encryption fields are like a secret codes. The keys are used to encrypt or decrypt the data in cloud environment. The keys ensures that the data should be accessed by the authorized persons. In cloud environment we are having different types of resources and they are protected using various types of keys. These keys stored in cloud infrastructure. It is a challenging issue that how to memorize and protect the data encryption keyes. Thus, there is a need of a key manage technique that can protect, recover and secure the key of our cloud data. For key management we are having different types of techniques as given below:

1. We can secure the key by storing them in data centers. The datacenters ensures that the keys are protected from unauthorized access.

2. We can secure are keys by storing it in another trustworthy cloud service provider. With this approach we shall keep seprated our data and keys.

3. Another approach for key management is to store our data encryption keys withing same cloud environment. For key management different security services can be activated to protect it from unauthorized access.

For key managemt purposes, the cloud service providers make the use of different types of tecniques. For example, AWS employs AWS Cloud HSM and AWS KMS to oversee customer keys. In contrast, IBM relies on unique techniques to key management, including IBM cloud key protection, IBM Multicloud data encryption, IBM Cloud hyper protect services, and IBM cloud hardware security module.

The role of key management is to uphold the integrity of key storage and sharing. When data voyages from one location to another, it does so under the watchful gaze of key management. Only those granted permission who are authorized to access the data. Different type of encryptions are supported by key management techniques like file, object, block, and database encryption. For more security the key management consists the hardware security module (HSM). It can provide various levels of key protection, recovery and distribution of keys as shown in Fig. 1.5.

1.3.3 Control of Data Access

Data access control works like a bridge of trust between various applications. It ensures that the application can trust on other applications for access of data. Data access control techniques support various types of authentication approaches as given below:

- Username and Password
- AD or OpenLDAP

Table 1.2 : Security provided by different Cloud Service Providers.

Amazon Web Services (AWS)	Shared Responsibility Model Identity and Access Management (IAM) Encryption AWS WAF and Shield AWS Inspector and GuardDuty
Microsoft Azure	Azure Security Center Azure Active Directory Azure Firewall Azure DDoS Protection Azure Key Vault

Google Cloud Platform (GCP)	Google Cloud Identity and Access Management (IAM) Google Cloud Security Scanner Google Cloud Security Command Center Google Cloud DDoS Protection
IBM Cloud	IBM Cloud Security Advisor IBM Cloud Identity and Access Management IBM Key Protect IBM Cloud Firewall IBM Guardium

- S3 secret access key
- OpenStack Keystone identity service
- Public key infrastructure (PKI) certificate and private key.

1.3.4 Certification Management

The internal certificate authority produces TLS or SSL certificates by default. However, these certificates are not trusted by end-user hardware nodes or browsers. This situation poses a security concern. Replacing this default certification process with certificates properly signed by an external third-party or an enterprise Certificate Authority (CA) is advisable for more security. For the best security practices, it's strongly recommended that customers adopt guidelines that align with their organization's needs. Typically, this involves utilizing a recognized enterprise Certificate Authority (CA) to issue certificates. This approach ensures that the certificates are reliable and confirmed, bolstering the overall security posture and instilling confidence in the digital interactions of the organization.

1.4 DATA SECURITY SERVICES PROVIDED BY DIFFERENT CLOUD SERVICE PROVIDERS

For data security, cloud service providers offer different data security services [6]. A wide range of cloud service providers like Microsoft Cloud, Amazon AWS, Google

Cloud Platform and Microsoft Azure exist. Most ot these service providers provide identity management, access management, data protection and key management services to cloud users. Before shifting to the cloud, a client and provider must assess the many security methods available to protect the environment. [7]. These providers provide end-to-end data security services to protect data from various security threats [8], as shown in Figure 1.7.

1.5 IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and access management (IAM) is intended to handle the valid authentication and authorisation processes for the users, administrators, and programmers trying to use the cloud's resources [9]. This is the most crucial configurations that cloud architects must address from the beginning. Cloud computing is a multitenancy system, which means that resources are shared among several tenants. In terms of network, physical, and application containerization, there are many levels of segregation. Nonetheless, permission to the correct client necessitates the avoidance of security threats. IAM maintains an access list for tenants and grants access based on the user's job. The list must be clarified during the SME dialogue between the cloud provider and the consumer. For example, if a company's IT administrator.

An application team or a developer, on the other hand, will have additional privileges determined by their jobs in the cloud. Security teams collaborate to efficiently manage the access list. Customers require security assurance at every level once they agree to shift their workload to the cloud.

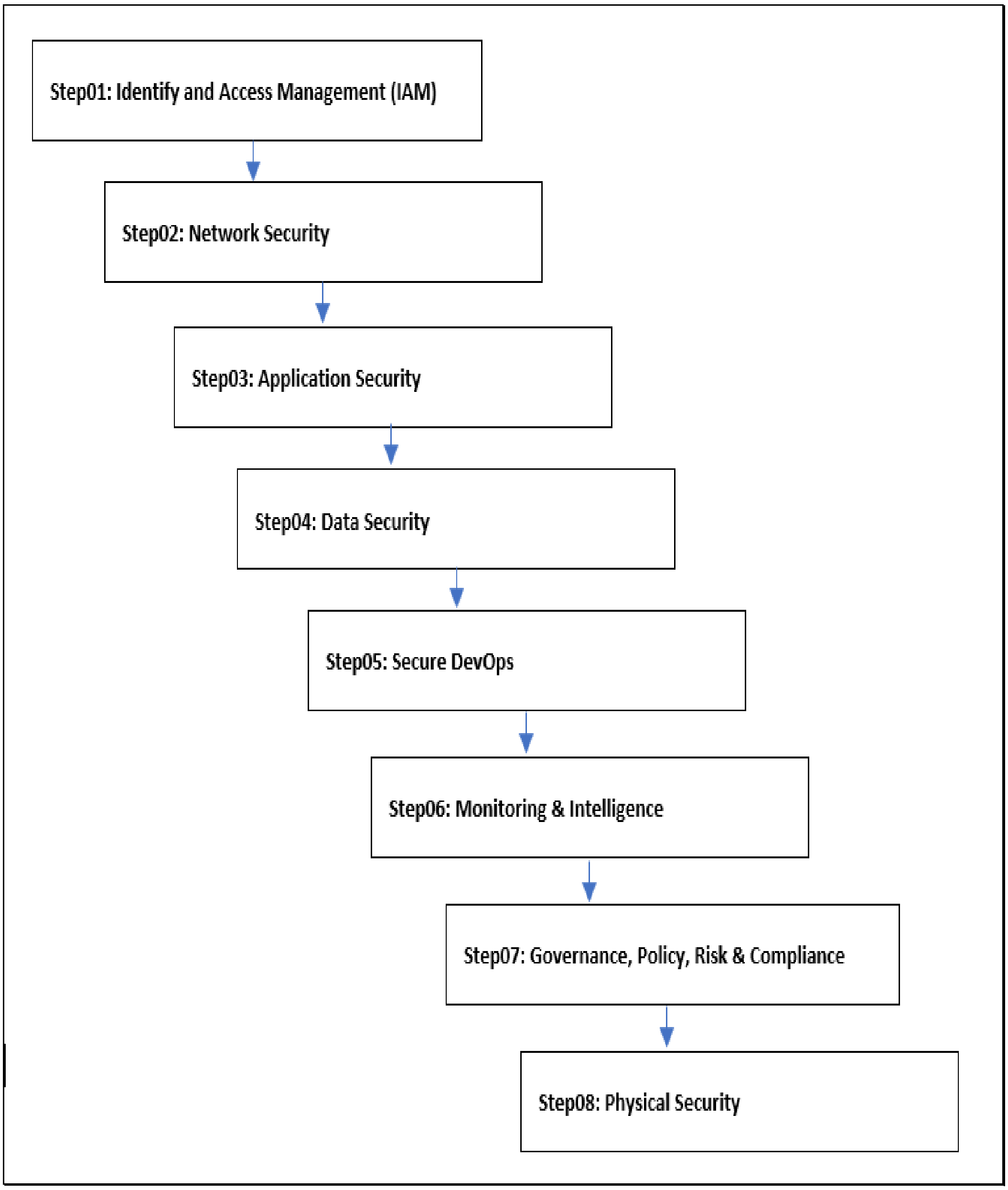


Fig. 1.8 : End to End Security in Cloud.

IAM supports a variety of authentication techniques. It also assists customers by providing Single-Sign-On (SSO) authentication, which allows users to validate numerous applications with the same credentials.

- Multi-level authentication
- Single-Sign-On (SSO)
- authentication and authorization

- Controlling access to the multitenant setting
- Manage the environment's Access Control List.
- Assigns authorization via working with security groups
- User password synchronization
- Account activation and deactivation.
- External user federation services
- User access audit and compliance
- Integration with SaaS-hosted apps
- The administration interface for access control

1.5.1 Network Security

Any environment's key element is the network, which links the inside of the IT structure to the outer world. The safety of networks is the most crucial factor to take into account while moving to the cloud because the environment of the cloud runs through the internet. The implementation of network security by both the cloud service provider and the client [10]. It blocks unauthorized traffic and stops security risks in their tracks. Technical measures are required for secure networks. Deep packet analysis, traffic throttling, and packet black-holing are all effective strategies. These strategies will aid us in detecting and responding to complex network-based threats. It is also capable of mitigating Distributed Denial-of-Service (DDoS) attacks. Encryption, firewall, routing, NAT, and VPN services are available in the cloud, as are deep packet inspection, Site filtering, traffic shaping, antimalware and antivirus protection, SSL inspection, incursion prevention, data loss mitigation, and sandboxing. A network's design detects situations of significant risk and data transfers that could affect statutory, legal, and compliance with regulations.

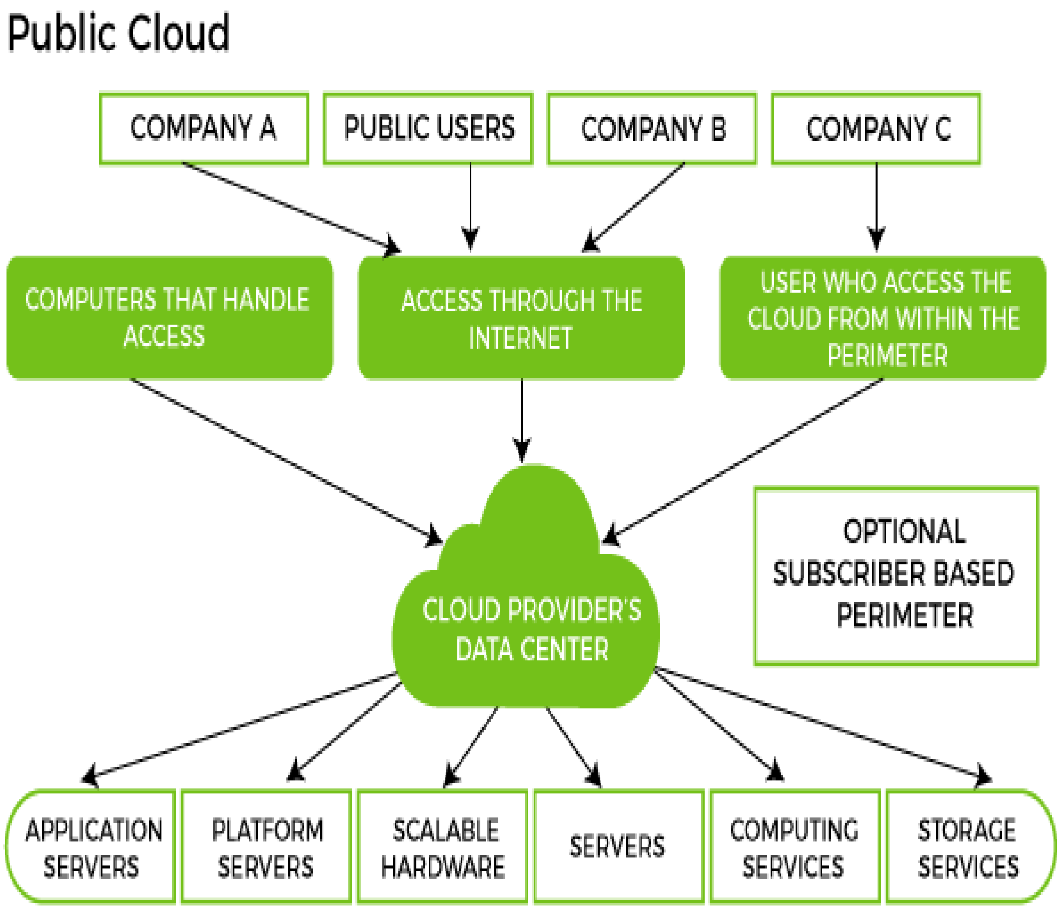


Fig. 1.9 : Network Design of Datacentre (Source Java T Point).

1.5.2 Application Security

PaaS (Platform as a Service) provides access to security protection apps. In contrast, while shifting workloads to the cloud, application dangers and assaults must be taken into account. An application developer must additionally ensure and pay attention to user input variables. It must be validated that application authorisation is a secure process. The security risks posed by unsafe coding must be understood by the application team and cloud providers which can lead to various sorts of attacks.

1.5.3 Data Security

One of the most crucial things to take into account while handling new requirements or shifting workload from an old system is data security. Due to the fact that infrastructure is shared by numerous tenants, customers are frequently concerned about data security. The cloud provides numerous advantages in terms of cost and deployment, as well as advantages in running the application on the cloud. The majority of individuals use cloud services, whether as SaaS, PaaS, or IaaS. Despite these benefits, there are numerous worries about data security. Customers are concerned about their personal and confidential information being uploaded to the cloud. They are constantly concerned about the storage and accessibility of their data. Companies and cloud providers take the appropriate steps to manage security risks in a variety of ways. Cloud providers and clients must pay attention to both data at rest and data in transit. When data is in transmission mode and kept in the cloud, several types of authentication, such as encryption and vital management procedures, are employed to protect it. Section 4 of this chapter goes into great length about data security. [11]

1.5.4 Secure DevOps

DevOps is an acronym that stands for development and operations, and it combines the two on a single platform. Its agility, accessibility, and security increase its significance. It serves as a location for the development, testing, and acquisition of apps. DevOps security [12] is another top consideration due to the fact that once an application is developed, any flaws can hurt the production environment. Software Development Lifecycle (SDLC) guidelines are followed by Secure DevOps. All SDLC procedures must be safe and secure due to adequate management and code testing. Previously, developers would create the codes and send them to the security team for assessment. However, in the context of DevOps, development teams regularly release code and distribute it to security teams. The security staff checks every hour, as opposed to six months or a year ago.

1.5.5 Monitoring & Intelligence

The maxim prevention is better than cure is a common one. The same holds true for cloud computing and IT infrastructure.

Table 1.3 : Compliance Regulations.

Certifications for conformity	ISO 27001/27017/27018/22301/31000/900, SOC1, SOC2, SOC3, PCI, HIT RUST, FedRAMP, IRAP, and IBM accreditation for ISO management systems, SSAE16, ISAE 3402
Worldwide legislation	FERPA, HIPAA, ITAR, FU model clauses, and a compliance control list for cloud computing (C5-Germany), FIPS 140-2, DOD CSM Level1-5, My no. act (Japan).
Alignment & frameworks	CJIS, CSA, FFIEC, FISC, FIRMA, MPAA, FERPA, EU-US privacy shield, and FISC

Our infrastructure requires ongoing monitoring and predictive analysis. It is vital to monitor any environment 24 hours a day, seven days a week in order to avert any undiscovered risk or hazard. Monitoring [13, 14] and intelligence are two principles that enable achieving 99.99% SLA easier. It exposes the cloud environment, including applications, data, and networks. Monitoring methods thoroughly examine the total environment and provide alerts and events when errors and unexpected events are detected. The monitoring system analyzes records and prior scenarios using intelligent devices and tools such as vRealize Operations. It warns of potential risks and threats ahead of time. Monitoring tools for firewalls and other security devices can be implemented. It will automatically patch any flaws that are found or alert the specialized team. The notifications from the monitoring tool may be anticipated or unexpected. Screening unauthorized logins and operations is made possible via alerts and logs. Monitoring tools can also be used to analyze traffic and trends. It is also best practice to use when making changes or carrying out any operation in the environment, utilizing the ITIL approach the correct problem ticketing record. Intimate users who have broken the rules should be tracked down using an intelligence tracking program that detects unlawful or non-ticketing movements. It assists in avoiding environmental security risks and illegal user access.

1.5.6 Policy, Governance, Risk, and Compliance

Strong security standards, policies, and governance should be implemented by cloud providers and users in order to decrease risk and achieve compatibility [15]. It makes sure the company abides by industry regulations and regularly evaluates dangers using security controls. Just following the rules can pose serious security hazards.

- Theft of product designs and trade secrets
- Sensitive data exposed in the big data and cloud environments
- Loss of data related to accountable clients, partners, or suppliers
- Insider risks that go undetected
- There are the following standards, which must be managed and adhered to.

1.5.7 Physical Security

Physical security is an important consideration when building or migrating workloads to the cloud. Cloud providers and consumers must maintain physical data center equipment security. Proper physical entrance auditing, access control for approved individuals only, security for hardware devices, data center temperature, and hardware failures are all examples of physical security. It guards against the intentional and unintentional destruction of physical assets, locations, restoration sites, backup tape libraries, tape vaults, and data centers. It also includes physical assets and regions such as networks, data centers, and an individual's protection. With regard to the threats described below [16], physical security is necessary.

- Failure of physical equipment
- Flood and Water; Fire and Smoke
- Storms, Rain, Explosion, Wind, Snow, Lightning, Landslide, Earthquake
- Issues with power, heating, air conditioning, water, or cooling
- Unknown Disasters
- Individual Problems
- Internet Loss as a result of Oceans Cable Loss

Cloud providers and consumers must have data center availability in other areas as part of best practice, and cloud resources and tenants must be located in other locations. It is also preferred that internet connectivity come from many suppliers and be in load balancing mode in order to properly monitor the physical data center. To avoid physical threats, there should always be a Business Continuity Plan (BCP).

1.6 MOTIVATION

The rapid advancement and widespread adoption of cloud computing technologies have revolutionized how data is stored, processed, and shared. While cloud computing provides many benefits in terms of scalability, cost-efficiency, and flexibility, it also introduces significant data security and privacy challenges. As more organizations and individuals entrust their sensitive data to cloud service providers, it becomes paramount to ensure robust encryption and stringent security measures. My research motivation in this field stems from the desire to contribute to developing and improving data encryption and security techniques in the cloud environment. Our research driven by the opportunity to address the existing vulnerabilities and limitations in current encryption methods and to propose novel solutions that can enhance the confidentiality, integrity, and availability of data stored and processed in the cloud.

Through in-depth research, I aim to gain a comprehensive understanding of various encryption algorithms, protocols, and mechanisms deployed in cloud environments. By analysing their strengths, weaknesses, and potential threats, I seek to identify areas where advancements can be made. This includes exploring new cryptographic techniques, such as homomorphic encryption or secure multiparty computation, that allow for secure data processing and analysis without compromising privacy. Understanding the potential vulnerabilities posed by quantum computers and developing post-quantum encryption methods will be crucial to ensuring long-term data protection in an evolving technological landscape.

1.7 PROBLEM FORMULATION

With the advancements made in data storage and communication systems, the necessity to secure data on the cloud. The behaviour of chaotic systems and their applications in numerous sectors, such as data encryption, have drawn more attention recently. Chaotic maps use a special chaotic function that exhibits high levels of chaotic activity and uniform bifurcation over a large range of parameters to create a random sequence that is used to encrypt the input data. Chaotic maps often have parameters that affect their data encryption quality. Manual selection of chaotic maps parameters is a time-consuming task. Thus, there is a need for soft computing based approaches to identify optimal parameters of chaotic maps.

The Internet of Things (IoT) and cloud computing paradigm have gained broad traction as a result of recent advancements in wireless communication and mobile technology. By combining IoT and cloud technology, healthcare applications may be monitored in real-time from any location at any time. Using wireless channels and devices like mobile phones, PDAs, etc., the medical professional can obtain this data instantly. Hence, user authentication becomes a crucial issue and must be addressed for the successful execution of cloud-IoT paradigms. Thus, there is a need for a robust and lightweight remote user authentication solution. Password-based single-factor authentication schemes are more vulnerable than those that include a smart card as a second element, increasing the security of the scheme. Due to the limited processing power, battery life, memory, etc. of the nodes in IoT networks, multi-factor authentication systems offer a lightweight security solution. The mutual authentication of persons communicating must be ensured by the authentication mechanism. The suggested method prevents potential network attacks and creates a shared secret key for each session.

1.8 OBJECTIVES

This research work was to focus on the following objectives:

1. To study various threats in data security in cloud computing.
2. To Propose an Integrated coded cryptosystem for cipher security.
3. To propose a new framework for data security in cloud.
4. To evaluate the performance of proposed approaches based on encryption time, decryption time, memory utilization.

1.9 THESIS ORGANIZATION

The various thesis chapters are structured as follows:

Chapter 1 introduces various Encryption and decryption techniques, the causes and significance of data storage on the cloud, Machine learning techniques, encryption parameters, and different safety measurements for securing the data. It primarily describes the research gaps and objectives of the research. This chapter additionally introduces the significant contribution of this research to society. The methodology adopted for carrying out research is mentioned further in this chapter.

Chapter 2 presents a literature review of existing data security approaches for the cloud. This chapter discusses the research gaps identified from the existing data security approaches.

Chapter 3 proposed big bang big crunch algorithm based approach for Encryption and decryption with 2D chaotic map approach used to secure the data on local and cloud-based databases.

Chapter 4 proposed a multi-factor based approach to secure data in the cloud environment. The proposed approach is compared with 7 approaches available in the literature.

Chapter 5 presents a Light weighted two-factors-based approach to secure data in the cloud environment. From performance analysis, we observed that the proposed approach outperformed its competitors.

Chapter 6 concludes the research work and presents future work.

Chapter – 2

LITERATURE SURVEY

Our world has transformed as a result of the development of smart homes, smart cities, and intelligent things. The Internet of Things environment's smart connected gadgets generate a large volume of volumetric data. With the enormous growth in data and the need to access it from different devices, users are shifting their data to the Cloud. The domain of cloud computing has shown enormous promise, impact, and growth. Without spending money on new equipment, hiring new staff, or licencing new software, cloud computing has improved its capabilities. However, data privacy and security remain crucial concerns in the cloud environment. Since public cloud providers are unreliable, data stored there would be vulnerable to both internal and external threats. This literature survey is divided into two parts i.e., data encryption approaches and data security in the cloud environment. This chapter reviews the possible attacks on the data and solutions to those issues proposed in the literature.

2.1 INTRODUCTION

A notable increase in internet users has been observed in recent years due to the rapid expansion of wireless and mobile communication. Our world has transformed as a result of the development of smart homes, smart cities, and intelligent things. The Internet of Things environment's smart connected gadgets generate a large volume of volumetric data. The exponential rise in data is the prime driver for the Cloud paradigm. National Institution of Standards and Technology defined cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [17]. Garner at. el [18] cloud computing is “a style of computing where massively scalable IT-enabled capabilities are delivered ‘as a service to external customers using Internet technologies.” The significant features of the cloud, such as the minimum cost involved, highly elastic, ubiquitous access to services, scalability, and cheap data storage, have shifted the mass towards the cloud. Figure 1 shows the advantages offered by the cloud. Public, private, and hybrid clouds are among the three types of deployment models available [19]. The list of cloud service providers for various cloud service models is shown in Figure 2.

Cloud computing facilitates services to users at a low cost. It offers users virtual computing services such as processing, software, hardware, and storage efficiently. The data generated from smart devices is stored in the cloud. Users can retrieve their data at any time, anywhere across the globe. Shifting their data to the cloud offers advantages such as a) permanent storage of their data; b) fast retrieval at any time and place; c) no need for actual purchasing of resources; d) minimal maintenance required for resources. This platform is not only suitable for organizations but also for individual users. They can easily access their data using smartphones, laptops, etc., sitting at any remote location.

Figure 2.1: Features of Cloud Computing

The immense popularity of the cloud has created a profound marketplace for cloud providers. Cloud providers must consider the security aspect as vital importance. The biggest threat to this paradigm is data security [20]. Data security has emerged as a significant hindrance prohibiting users from shifting to the cloud as a third party store and manages the data. Cloud providers must ensure the security of servers. There must not be a leak of any users' confidential data stored on the servers. With the increasing computational power, attackers have become more computationally efficient and try different attacks to break down the servers to gain access to the stored data. This chapter outlines possible key threats in the cloud environment and potential security solutions to these threats.

SaaS	Google Apps, Cloud9 Analytics, IBM, Antenna Software, Solutions, Exoprise Systems, Host Analytics, Knowledge Tree, Reval, Taleo, NetSuite, Microsoft 365
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock, CSC, GoGrid, IBM, OpenStack, Rackspace, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SAP, SalesForce, Intuit, Netsuite, IBM, WorkXpress, and Joyent

Figure 2.2 : Cloud Service Providers

Section 2.2 of this chapter discusses possible data security threats in the cloud environment. Section 2.3 presents different available data encryption and security approaches on the cloud.

Section 2.4 discusses the research gap, and last

Section 2.5 concludes the chapter.

2.2 POSSIBLE THREATS IN THE CLOUD ENVIRONMENT

This section discusses the possible threats in a cloud environment. The threats in a cloud environment can broadly be categorized as threats to Data, networks, and Cloud Environment.

a. Threats on Network

- ***DOS Attack*:** Denial of Service is one of the most widespread security attacks in which the attacker repudiates the access of resources to authorized users. The attacker makes the resource unavailable by flooding the network. He disrupts the services by flooding the web with unwanted packets, which consume most of the cloud resources, such as computation power, the bandwidth of the network, and memory. Thus, users are unable to access the services [21].

- ***Insider Attack*****:** The privileged user may try to access the data of some other users deliberately. The users' confidential data is one of the vulnerable resources, and it comes to high risk when some privileged insider gets access to it. The frequency of such attacks is high and is one of the most common.

- ***Impersonation Attack*****:** The attacker impersonates an authentic entity to access services. He may try to transmit recorded messages, such as the user's identity to gain access to the secret data successfully. If the cloud has a robust authentication mechanism, these impersonated messages will not be authorized to access services.

- ***Password Guessing Attack*****:** The attacker initially listens to the ongoing communication of the authentic entity and server, which mutually authenticate each other. He then uses information from the eavesdropped messages and guesses probable passwords. This attack can be attacked in two ways, online and offline. The attacker may try to guess in real-time or later in offline mode. This is like an exhaustive search where he executes all password possibilities [22].

- ***Replay Attack*****:** The attacker captures the messages communicated between legitimate entities in a session and replays them later. The attacker secretly listens to the news. He then resends the notes to gain access to resources. To avert this attack, the authentication mechanism must employ nonce and timestamps. Suppose an attacker tries to start an afresh session using recorded messages. In that case, it will be terminated as the permitted timestamp delay will be high.

- ***Service/ Account Hijack:*** Cloud services are accessible through the Internet. This also brings risk to the account of the users. Users may lose control of their accounts, thus, losing their confidential data. Public networks bring several threats to the user account on cloud.

b. Threats about the Data

- ***Data Breach*** **:** The attackers may resort to numerous ways to breach the system's security and get access to the data. The attackers find every loophole to gain access to the data, such as poor authentication mechanisms, flaws in application design and infrastructure, and lack of audit control [23, 24]. This dramatically affects companies such as Google, Yahoo, and Microsoft.

- ***Data Loss*****:** Data loss is one of the main issues with the cloud. The personal data of users is stored in the cloud. Several threats, such as data deletion, failure of keys used for data encryption [25], data corruption, natural disasters, network attacks, etc., lead to data loss. Users move their data to the cloud to store, manage, and access it as and when needed in the future. However, the loss of this data has a devastating effect [26].

c. Threats pertaining to Cloud Environment

- ***Transition in the Business Model*** **:** Cloud brings transfer of control of data to the third party. Additionally, there is a profound change in the business model compared to the traditional one. This model also brings significant new risks, and attackers try every possible way to intrude into the system.

- ***Abusive Use*****:** Cloud users may misuse cloud services. As the user's confidential data is stored on the cloud, intruders resort to different ways to access data illegally or unethically. They may violate their agreement or perform attacks to get access.

- ***API and Browser Vulnerabilities*** **:** Threat to the API of cloud provider or interface is one of the crucial risks in cloud environment. The intruders may perform browser-based attacks to breach the security.

- ***Shared Resources Vulnerabilities*** **:** Cloud platform brings sharing of resources which is one of the advantages as it reduces costs. This increase in the leverage of resources creates a single point of attack. For instance, sharing of technology is a hypervisor or cloud orchestration.

2.3 DATA SECURITY AND ENCRYPTION TECHNIQUES IN CLOUD

This section presents different existing data encryption and data security approaches in cloud. Section 2.3.1 discusses the recent data encryption approaches. Section 2.3.2 of this chapter presents various existing techniques for data security in cloud.

2.3.1 Data Encryption Techniques

To protect the security and privacy of data, many algorithms and techniques are used in data encryption systems. However, with the increasing volume of data, encrypting large and diverse datasets, including structured and unstructured data, poses a challenge. A dynamic data encryption strategy (D2ES) has been proposed to address this, which selectively encrypts data based on privacy classification methods and timing constraints. Another method that permits users to browse over encrypted material while maintaining privacy is searchable encryption (SE). Attribute-based encryption (ABE) also provides access control mechanisms for encrypted data in cloud storage. These encryption approaches aim to enhance privacy protection and ensure the secure handling of data in various application scenarios. Literature is rich with various data encryption techniques. Some most popular techniques and widely used data encryption techniques as below:

Famous asymmetric or public key cryptosystems include RSA. One of the most secure encryption methods now in use is RSA. The data is encrypted in a single round. A block cypher encrypts and decrypts data using two unique keys [27]. The factoring problem, which is crucial to the security of RSA, refers to the practical challenge of factoring the product of two prime numbers. Anyone with a decent understanding of prime numbers may decrypt the data. The following is how the RSA algorithm generates public and private keys.

Let the a and b are the two prime numbers; it computess n as the product of a and b and ψ (t) = (a – 1) (b – 1). Further, the approach selects e as 1 < e < ψ(t)), where e and t are co-prime numbers. Once e is choosen, the appraoch computes a value for d as (d $\Uparrow$ e) %ψ (n) = 1. The final private key is (d, t), and the public key is (e, t). Encryption and decryption are done using below given equations : equations 1 and 2, respectively.

$$C = M^{e} \ (mod \ t) \qquad (2.1)$$

$$M = C^{d} \ (mod \ t) \qquad (2.2)$$

RC6 and RC5 are both block ciphers used for symmetric key encryption. RC6 is an advanced version of RC5, incorporating multiplication, addition, subtraction, XOR, and rotations. It uses parameterized settings for the word size (w), number of rounds (r), and key size (b) to accomplish encryption in 20 rounds. In blocks of 32, 64, or 128 bits, data can be encrypted using RC5, with 64 bits being the optimal size. The suggested value for the key length is 128 bits, however it can be any number between 0 and 2040 bits. Due to its straightforward processes, RC5 can be implemented in both software and hardware.

RC4 is a symmetric stream cipher used in wireless routers. It encrypts characters one at a time and has variable key lengths ranging from 40 to 2048 bits. To achieve stronger encryption, 16-byte keys are commonly used. RC4 relies on keystream bytes, independent of the plaintext, for encryption.

IDEA is a block cipher algorithm using 64-bit data blocks and a 128-bit key. It divides the data block into four 16-bit sub-blocks and undergoes eight rounds of operations and an output transformation phase. Each round requires six unique keys generated from the original 128-bit key.

Triple-DES is an encryption algorithm that applies DES three times to each data block for enhanced security.It is considered more secure than DES but is slower in comparison.

Each of these encryption algorithms has its strengths and weaknesses, making them suitable for different scenarios depending on the required level of security and performance.

The big data approach by Priya Matta et al. has covered a number of encryption methods for data security, including DES, RSA, and AES., focusing on their application areas and issues. D2ES, which was developed by Dr. B. Sunil Kumar and colleagues, selectively encrypts data within the allotted execution time. [29]. Searchable encryption approaches: attacks and challenges by D. V. N. Siva Kumar et al. have discussed various encryption approaches used in searchable encryption schemes, including Order Preserving Encryption (OPE) and Paillier encryption [30]. Miguel Morales-Sandoval et al. suggest using attributes to encrypt data before it is stored, shared, and retrieved in the cloud. [31]. A unique data encryption technique known as Dynamic Data Encryption Strategy (D2ES) has been published in Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing by Keke Gai et al. D2ES uses privacy classification algorithms to only encrypt certain data [32]. Chen Weijie et al. created an encryption method based on data de-redundancy technology that uses a bloom filter and an elliptic curve encryption algorithm. They also discussed security vulnerabilities and encryption technology of computer information technology data under big data environments. [33].

In their study, An Approach for Efficient and Secure Data Encryption technique for Spatial Data, N. Chandra Sekhar Reddy and colleagues proposed a dual spatial data transformation and encryption technique for efficient and secure data encryption [34]. The Advanced Encryption Standard (AES) and RSA algorithm are combined in Pooja Verma et al.'s proposal, Multi Encryption Approach for Privacy Preserving Authentication over VANETs, to provide secure data communication in VANETs [35]. Shadi Aljawarneh at. el. has presented a resource-efficient encryption system that uses multithreaded programming and a multi-level encryption paradigm for massive multimedia data [36]. M. Sri Lakshmi et al. discussed a hybrid system employing digital watermarking and ARC6 encryption for data encryption [37].

Shahnawaz Ahmad et. Al proposed a Time-Oriented Latency-Based encryption approach to Secure the cloud. This method is utilized to deliver services with a higher performance quality. This strategy focuses on choosing the best encryption techniques at various timing stamps in accordance with the latency guess. Various encryption techniques have been used to accomplish this, and each one's quality of service support values (QoSV), depending on delay, are measured. Based on the QoSV values, an efficient strategy for the current duty cycle has been discussed and applied to cloud service data. The proposed solution minimises latency while improving the performance of several quality-of-service aspects.

Table 2.1: Data Encryption Techniques

Sr.No.	Approach	Reference	Findings
1	Big data perspective	[28]	Discussed the existing approaches for data encryption to secure data, focusing on their application areas and issues.
2	Execution of data encryption strategy in mobile cloud computing	[29]	Dynamic Data Encryption Strategy (D2ES), a revolutionary data encryption technique that selectively encrypts data within the allotted execution time, was proposed.
3	Searchable encryption methods: threats and difficulties	[30]	Order Preserving Encryption (OPE), Paillier encryption, and other encryption techniques utilised in searchable encryption schemes were discussed.
4	Cloud-Based Storage, Sharing, and Retrieval of Encrypted Data Using Attribute-Based Encryption	[31]	outlined a proposed attribute-based encryption method for cloud storage, distribution, and retrieval of encrypted data.
5	Big Data Privacy-Preserving Data Encryption Strategy in Mobile Cloud Computing	[32]	Dynamic Data Encryption Strategy (D2ES) is a unique data encryption methodology that selectively encrypts data based on privacy classification algorithms.
6	Under a large data environment, computer information technology data security vulnerabilities and encryption technologies are present.	[33]	proposed a data de-redundancy-based encryption method that uses the elliptic curve encryption algorithm and bloom filters.

Sr.No.	Approach	Reference	Findings
7	A Method for Secure and Efficient Data Encryption for Spatial Data	[34]	proposed a dual data encryption and transformation technique for spatial data that is both effective and secure.
8	Multi Encryption Approach for Privacy Preserving Authentication over VANETs	[35]	Proposed a multi-encryption approach using the Advanced Encryption Standard (AES) and RSA algorithm for secure data communication in VANETs
9	An method to multithreaded programming for huge data in multimedia	[36]	proposed a multi-level encryption concept and multi-threaded programming as a resource-efficient encryption system for large amounts of multimedia data.
10	A Hybrid Method for Protecting Digital Data Using Watermark Encryption	[37]	ARC6 encryption and the digital watermarking technique were suggested as a hybrid solution to data encryption.
11	The paper discusses various encryption techniques such as DES, RSA, and AES for securing data, with a focus on their application areas and issues.	[38]	1. Comparative evaluation of cryptographic and decryption methods 2. Determining the contexts in which encryption methods can be applied
12.	The paper proposes a novel data encryption approach called Dynamic Data Encryption Strategy (D2ES) that selectively encrypts data within required execution time requirements	[39].	1. Proposed approach is called Dynamic Data Encryption Strategy (D2ES) 2. D2ES maximizes privacy protection within execution time requirements.

Sr.No.	Approach	Reference	Findings
13.	The Order Preserving Encryption (OPE) and Paillier encryption techniques are just two of the encryption methods covered in this work.	[40]	1. Review of existing SE approaches concerning precision and security 2. Information disclosure attacks and remedies for each approach
14.	The article proposes an attribute-based encryption technique for storing, sharing, and retrieving encrypted data on the cloud.	[41]	1. Proposed a secure scheme based on attribute-based encryption 2. Provided Type-III constructions for CP-ABSE and DET-ABE
15.	The research suggests a unique method for data encryption dubbed Dynamic Data Encryption Strategy (D2ES), which selectively encrypts data using privacy categorization techniques.	[42]	1. Proposed approach, D2ES, maximizes efficiency of privacy protections. 2. Experimental evaluations showed adaptive and superior performance.
16.	The research suggests a data de-redundancy-based encryption method that makes use of a bloom filter and an elliptic curve encryption algorithm.	[43]	1. Proposed de-redundancy method for big data encryption 2. Increased encryption speed and improved security
17.	For effective and safe data encryption for spatial data, the study suggests a dual transformation and encryption approach.	[44]	1. Dynamic grid structure is more efficient than progressive confidentiality technique. 2. Existing methods have restrictions and high overhead communication.

Sr.No.	Approach	Reference	Findings
18.	The paper proposes a multi-encryption approach using the Advanced Encryption Standard (AES) and RSA algorithm for secure data communication in VANETs	[45]	1. Proposed multi-encryption approach for secure communication 2. Implemented AES and RSA algorithms and estimated performances
19.	The paper proposes a resource-efficient encryption system using multithreaded programming and a multi-level encryption model for big multimedia data.	[46]	1. Proposed system has the least run time and higher throughput 2. System improves computation run time by approximately 75%
20	The paper proposes a hybrid approach using ARC6 encryption and a digital watermarking technique for data encryption.	[47]	1. Proposed method suitable for copyright protection of digital images. 2. ARC6 encryption algorithm and RDM watermarking method used.
21.	Time Stamp technique based technique to secure data on cloud	[48]	The suggested strategy has lowered the latency factor while enhancing the performance of various QoS parameters.

2.3.2 Data Security Approaches in Cloud

Researchers have proposed several remote user authentication schemes to secure data stored on the cloud. Das et al. [49] presented an authentication technique for remote users in public networks that uses smart cards. The scheme provides users with the freedom to freely select and update their passwords. This is crucial in ensuring security. As businesses continue to grow on a global scale, the significance of IT infrastructure becomes even more pronounced. Digitalization has become an integral aspect of every business model, impacting all aspects, both small and large. These advancements have expanded the reach of IT infrastructure, transcending boundaries.

With each passing day, the industry presents fresh demands, placing immense pressure on IT infrastructure to drive and propel business objectives forward. The dynamic nature of these requirements calls for constant adaptation and acceleration, making IT infrastructure an indispensable component in achieving business goals. As a result, modern infrastructure must be adaptable, efficient, safe, and scalable. To enable mission-critical applications in the environment, every business model demands an appropriate infrastructure. To host any application, customers must have specific hardware and software in the data centre. Customers that want to expand their businesses abroad must not rely on the limited capabilities of their applications. Because we need to modify the foundation of infrastructure, our typical data centre cannot withstand the pressures of the digital age and the impact of globalisation. A similar situation exists for applications where we cannot reach our business objectives without altering our data centres to meet the needs. It indicates a need for regular infrastructure and application updates in any business.

Several schemes to ensure data security in a cloud environment have been proposed in the literature. It dramatically minimizes the cost by reducing the output length, thus, providing a better compression ratio. It also enhances security. In 2012, Chen & Zhao [50] analyzed data privacy and security concerns in cloud computing. The current solutions adopted to tackle these concerns have also been discussed. In Liu et al. [51], Mona is a dynamic multi-owner data-sharing scheme. Users can share their data with other participants using an untrusted cloud. It employs bilinear maps and ensures efficient joining of new users and user revocation.

Furthermore, it is computationally inefficient. In 2014, Wei et al. [52] established an auditing protocol named *SecCloud*. It permits the storage of user data on the cloud securely. It employs probabilistic sampling and verifier signatures to perform storage and computation auditing. However, it is not computationally efficient as it costs more than the existing schemes. Another scheme in the same context was put forth by Dong et al. [53] in 2015, *SECO*. The technique uses hierarchical identity-based encryption to secure cloud data collaboration services. But this scheme to suffers from several issues. It needs synchronisation and fails to ensure the data is complete. The method has not been implemented on the cloud to ensure its performance.

In the realm of authentication and user verification, a series of research findings and proposals have been put forth by various authors, leading to a complex web of improvements and vulnerabilities.

Wang et al. [54], discussed their initial scheme fell short in ensuring mutual authentication and user verification without relying on passwords. In response, the authors devised an improvised scheme to address these shortcomings. Wen & Li [55] later scrutinized Wang et al.'s [54] scheme and identified critical vulnerabilities related to forgery and information disclosure attacks. As a remedy, they suggested an enhanced version of the scheme, aiming to bolster its security. Chang et al. [56] performed thorough cryptanalysis of Wen & Li's [55] enhanced scheme and unearthed its vulnerability to anonymous identity. Chang et al. [56] proposed an improvised strategy to close the discovered gaps. Chang et al.'s [56] technique was found to be vulnerable to forging and password guessing attacks by Kumari et al. [57]. To fortify the security, they proposed an enhanced version of the scheme. Nikooghadam et al. [58] examined Kumari et al.'s [57] enhanced scheme and identified a deficiency in safeguarding against offline guessing attacks and ensuring user anonymity. To tackle these shortcomings, Nikooghadam et al. [58] suggested further improvements to enhance the security of the scheme. This dynamic interplay of discoveries, enhancements, and challenges showcases the continuous pursuit of improving authentication and security systems as researchers strive to create robust and reliable solutions for user protection.

Song [59] conducted a cryptanalysis of Xu et al.'s [60] scheme and exposed its vulnerability to impersonation attacks. In response, Song [59] presented an improvised scheme, aiming to address and strengthen the security concerns. Chen et al. [61] delved into Song's [59] scheme to review its effectiveness. To their evaluation, Chen et al. [61] uncovered that the improvements suggested by Song [59] were susceptible to major threats, indicating further room for enhancement. One notable weakness of Song's scheme lies in its inability to withstand offline password guessing attacks, leaving it exposed to potential breaches. As a solution, the authors proposed an alternative authentication mechanism to mitigate the identified security flaws. The intricate assessments and countermeasures in this cryptographic landscape demonstrates the iterative process of fortifying security mechanisms. Researchers persist in their pursuit of robust solutions, acknowledging the evolving nature of threats and the ever-pressing need for enhancing cryptographic systems to safeguard against potential vulnerabilities. Lwamo et al. [62] put forth a scheme known as SUAA: secure user authentication scheme with anonymity for both single and multi-server environments. This innovative approach leverages biometric factors for the authentication process, introducing a novel dimension to security measures. However, one critical drawback of this scheme lies in its high computational cost. The complexity of calculations and processing required hinders its efficiency, making it less viable for resource-constrained environments where computing power and resources are limited. Sharma & Kalra [63] proposed remote user authentication schemes for insecure public networks. Table 2.4. shows summary of literature review.

Table 2.2 : Summary of Literature Review

Existing schemes	Cryptanalysis by	Limitations
Das et al.,2004	Wang et al., 2009	- No mutual authentication - Verification of user without the need of password
Wang et al., 2009	Wen & Li,2012	- Forgery attack - Information disclosure attack
Wen & Li, 2012	Chang et al., 2013	- Anonymous identity attack
Chang et al., 2013	Kumari et al., 2014	- Forgery attack - Password guessing attack
Kumari et al., 2014	Nikooghadam et al.,2016	- Offline guessing attack - No user anonymity
Xu et al., 2009	Song 2010	- Impersonation attack - Eavesdropping attack
Song 2010	Chen et al., 2014	- Man-in-middle attack - Offline password guessing attack

In 2016, Yao et al. [64] developed a framework that integrated big data processing and semantic analysis to process and analyse data. It specified stages in semantic security, such as collection, storage, processing, and analysis using the semantic framework. The chapter lacks actual results. The framework has neither been implemented using any tool nor discussed the cost of performing this semantic analysis. In the same year, Aldossary& Allen [65] put forth a survey chapter that explained prominent issues faced in cloud platforms, such as data loss, virtualisation security, the integrity of data, confidentiality, and possible solutions that had been discussed. In 2019, Lin & Liu [66] put forth the idea of using deep learning to process and analyse data. The authors have used this in the context of the industrial internet and discussed several steps for acquiring and representing data.

In the same year, Sun [67] 2019 discussed privacy issues of cloud computing, and searchable encryption techniques, mainly employing models for attributed-based encryption, proxy re-encryption, hierarchical encryption, and a framework for achieving privacy protection. Yadav et al. [68] used Blockchain to achieve a two-factor authentication system for real-time monitoring. The authors claimed it is trustworthy and efficient for storing data in the cloud. It lacks effectiveness In 2021, Tahir et al. [69] presented *CryptoGA*, which employs a Genetic Algorithm (GA) to produce keys for performing encryption and decryption. CryptoGA tackles privacy issues and data integrity. However, the scheme has significant memory overhead.

Software-defined data centers [70, 71] emerged to mitigate these challenges. Virtualization and cloud computing have supplanted the traditional physical data centre, allowing many hardware devices to remain in a data centre. Virtualization technology allows IT infrastructure to be stored on a virtual layer. Virtualization in cloud computing has reduced the investment of business owners. Customers in a Cloud environment only pay for resources as they are needed, which is known as the Pay-As-You-Go approach. Our budget will only use the cash required to fulfil the business objectives. Cloud computing has played an important role in modernising our business and minimising the limits imposed by IT data centres.

Cloud computing simplifies application development and delivery by providing ready-to-use infrastructure, platform, and software services [72]. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) are three cloud computing models. There are two parts to cloud computing. The consumer (Guest) is the first, while the cloud provider (Host) is the second. Fig. 3 above depicts service management responsibility.

Customers can scale the burden from a single application to the full infrastructure and utilise it as needed. There is no reason why servers in a data centre should be idle. Different cloud models, such as private, public, or hybrid, are available. It is determined by the sensitive application and data requirements, as well as the importance that must be relocated to the cloud.

Cloud computing optimises resource utilisation, lowers capital and operating costs, reduces downtime, and boosts IT productivity, agility, efficiency, responsiveness, faster provisioning of any application and servers, and higher business continuity. It also handles catastrophic scenarios, streamlines data centre management, and allows for flexibility and scalability while saving money. Workload mobility, enhanced performance, availability, and operational automation are also key benefits of cloud computing. Cloud computing simplifies, reduces costs, and makes IT easier to manage. It provides clients with a legal environment while permitting the most creative and competitive technology available. According to Forbes [73], global cloud computing services will be worth $411 billion by 2019, growing at a 15% annual pace.

However, there is still a considerable increase in privacy restrictions, security vulnerabilities, and evolving cyber security risks as a result of cloud use. It works because the cloud is about the availability of resources across the internet. Security concerns and vulnerabilities arise in a multitenancy setting. These security concerns limit any customer's ability to migrate on-premises workloads to the cloud. Cloud adoption faces substantial problems in terms of security and privacy [74]. Customers are still concerned about shifting their on-premises datacenters to the internet due to such concerns.

Although cloud providers and customers are investing significant resources in security mitigation, there are still many security issues with cloud adoption, as attackers quickly gain illegal access to data loaded on the cloud, threatening network security and incurring significant costs for any business. In 2014, CSIS estimated [75, 76] that "*cybercrime costs the world's economy almost $600 billion, or about 0.7% of global income is more than a handful of countries, making cybercrime a very lucrative occupation." . According to the most recent report, cybercrime may currently cost about $600 billion, or 0.8% of global GDP. According to the various Gartner, IDC, and CSIS [77] reports represented in Fig.4, the overall budget to minimise security losses increased by 26% in 2017.* Total IT expenditure has risen by 4.6%. To comprehend the most sensitive components of an IT infrastructure, security and privacy, we must first comprehend the architecture and several techniques to avoiding security vulnerabilities in cloud systems [78]. We must extend and implement safeguards to make the cloud more secure. When data is moved to the cloud, security standards become more stringent. Shared-responsibility models, risk management, and security should all be considered when considering cloud adoption.

We concentrated on other security-related concerns and potential security and privacy approaches offered by various service providers in the cloud computing environment. Additionally, the potential hazards at each interface are examined in order to protect customer trust by transforming security. The following section of this chapter discusses the cloud environment's security architecture, ways to consider when shifting workload to the cloud, and maintaining a secure environment by monitoring and controlling risks.

Gupta and Chaudhary presented a comprehensive review that covers various aspects of data security in cloud computing, including encryption, access control, and authentication. However, it does not provide a detailed analysis of the effectiveness of different security measures [79]. Alqahtani et al. discusses data security and privacy in cloud computing, including challenges and solutions. However, it does not provide a systematic analysis of the existing literature [80]. Li and Zhang focuses on data security technology in cloud computing, including encryption, access control, and intrusion detection. However, it does not provide a comprehensive review of the literature [81]. Kumar and Singh (2021) this paper reviews data security challenges in cloud computing, including data breaches and unauthorized access. However, it does not provide a detailed analysis of the effectiveness of different security measures [82]. Li, Li, and Chen (2021) This survey paper discusses data security and privacy protection in cloud computing, including encryption and access control. However, it does not provide a detailed analysis of the effectiveness of different security measures [83]. Alharbi, Alshammari, and Alqahtani (2020) this review discusses data security techniques in cloud computing environments, including encryption and access control. However, it does not provide a comprehensive analysis of the existing literature [84]. Zhang, Wang, and Wu (2020) this review discusses data security and privacy protection in cloud computing environments, including encryption and access control. However, it does not provide a comprehensive analysis of the existing literature [85].

This study by Kumar and Singh (2020) examines data security concerns in cloud computing, such as data leaks and unauthorised access. However, it does not provide a detailed analysis of the effectiveness of different security measures [86]. Alshahrani and Alshehri (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [87]. Singh and Singh (2021) this comprehensive review covers various cryptographic transformations improving cloud computing data security, including encryption, decryption, and key management. [88]. Raza and Khan (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [89]. Li and Zhang (2020) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [90]. Alharbi, Alshammari, and Alqahtani (2020) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [91]. Alghamdi and Alghamdi (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [92].

Zhang and Li (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. The paper also provides a comprehensive analysis of the existing literature [93]. Alharbi, Alshammari, and Alqahtani (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. The paper also provides a comprehensive analysis of the existing literature [94]. Alqahtani and Alqahtani (2021) this comprehensive review covers various cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. The paper also provides a detailed analysis of the effectiveness of different cryptographic transformations [95]. Liu and Chen (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. The paper also provides a comprehensive analysis of the existing literature [96]. Khan and Raza (2021) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. The paper also provides a comprehensive analysis of the existing literature [97]. Alshahrani and Alshehri (2020) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [98]. Alharbi et al. (2020) this review discusses the use of integrated cryptographic transformations for improving cloud computing data security, including encryption, decryption, and key management. However, it does not provide a comprehensive analysis of the existing literature [99].

Table 2.3 : Data Security Approaches in Cloud

Sr.No	Approach	Author	Findings
1.	Analyzed data privacy and security concerns in cloud computing. The current solutions adopted to tackle these concerns have also been discussed	Chen & Zhao 2012 [50]	An analysis of data security issues utilises a unique data structure on the user's end
2.	The paper likely conducted an analysis of data security and focused on the protection of data. It may have evaluated existing security measures, identified vulnerabilities, and proposed recommendations for enhancing data security.	Liu et al 2013 [51]	Anonymous data exchange Computer-processing ineffective
3.	The paper introduced a novel scheme called Mona, which enables multi-owner data sharing in the cloud. It may have presented the design, implementation, and evaluation of the proposed scheme, highlighting the use of bilinear maps and group signature techniques.	Wei et al. 2014 [52]	Secure computation auditing protocol Enhanced cost than existing

Sr.No	Approach	Author	Findings
4.	The paper introduced a system called SecCloud, which likely utilizes probabilistic sampling and the verifier's signature. It may have presented the architecture and mechanisms of SecCloud, focusing on how it improves security in cloud environments.	Dong et al. 2015 [53]	Ensure cloud data access and updating Need of synchronization Privacy issues
5.	The paper introduced SECO, a system that utilizes hierarchical identity-based encryption. It may have discussed the design and implementation of SECO, emphasizing its ability to provide secure data encryption and access control in a hierarchical manner.	Yao et al. 2016 [64]	Ensures security of data No practical implementation of semantic analysis and HCI to meet data security analysis
6.	The paper presented a framework for processing big data, likely leveraging semantic association and inference methods. It may have described the framework's architecture, algorithms, and techniques used to analyze and extract meaningful insights from large datasets.	Allen 2016 [65]	Issues about cloud platforms are discussed Current solutions have flaws in achieving confidentiality of data integrity Lacks availability

Sr.No	Approach	Author	Findings
7.	The paper likely discussed various schemes aimed at achieving data confidentiality, integrity, and availability in cloud environments. It may have reviewed existing approaches, evaluated their effectiveness, and provided recommendations for ensuring data security in the cloud.	Lin & Liu 2019 [66]	Analyze big industrial data Lacks effectiveness
8.	The paper likely developed an algorithm that utilizes deep learning techniques for analyzing industrial data, specifically focusing on big data. It may have described the design and implementation of the algorithm, highlighting the use of deep learning models and their applications in industrial data analysis.	Sun 2019 [67]	Achieved privacy Flaws in privacy protection
9.	The paper introduced an attribute-based encryption framework aimed at enhancing privacy protection. It may have presented the framework's design, algorithms, and mechanisms for controlling access to sensitive data based on user attributes or policies.	Yadav et al. 2020 [68]	Enhanced security Lacks effectiveness

Sr.No	Approach	Author	Findings
10.	The paper proposed the utilization of Blockchain technology to enhance the security of hospital websites. It may have discussed the design and implementation of a Blockchain-based system, highlighting its potential benefits in securing patient data, improving data integrity, and ensuring access control.	Tahir et al. 2021 [69]	To address concerns about data privacy and integrity. Great memory overhead
11.	The paper introduced a novel approach called CryptoGA, which likely utilizes genetic algorithms for cryptographic purposes. It may have presented the design and implementation of CryptoGA, emphasizing how genetic algorithms can enhance cryptographic operations or improve security mechanisms.	Gupta et al. 2021 [79]	Provides a comprehensive review of data security in cloud computing, discussing various techniques and challenges, including encryption, access control, authentication, and privacy. The paper lacks an in-depth analysis of the impact of emerging technologies (e.g., blockchain, AI) on data security in cloud computing and their potential integration for enhanced protection.

Sr.No	Approach	Author	Findings
12.	As indicated by the title, the paper likely presents a comprehensive review on a specific topic within the scope of the authors' expertise. It may involve systematically examining existing research, summarizing key findings, identifying trends or gaps, and providing an overall assessment of the field.	Alqahtani et al. 2021 [80]	In reviewing data privacy and security concerns in cloud computing, the article emphasises the value of encryption, access control, and secure communication protocols for safeguarding sensitive data. The implications of regulatory compliance requirements as well as the unique issues with data security and privacy in multi-tenant cloud settings are not addressed in the article.
13.	This paper is expected to provide a literature review, which involves surveying and summarizing existing literature on a particular topic. It may present a critical evaluation of relevant research, identify key themes or concepts, and offer insights or recommendations for future studies.	Li et al. 2021 [81]	The paper examines data security technology for cloud computing, concentrating on techniques for secure data storage, access management, and encryption as important safeguards for the confidentiality and integrity of data. The report does not include a thorough analysis of encryption methods and their efficiency in preserving data integrity and secrecy in cloud computing.

Sr.No	Approach	Author	Findings
14.	This survey paper discusses data security and privacy protection in cloud computing, including encryption and access control. However, it does not provide a detailed analysis of the effectiveness of different security measures	Kumar et al. 2021 [82]	The paper reviews data security challenges in cloud computing, discussing issues related to data breaches, unauthorized access, data loss, and the importance of encryption and access control mechanisms. The paper does not explore the challenges and potential solutions related to data security in hybrid cloud environments and the integration of on-premises and cloud-based resources.
15.	This paper indicates that it presents an original research study conducted by the authors. The approach likely involves formulating research questions, conducting empirical or theoretical investigations, collecting and analyzing data, and drawing conclusions based on the findings.	Survey, Li et al2021. [83]	The paper presents a survey of data security and privacy protection in cloud computing, discussing encryption, access control, and data anonymization techniques as essential measures for safeguarding data. The paper does not address the specific challenges and techniques for securing data in edge/cloud computing environments and the impact of edge computing on data security and privacy.

Sr.No	Approach	Author	Findings
16.	The paper denotes that it is a survey, indicating that it provides a comprehensive overview of a specific topic. It may involve collecting and summarizing information from various sources, highlighting key aspects, trends, or challenges related to the surveyed topic.	Literature Review, Alharbi et al. 2020 [84]	The paper reviews data security techniques in cloud computing environments, including access control, encryption, authentication, and intrusion detection systems, emphasizing the need for a layered security approach. The paper does not explore the specific challenges and techniques related to data security in multi-cloud environments.
17.	The paper likely conducted a literature review, which involves gathering and analyzing existing research on a specific topic. It may have summarized key studies, identified trends or gaps in the literature, and provided an overview of the current state of knowledge in the field.	Zhang et al. 2020 [85]	The paper reviews data security and privacy protection in cloud computing, discussing encryption, access control, and secure data transmission protocols as important measures to protect data confidentiality and integrity. The paper does not provide a comprehensive analysis of the impact of emerging technologies (e.g., blockchain, IoT) on data security and privacy in cloud computing.

Sr.No	Approach	Author	Findings
18.	This paper is expected to present a literature review, which involves systematically reviewing and summarizing existing literature on a particular topic. It may have analyzed relevant studies, identified common themes or research methodologies, and provided insights or suggestions for future research directions.	Kumar et al. 2020 [86]	The paper provides a review of data security techniques in cloud computing environments, highlighting the importance of encryption, access control, and secure data storage mechanisms. The paper lacks an in-depth discussion on the potential vulnerabilities and attacks in cloud computing environments and their mitigation techniques.
19.	The paper likely conducted a literature review to explore existing research on a specific topic. It may have reviewed and synthesized relevant studies, identified key concepts or theories, and provided a critical analysis of the literature's strengths, weaknesses, and gaps.	Alshahrani et al. 2021 [87]	The study discusses the advantages and difficulties of employing integrated cryptographic transformations to improve data security in cloud computing. The trade-offs between performance and efficiency that come with integrating cryptographic transformations for bettering data security in cloud computing are not examined in this work.

Sr.No	Approach	Author	Findings
20.	This paper likely presents a literature review that surveys existing research on a particular topic. It may have analyzed relevant studies, identified research trends or emerging areas, and provided a comprehensive overview of the current state of knowledge in the field.	Singh et al. 2021 [88]	The paper provides a thorough analysis of integrated cryptographic transformations for improving data security in cloud computing, outlining their benefits, drawbacks, and prospective uses. The specific difficulties and methods for protecting data in edge/cloud computing environments, as well as the incorporation of cryptographic transformations in such settings, are not covered in the paper.
21.	As indicated by the title, this paper likely provides a comprehensive review on a specific topic. It may involve examining and analyzing existing research in a systematic and thorough manner, evaluating key findings, synthesizing information, and offering a comprehensive assessment of the topic.	Raza et al. [89] 2021	The study examines how integrated cryptographic transformations might improve data security in cloud computing and highlights the advantages of these methods in terms of confidentiality, integrity, and privacy protection. The implications of integrated cryptographic transformations for data security in cloud computing, particularly in large-scale and high-throughput settings, are not explored in this article with regard to scalability and performance.

Sr.No	Approach	Author	Findings
22.	This paper is expected to present a literature review that explores and analyzes existing research on a particular topic. It may involve reviewing relevant studies, synthesizing information, identifying research gaps or areas requiring further investigation, and providing recommendations for future research.	Li et al. 2020 [90]	The study examines how integrated cryptographic transformations can improve data security in cloud computing and discusses the benefits, drawbacks, and prospective uses of these methods. The potential weaknesses and assaults linked to integrated cryptographic transformations and associated defence mechanisms in cloud computing settings are not covered in the article.
23.	The paper likely conducted a literature review to summarize and analyze existing research on a specific topic. It may have critically reviewed relevant studies, identified key findings or trends, and presented a synthesis of the literature to provide insights into the topic area.	Alharbi et al. 2020 [91]	The paper examines how integrated cryptographic transformations might improve data security in cloud computing and highlights the advantages of these methods in terms of confidentiality, integrity, and safe data transport. The specific difficulties and methods for secure key distribution and management in the context of integrated cryptographic transformations for data security in cloud computing are not covered in the paper.

Sr.No	Approach	Author	Findings
24.	The paper likely conducted a literature review to examine and analyze existing research on a specific topic. It may have identified key studies, synthesized their findings, and provided a critical assessment of the current state of knowledge in the field.	Alghamdi et al. 2021 [92]	The study covers the use of integrated cryptographic transformations to improve data security in cloud computing and discusses the benefits, drawbacks, and prospective uses of these methods. The impact of legal compliance standards (such as GDPR and HIPAA) on the adoption of integrated cryptographic transformations for data security in cloud computing is not discussed in the article.
25.	This paper is expected to present a literature review that explores and summarizes existing research on a particular topic. It may have reviewed relevant studies, synthesized information, and identified gaps or emerging trends in the literature.	Zhang et al. 2021 [93]	The evaluation of integrated cryptographic transformations for improving data security in cloud computing in this research emphasises the advantages of these methods in terms of confidentiality, integrity, and secure data storage. A comparison of several integrated cryptographic transformation approaches and their applicability for various cloud computing situations and use cases is not included in the article.

Sr.No	Approach	Author	Findings
26.	The paper likely conducted a literature review to analyze and summarize existing research on a specific topic. It may have reviewed relevant studies, synthesized key findings, and provided insights or suggestions for future research directions.	Zhang et 2020al. [94]	The study examines how integrated cryptographic transformations can improve data security in cloud computing and discusses the advantages, difficulties, and prospective uses of these methods. The integration of integrated cryptographic transformations with other security mechanisms (such as access control, intrusion detection) for comprehensive data protection in cloud computing is not covered in depth by the research.
27.	This paper likely presents a literature review that surveys and summarizes existing research on a specific topic. It may have analyzed relevant studies, identified common themes or research methodologies, and provided a comprehensive overview of the current state of knowledge in the field.	lqahtani et al. 2021 [95]	The paper gives a thorough analysis of integrating cryptographic transformations to improve data security in cloud computing, outlining its advantages, drawbacks, and potential future research areas. The potential trade-offs between data security and efficiency when using integrated cryptographic transformations in cloud computing settings are not examined in the article.

Sr.No	Approach	Author	Findings
28.	As indicated by the title, this paper likely provides a comprehensive review on a specific topic. It may have systematically examined and evaluated existing research, synthesized key findings, and provided a comprehensive assessment or analysis of the topic.	Liu et al2021. [96]	The study covers the use of integrated cryptographic transformations to improve data security in cloud computing and discusses the advantages, difficulties, and prospective uses of these methods. The impact of upcoming technologies (such blockchain and AI) on the efficacy and application of integrated cryptographic transformations for data security in cloud computing is not examined in the paper.
29.	This paper is expected to present a literature review that critically evaluates existing research on a particular topic. It may have reviewed relevant studies, identified gaps or limitations in the literature, and provided suggestions for future research.	Khan et al2021. [97]	The paper examines how integrated cryptographic transformations might improve data security in cloud computing and highlights the advantages of these methods in terms of confidentiality, integrity, and safe data transport. The challenges and methods for implementing integrated cryptographic transformations in cloud computing to ensure data integrity and guarantee data provenance are not discussed in the article.

Sr.No	Approach	Author	Findings
30.	The paper likely conducted a literature review to summarize and analyze existing research on a specific topic. It may have critically reviewed relevant studies, identified key findings or trends, and presented a synthesis of the literature to provide insights into the topic area.	Alshahrani et al. 2020 [98]	The study examines how integrated cryptographic transformations can improve data security in cloud computing and discusses the advantages, difficulties, and prospective uses of these methods. The impact of various deployment options (such as public, private, and hybrid clouds) on the efficiency of integrated cryptographic transformations for data security is not examined in the paper.
31.	This paper likely presents a literature review that surveys and analyzes existing research on a specific topic. It may have reviewed relevant studies, synthesized key information, and provided an overview of the current state of knowledge in the field.	Alharbi et al. 2021 [99]	The study offers an overview of integrated cryptographic transformations for improving data security in cloud computing, outlining their benefits, drawbacks, and prospective uses. The possible drawbacks and weaknesses of integrated cryptographic transformations as well as the requirement for ongoing monitoring and updates to guarantee data security in cloud computing are not discussed in the article.

Sr.No	Approach	Author	Findings
32.	Data security is a major concern in cloud computing, and this paper discusses various techniques and challenges related to data security in the cloud.	Nidhi Shah, Digvijay Mahida - 2018 [100].	Techniques and challenges of data security in cloud computing Proposal of a novel data-sharing mechanism
33.	This paper provides an overview of data security issues in cloud computing and highlights common solutions used to secure data in the cloud.	Lynda Kacha, Abdelhafid Zitouni - 2018 [101].	Problems with data security in cloud computing Typical approaches to cloud data security
34.	The paper discusses the security of data in cloud computing and proposes objectives for improving encryption algorithms to ensure data confidentiality.	Bajirao Subhash Shirole, L.K. Vishwamitra - 2020 [102].	Encryption algorithm and key issues for data security Objectives for improving encryption in the cloud environment

Sr.No	Approach	Author	Findings
35.	Presented a dynamic access control model called RA-HASBE to address the data security issue.	Rajanikanth Aluvalu, V. Uma Maheswari, Krishna Keerthi Chennam, S. Shitharth - 2021 [103]	RA-HASBE, a scalable and adaptable dynamic access control method, was proposed.
36.	This research paper focuses on data security in cloud storage, including encryption, integrity verification, access control, and data availability.	Rongzhi Wang - 2017 [104]	1. research of data availability and data detection problems in depth 2. Proposed remedies based on the POR system and the DSBT scheme

2.4 RESEARCH GAP

Literature is rich with various existing data encryption and security approaches in cloud. From the detailed review of all the existing approaches, we have observed the following issues:

1. Existing data encryption approaches are successfully encrypting the data but they are having high computational, space and timing complexities. Existing algorithms are having so many operations in it to encrypt the data.

2. Existing algorithms to secure the data on cloud is based upon single factor only. The single security factors are easy to break. Thus, there is a need of multi factor algorithms to enhance the data security in cloud.

3. Most of the existing algorithm are securing the data at one level. It could be during login or authentication level. So, New algorithms are needed to develop that could provide data security on all phase of cloud namely Registration, login, authentication phases.

4. The existing data security approaches are not complete. Some algorithms are encrypting data but they are not providing the module to secure the data on cloud. Further, many algorithms are providing some security features to secure data on cloud but data encryption module is missing from these frameworks. Thus, there is a need of complete framework that could provide efficient both data encryption and security on cloud data.

2.5 CONCLUSIONS

This chapter presents a detailed review of data encryption and security approach on cloud. We divided this review in two part i.e. data encryption and data security on cloud. From this survey we observe that the literature is having different data encryption approaches but these approaches are having high computational, space and timing complexities. Further in this chapter, we presented recent data security approaches for cloud environment. The existing approaches are having few limitations. Most of the available data security approaches works algorithms upon single factor only. Thus, these approaches could be extended by introducing the multi factor mechanism in it. Another issue with existing approaches is that they are securing the data at one level. It could be during login or authentication level.

Chapter – 3

DATA ENCRYPTION : AN BIG BANG – BIG CRUNCH BASED APPROACH

Data security is the major issue of current digital technology. This issue can be resolved with the help of data encryption. The chaotic maps are the most popular and secure method for data encryption. We can generate good-quality cipher text with the use of chaotic maps. Chaotic maps are preferred in data encryption because they can produce nonlinear, randomness, and sensitivity to initial conditions. These chaotic map features provide a robust private key, which is difficult to predict. Chaotic maps-based techniques are considered efficient approaches to generate complex and unpredictable sequences. Chaotic maps's primary issue is that they are highly sensitive to the initial conditions. This chapter proposes an integrated Big Bang – Big Crunch (BBBC) and chaotic map-based approach for data encryption and decryption. We used the BBBC algorithm to optimize the parameters of chaotic maps and to produce a highly secured and complex private key. This complex primary key can be applied to data to create complex cipher text. We implemented the proposed approach in python and compared it with the genetic Algorithm integrated 2D chaotic map approach. The results showed that the proposed approach outperformed the existing one.

3.1 INTRODUCTION

A chaotic map is a mathematical function that exhibits chaotic behaviour, meaning that minor variations in the system's primary settings can lead to massively different results over time. Chaotic maps have become a valuable tool for scientists and researchers seeking to simulate the behaviour of complex systems. By identifying the patterns of chaos within these systems, scientists can gain a deeper understanding of how they operate and potentially develop new solutions to real-world problems. Chaotic maps are often used to model complex systems in physics, engineering, biology, and other fields. One of the most well-known chaotic maps is the logistic map, which is commonly used to model population growth [105]. The logistic map is a simple mathematical equation that describes how a population of organisms grows over time and how that growth is influenced by factors such as food availability and competition for resources.

Another example of a chaotic map is the Lorenz attractor, which is used to model atmospheric convection and weather patterns. The Lorenz attractor is a set of differential equations that describe how air moves through the atmosphere and how small changes in temperature or pressure can lead to large-scale weather patterns such as hurricanes and tornadoes. Despite their complexity, chaotic maps offer valuable insights into the behaviour of complex systems and have been used to make significant advancements in a various fields. As our understanding of chaos and complexity continues to grow, these mathematical models will likely become even more critical.

A common example of a chaotic map is the logistic map, a simple nonlinear recurrence equation that describes the population growth of a species with limited resources. The logistic map is represented using following equation:

$$\mathbf{pop\_(t+1) = rand * pop1\_t * (1 - pop1\_t)} \qquad \mathbf{(3.1)}$$

Where pop_t is the population size at time t, pop1_(t+1) is the population size at the next time step, and rand is a parameter that computes the population progress rate, and rand is a parameter that controls the growth rate of the population. At low values of rand, the logistic map exhibits stable behaviour, with the population size converging to a fixed point over time. However, as r increases beyond a certain threshold, the map enters a chaotic regime, with the population size oscillating between different values seemingly randomly and unpredictably. For certain values of r, the logistic map exhibits chaotic behaviour, with the population size oscillating unpredictably over time. Other examples of chaotic maps include the Hénon map, the Lorenz map, and the Henon-Heiles map.

This chaotic behaviour arises from the nonlinear nature of the logistic map, which causes small changes in the initial population size to be amplified over time, leading to vastly different outcomes. This sensitivity to initial conditions is a hallmark of chaotic systems and is what makes them so difficult to predict and control. Despite their unpredictable nature, chaotic maps like the logistic map have numerous applications in fields such as physics, engineering, and biology [106]. For example, they can be used to model the spread of infectious diseases, the behaviour of financial markets, and the dynamics of chemical reactions. By studying the patterns of chaos within these systems, scientists and researchers can gain a deeper understanding of their underlying mechanisms and potentially develop new solutions to real-world problems.

A 2D chaotic map is a mathematical function that describes the behaviour of a system in two-dimensional space over time. It is often represented as an iterative equation that maps the values of two variables, typically denoted as (x, y), onto a new set of values at the next time step. These maps can show chaotic behaviour, meaning that minor changes in the begining conditions can lead to dramatically different results over the time. One of the most popular 2D chaotic maps is the Henon map shown in followng equations:

$$x_{(n+1)} = 1 - a * x_n^2 + y_n \tag{3.2}$$

$$y_{(n+1)} = b * x_n \tag{3.3}$$

where a and b are parameters that determine the behaviour of the system. The Henon map exhibits chaotic behaviour for certain values of a and b, with the trajectories of (x, y) in phase space exhibiting intricate and unpredictable patterns. Another example of a 2D chaotic map is the standard map, which is commonly used to model the dynamics of particles in a billiard table. The standard map is given by the equations:

$$x_{(n+1)} = x_n + y_n + K * \sin(2 * \pi * x_n) / (2 * \pi) \tag{3.4}$$

$$y_{(n+1)} = y_n + K * \sin(2 * \pi * x_n) / (2 * \pi) \tag{3.5}$$

where K is a parameter that determines the strength of the perturbation. The standard map exhibits chaotic behaviour for certain values of K, with the trajectories of (x, y) in phase space exhibiting complex and unpredictable patterns. 2D chaotic maps have numerous applications in fields such as physics, engineering, and biology. They can be used to model the behaviour of complex systems such as fluid flows, chemical reactions, and neural networks, and can provide insights into their underlying dynamics [107]. Despite their unpredictable nature, chaotic maps have proven to be a powerful tool for understanding and simulating a wide range of phenomena in the natural world.

There are many types of 2D chaotic maps, each with its own unique properties and applications. Here are some of the most well-known and widely studied types:

I. **Hénon Map :** The Hénon map is a classic example of a 2D chaotic map, and is often used as a simple model for population dynamics and other complex systems.

II. **Logistic Map :** The logistic map is a 1D chaotic map that is often extended to 2D for more complex modelling.

III. **Henon-Heiles System :** The Henon-Heiles system is a 2D Hamiltonian system that exhibits chaotic behaviour. It is often used to model celestial mechanics and other physical systems. It is defined by the equations:

$$x_{(n+1)} = px_n + 2y_n - 2x_n(x_n^2 + y_n^2) \tag{3.6}$$

$$y_{(n+1)} = py_n - x_n + y_n(x_n^2 + y_n^2) \tag{3.7}$$

where p is a constant that determines the behaviour of the system.

IV. **Chua's Circuit :** Chua's circuit is an electronic circuit that exhibits chaotic behaviour, and can be modelled using a 2D map. It is often used in electronic circuit design and other engineering applications.

V. **Rossler Map :** The Rossler map is a 3D chaotic system that can be reduced to a 2D map by projecting onto one of the axes. It is often used to model chemical reactions and other physical systems.

These are just a few examples of the many types of 2D chaotic maps that exist. Each map has its own unique properties and applications, and can be used to model a wide range of complex systems and phenomena. 2D chaotic map data encryption algorithms are cryptographic algorithms that use 2D chaotic maps as their basis for encryption [108]. Overall, 2D chaotic map encryption algorithms are an important tool in the field of cryptography, and their use is likely to continue to increase as the need for secure data transmission and storage becomes ever more critical in today's digital world. These maps generate a stream of pseudorandom numbers that are used to encrypt the plaintext data.

Here are some common 2D chaotic map encryption algorithms:

1. **Arnold Map Encryption Algorithm:** This Algorithm uses the Arnold map, which is a 2D chaotic map that rearranges the positions of the plaintext data. The positions of the rearranged data are then scrambled using a secret key.

2. **Logistic Map Encryption Algorithm:** This Algorithm uses the logistic map, which is a 2D chaotic map that generates a stream of pseudorandom numbers. The plaintext data is then XORed with the pseudorandom numbers generated by the map.

3. **Baker Map Encryption Algorithm:** This Algorithm uses the Baker map, which is a 2D chaotic map that stretches and folds the plaintext data. The stretched and folded data is then XORed with a pseudorandom sequence generated by the Baker map.

4. **Henon Map Encryption Algorithm:** This Algorithm uses the Henon map, which is a 2D chaotic map that generates a stream of pseudorandom numbers. The plaintext data is then XORed with the pseudorandom numbers generated by the map.

Additionally, it's important to note that while 2D chaotic map encryption algorithms can provide a high level of security, they can also be vulnerable to brute force attacks or cryptanalysis attacks. Therefore, it's important to use strong and complex keys and other security measures such as authentication and access control to ensure the confidentiality and integrity of the encrypted data [109].

We can use 2D chaotic maps to encrypt data using the chaotic evaluate of the system to generate a robust secret key. The 2D chaotic map data encryption system can be developed using the following Steps:

(a) **Select a 2D chaotic map:** We have different types of 2D chaotic maps such as Henon, Arnold chat, Logistic, and Circle maps.

(b) **Chaotic Map Key Generation:** The secret key for data encryption and decryption is generated using the chaotic evaluate of the map. We can generate secret key with an initial value of map and apply the map many times. The output values of the map can be used as the private key.

(c) **Data Encryption:** We can apply XOR operation between generated secret key and data for data encryption.

(d) **Data Decryption:** The secret key is XORed with ciphertext data for data decryption.

This chapter is divided in 4 sections. Section 3.1 introduces the chaotic map-based data encryption techniques. Section 3.2 presents the Big Bang Big Crunch (BBBC) algorithm. Section 3.3 proposes the integrated BBBC and 2D Chaotic map approach. Section 3.4 presents the simulation, results and discussion. Section 3.5 concludes the chapter.

3.2 BIG BANG BIG CRUNCH ALGORITHM (BBBC)

Big Bang Big crunch (BBBC) algorithm is based upon the evolution of the Universe theory. In this theory, the universe started as an extremely hot and dense point about 13.8 billion years ago. It rapidly expanded and cooled down, forming subatomic particles, atoms, and eventually stars and galaxies. In the big crunch phase, the universe will stop growing and start contracting, eventually collapsing in on itself. During this time, everything in the universe would get hotter and denser until it became a tiny, infinitely dense point called a singularity. Based upon BBBC theory, Erol et al. proposed a new soft computing-based algorithm called Big Bang – Big crunch algorithm (BB-BC). The BB-BC Algorithm consists of two operations: Big Bang and Big Crunch. In the Big Bang operation, energy dissipation produces disorder and randomness, which is this phase's main feature. In this operation, the population of candidate solutions are created randomly. In this phase, candidate solutions are spread uniformly throughout the search space. Randomness is the main feature of this operation.

The randomly distributed particles in the Big Bang phase are drawn into an order using the Big Crunch phase. The Big crunch is a convergence operation. In this operation, many candidate solutions are converged into one candidate solution. This one converged solution is referred to as the "Center of Mass". The center of Mass can be calculated using equation 3.8.

In equation 3.8, x^i is a point within an n-dimensional search space generated, f^i is a fitness function value of this point, and N is the population size in the Big Bang phase. In our research work, the center of Mass is the best candidate solution amongst all the candidate solutions. The best candidate solution is referred to as "elite". After calculating the elite value, The Big Bang operation would be started. In Big Bang operation, a new population of candidate solutions is generated around the elite by adding or subtracting a small random number. The new population around the elite can be generated using equation (3.9).

In equation 3.9, x^c stands for center of Mass, l is the upper limit of the parameter, r is a normal random number and k is the iteration step. Then new point x^{new} is upper and lower bounded.

The Big Bang and Big Crunch operations are repeated continuously until the termination criteria is not met. The termination criterial could be any one from the following:

- Maximum Number of Iterations
- Allowed time is Exceeded
- Desired Performance is achieved

We can select any one above mentioned criteria to stop the big bang and big crunch operations in the Algorithm. The Big Bang and Big Crunch algorithm is shown as Algorithm 3.1.

Algorithm 3.1: Big Bang Big Crunch Algorithm

Begin

Generate initial of population of random candidate solutions by respecting the limits of the search space.

While (Termination Criterial not Met)

Calculate the fitness of all randomly generated candidate solutions

/*Big Crunch Phase Started*/

Compute the Center of Mass using equation 3.8.

$$\vec{x}^{c} = \frac{\sum_{i=1}^{N} (1/f^{i}) \vec{x}^{i}}{\sum_{i=1}^{N} (1/f^{i})} \tag{3.8}$$

/*Big Crunch Phase Ended*/

/*Big Bang Phase Started */

Calculate new candidates around the center of Mass using equation 3.9.

$x^{new} = x^{c} + lr/k$ (3.9)

End While

End

3.3 PROPOSED BIG BANG BIG CRUNCH INTEGRATED 2D CHAOTIC MAPS APPROCH FOR DATA ENCRYPTION AND DECRYPTION

This section proposes an integrated Big Bang Big Crunch and 2D Chaotic approach for data encryption and decryption. Chaotic maps are very sensitive to initial conditions, which means that even minor changes in the initial conditions can result in drastically different output values. This can make the encryption unstable, making it challenging to generate and manage the keys accurately. Thus there is a need for an intelligent search & optimization approach to optimize the parameters of chaotic maps. The Big Bang Big Crunch algorithm utilizes Circle Map and Henon map for data encryption and decryption. The circle maps and Henon maps can be defined using equation 3.10 and equation 3.12 as given below:

$$\mathbf{x(i+1) = C(a, b, y(i)) \bmod 1} \qquad \mathbf{(3.10)}$$

Where x(i) is the state of the system a iteration i. C(a, b, y(i)) can be defined using equation 3.4.

$$\mathbf{C(a, b, y(i)) = a + (b - a) * y(i)} \qquad \mathbf{(3.11)}$$

where a and b are the parameters that compute the parameter y(i) range. The parameter y(i) can be any value between 0 and 1 and normally selected randomly. In our research work the range of a is between 1 to 4 and range of b parameter should be between 0.1 to 0.4

$$\mathbf{y(I + 1) = H(a, x(i))} \qquad \mathbf{(3.12)}$$

The encryption system equation can be defined as below:

$$\mathbf{x(I + 1) = x(i) + d + (a \sin(2\pi y(i))) \bmod 1} \qquad \mathbf{(3.13)}$$

$$\mathbf{y(I + 1) = 1 - ax(i)2 + y(i)} \qquad \mathbf{(3.14)}$$

The working of the proposed approach is shown in algorithm 3.1.

Algorithm 3.2: Proposed BBBC based approach for Data Encryption

Begin

Initialize a N sized random population of a and b parameters by respecting the bounds and violations. Each individual in the generated population is referred as candidate solution.

'or iteration = 1 to max_iteration /*Here max_iteration is the termination criteria */

For I = 1 to N

Generate chaotic map values for i^{th} candidate solution using equation 3.13 and 3.14.

Apply shuffling operation to these chaotic map values to generate the private key for i^{th} candidate solution in the population.

For the encryption purpose, Covert message into a list of ASCII codes and add each code to the corresponding private key value (This will generate the list of integers).

The cipher text is generated by covert back all lists of integers into strings

Record the fitness of the cipher text for i^{th} candidate solution using jackard index

End for

Select the best candidate solution among all generated candidate solutions on the basis of calculated fitness values.

If iteration == 1

elite = best fit candidate solution /* Here elite is the best candidate solution */

End if

If elite < best fit candidate solution

elite = best fit candidate solution

End if

Generate the new population of size “N” around the elite candidate solution by adding of subtracting a small random number into it.

End for

End

As shown in algorithm 3.2, we have to optimize chaotic maps' a and b parameters. The proposed algorithm starts with an initial random population of chaotic map parameters. We are optimizing the parameters for the specific number of iterations. In algorithm 3.2, "Max_iteration" is the termination criterial of the Algorithm. For each candidate solution in the population, compute the chaotic map values using equation 3.6 and 3.7. Using these chaotic map values, we identify the private key for each candidate solution using shuffled operation. Further, using the computed private key of each candidate solution we encrypt the data. The fitness of each candidate solution is computed by applying the jaccard index function on encrypted data and plain text data. In this research work, the Jaccard index is first calculated as the ratio of the size of the intersection of the two sets to the size of their union. This value is then multiplied by 100 to obtain a percentage score, subtracted from 100 to get the Jaccard similarity score. For example, if the Jaccard index is calculated to be 0.9, this means that the two input sets share 90% of their data elements. Therefore, the Jaccard similarity score would be 100 – 0.9*100 = 10, indicating that the sets are 10% dissimilar.

After the computation of the fitness of each candidate solution in the population, Identify the best fit candidate solution. The best fit candidate solution is referred as "elite". This is the big bang phase for proposed data encryption technique. For the proposed approach's big crunch operation, we generate a random population of chaotic map parameters around the elite. The new generated population is sent for next iteration optimization.

3.4 SIMULATION, RESULT AND DISCUSSION

For the simulation purpose, we implemented the proposed approach in python and tested it on different sized plain text sequences. The BBBC algorithm is deployed on 2D chaotic maps to produce the optimal a and b parameters. Table 3.1 and Figure 3.1 show the proposed approach's Performance on different data sequences. As shown in Table 3.1, The proposed method outperforms Genetic Algorithm based 2D Chaotic Map Approach. Figure 3.1 shows that the proposed approach achieved 93.3333 fitness of the plain text of size 10 characters. Whereas, on the same data size, Genetic Algorithm based approach produced 85.7142 fitness.

Table 3.1: Comparative Performance of proposed Approach on different sequences of data

Length of Plain Text	Genetic Algorithm Based 2D Chaotic Map Approach	Proposed BBBC Based Approach
10	85.7142	93.3333
50	94.5945	97.5609
100	95.9459	98.7341
500	99.5614	99.7041
1000	99.6996	99.8496

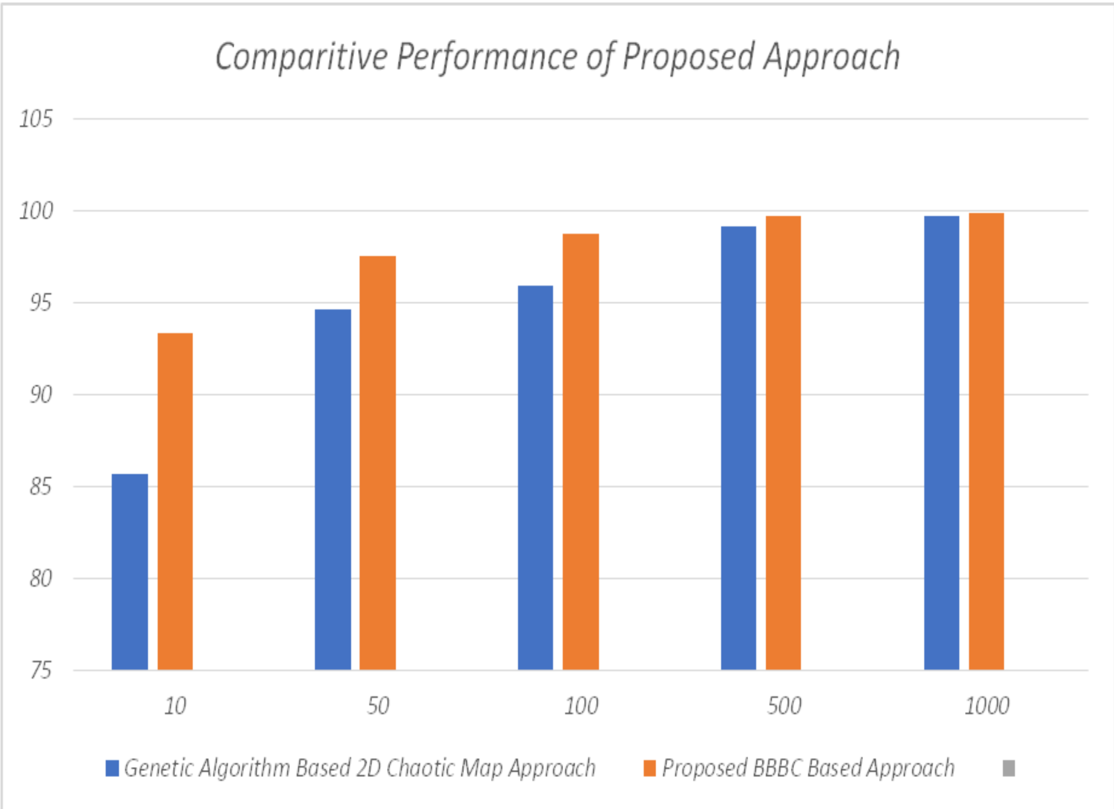


Figure 3.1: Comparative Performance of proposed Approach on different sequences of data

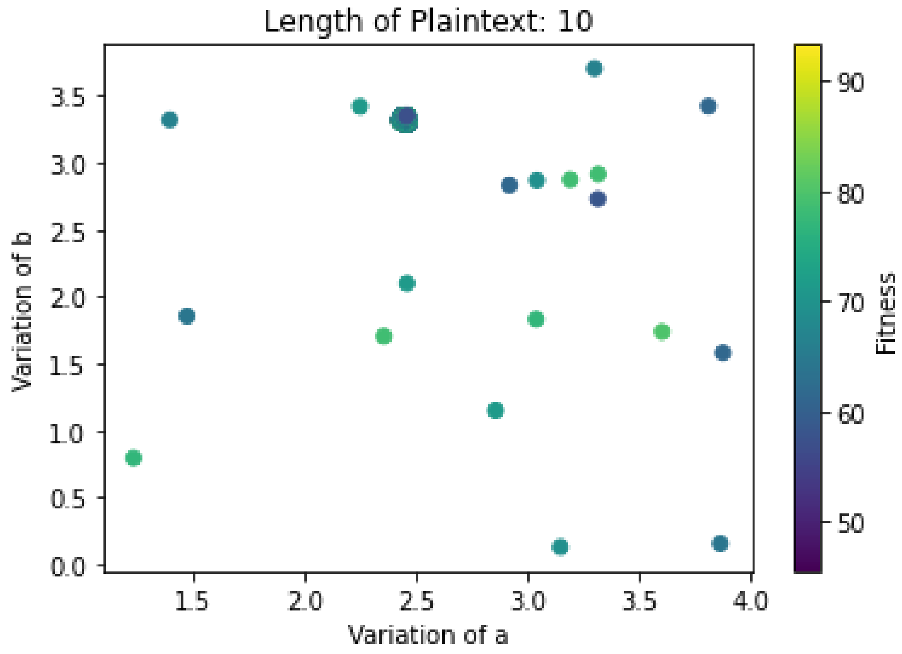


Figure 3.2: Fitness of the 2D Chaotic map data encryption using proposed approach on evolved a and b parameters values

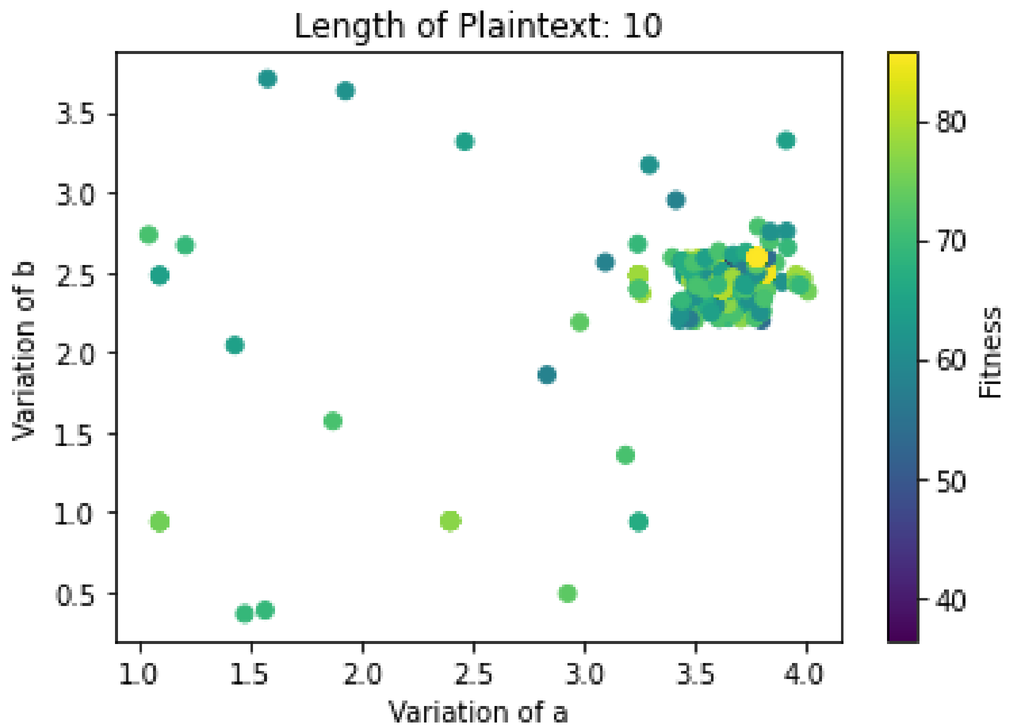


Figure 3.3: Fitness of the 2D Chaotic map data encryption using Genetic Algorithm on evolved a and b parameters values.

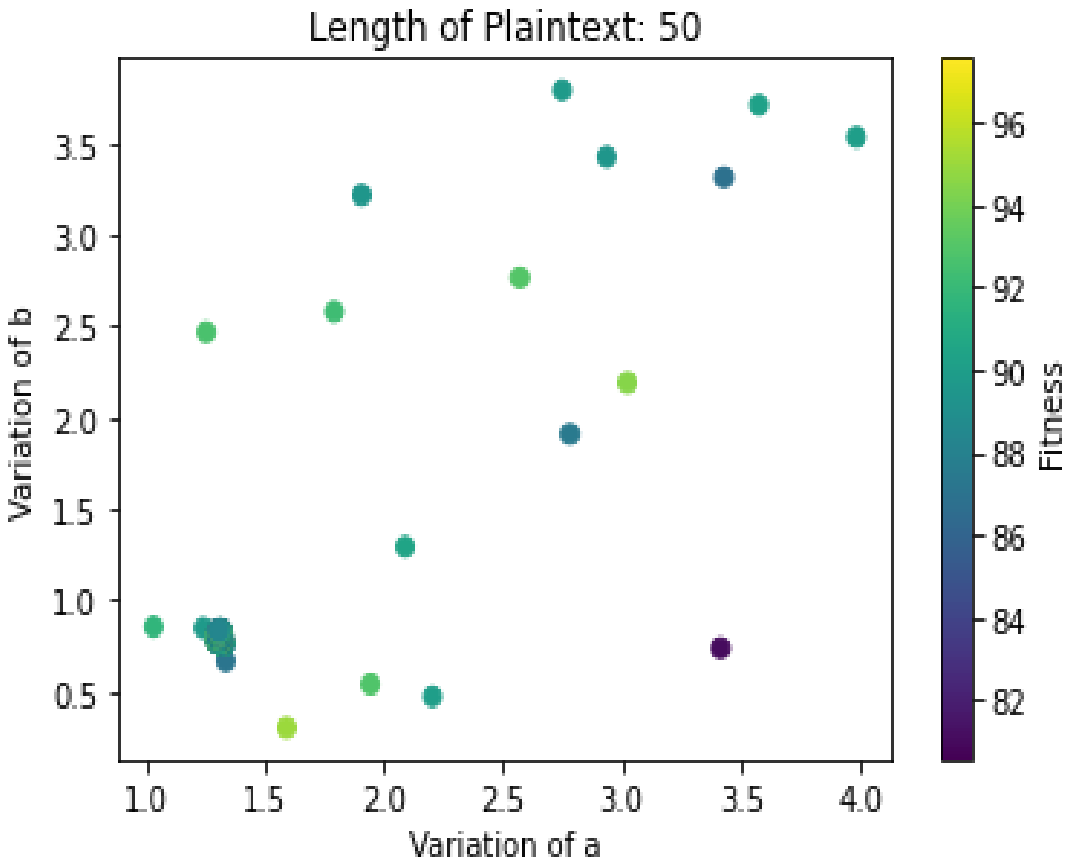


Figure 3.4: Fitness of the 2D Chaotic map data encryption for text length of 50 using proposed approach on evolved a and b parameters values

We tested the proposed approach on 50 character-sized data for the performance analysis purpose. Table 3.1, figure 3.1 and figure 3.2 show that the proposed approach achieved the cipher text with 97.5609 fitness. The genetic Algorithm based approach produced 94.5945 fitness on 50 character-sized data. Further, we observed that on 100, 500 and 1000 character-sized data, the genetic Algorithm based approach produced 95.9459, 99.1304, 99.6996 fitness respectively. The proposed method outperformed the genetic Algorithm based approach by achieving 98.7341, 99.7041, and 99.8496 fitness on 100, 500 and 1000 character-sized data.Figures 3.5-3.11 show the fitness of choatic maps on different values of a and b parameters.

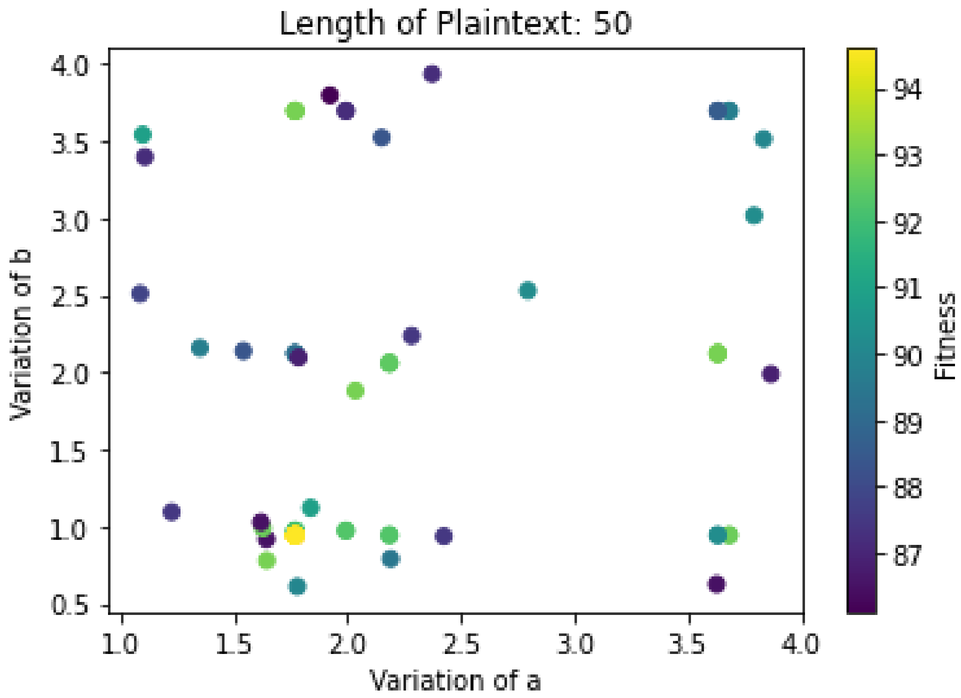


Figure 3.5: Fitness of the 2D Chaotic map data encryption for text length of 50 using genetic Algorithm on evolved a and b parameters values.

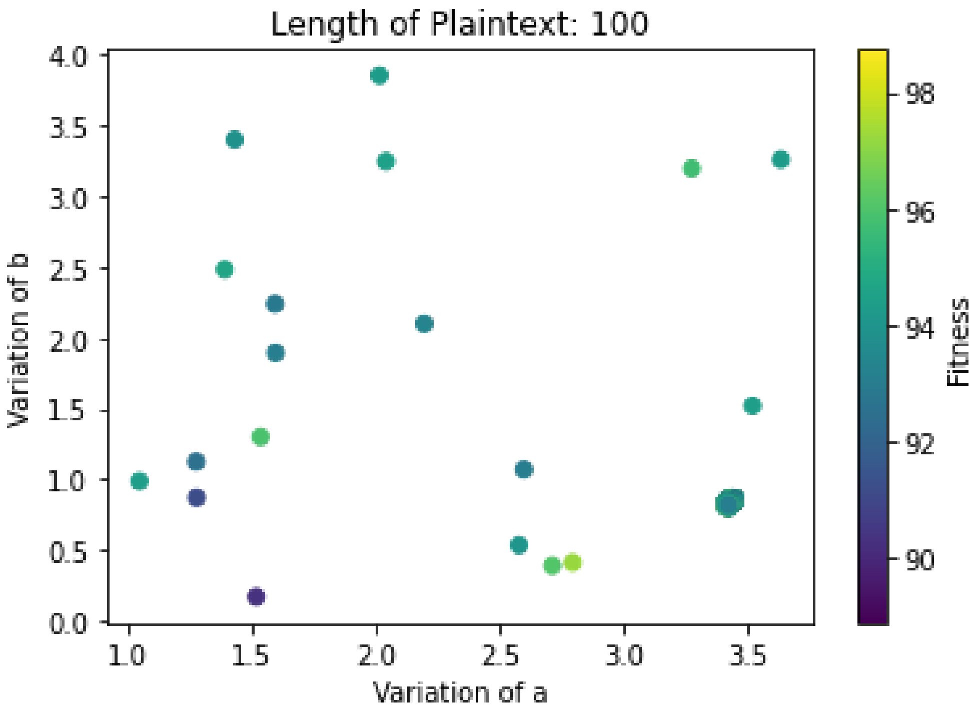


Figure 3.6: Fitness of the 2D Chaotic map data encryption for text length of 100 using proposed approach on evolved a and b parameters values.

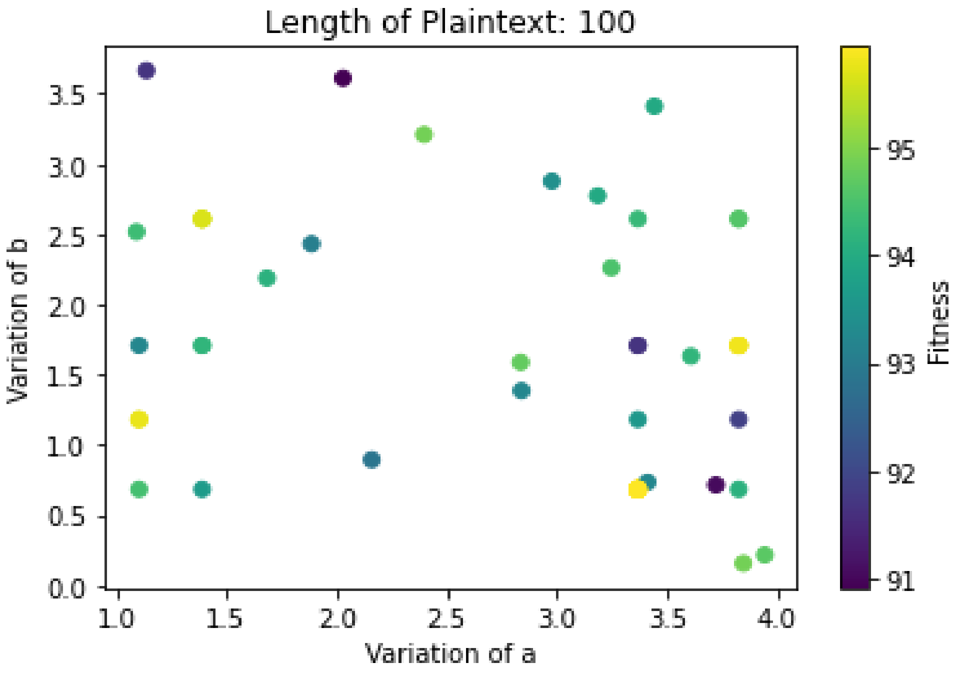


Figure 3.7: Fitness of the 2D Chaotic map data encryption for text length of 100 using genetic Algorithm on evolved a and b parameters values

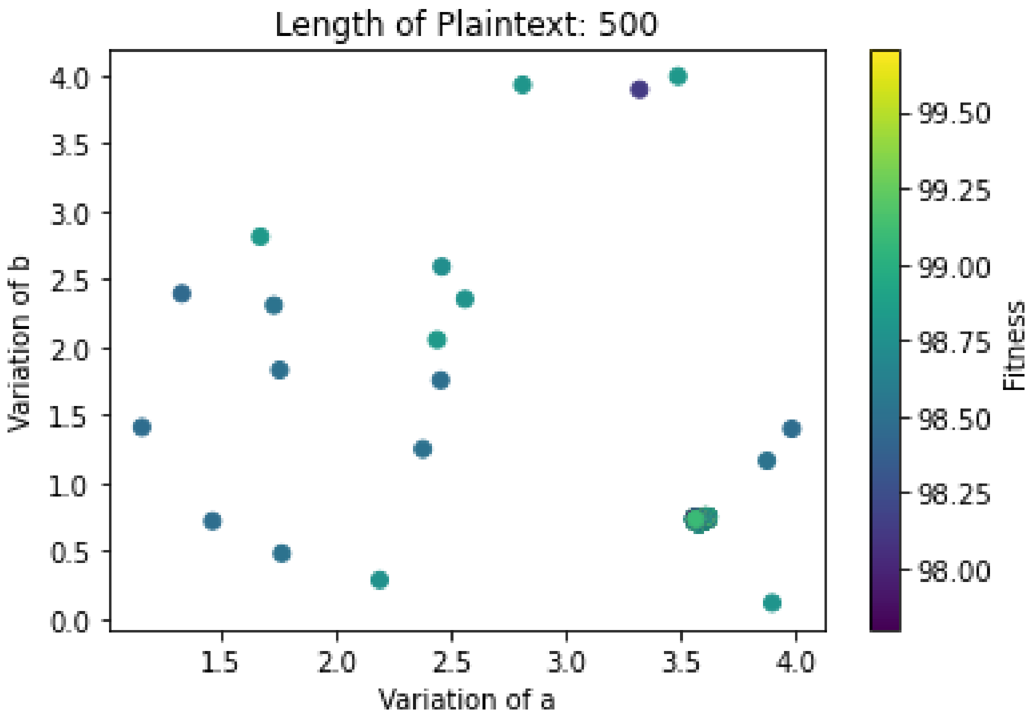


Figure 3.8: Fitness of the 2D Chaotic map data encryption for text length of 500 using proposed approach on evolved a and b parameters values

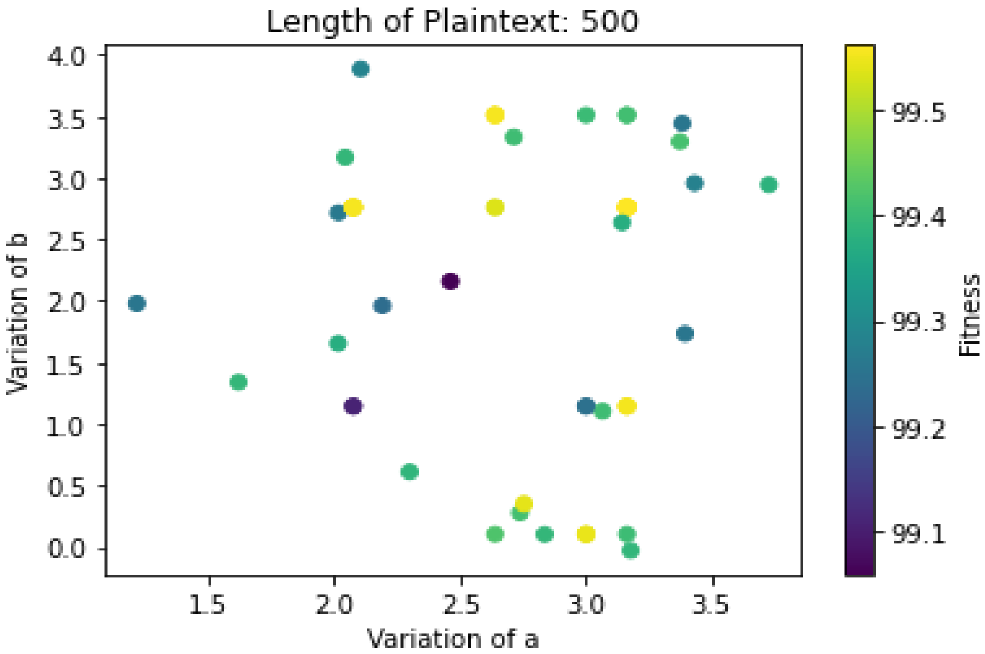


Figure 3.9: Fitness of the 2D Chaotic map data encryption for text length of 500 using genetic Algorithm on evolved a and b parameters values

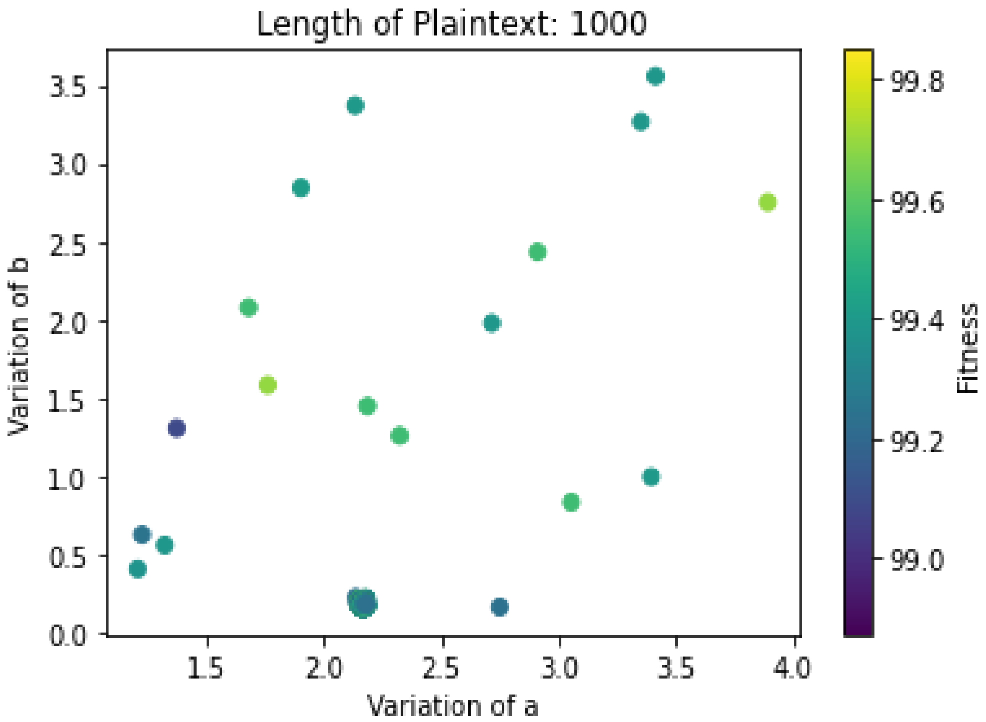


Figure 3.10: Fitness of the 2D Chaotic map data encryption for text length of 1000 using proposed approach on evolved a and b parameters values

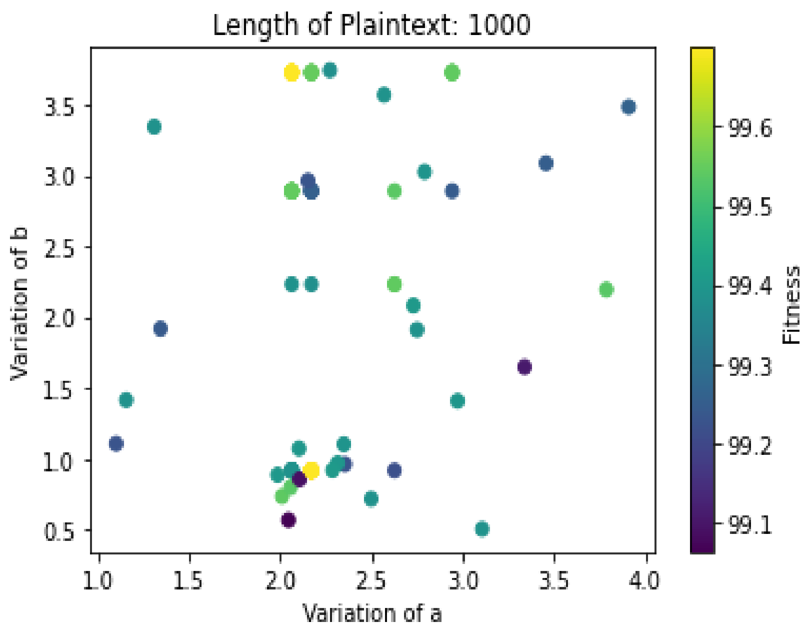
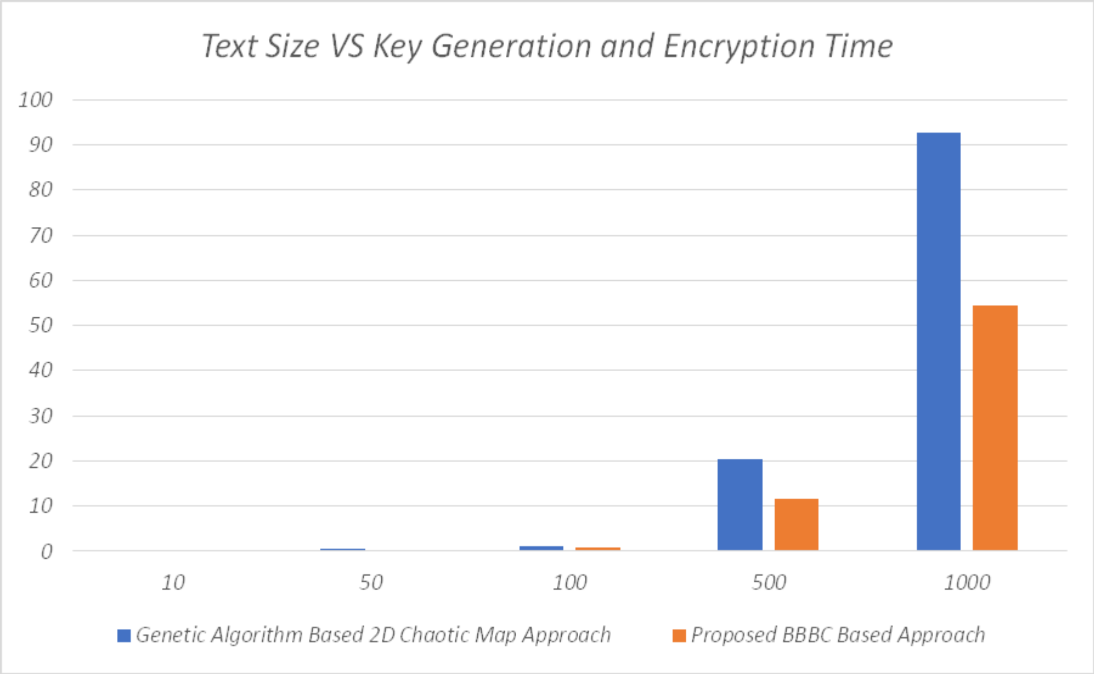


Figure 3.11: Fitness of the 2D Chaotic map data encryption for text length of 1000 using genetic Algorithm on evolved a and b parameters values

For comparison purpose we evaluate the performance of existing and proposed approach using encryption time. From table 3.2 we observe that the proposed approach generated private key and encrypted text in 0.0581, 0.2649, 0.7407, 11.6950, 54.3559 seconds for 10, 50, 100, 500 and 1000 text sizes. From these results we observe that the proposed approach generates the key and encrypt data more quickly as compared to genetic algorithm-based approach. Further, we also observe that if the chaotic map parameters are optimized then decryption time of proposed and existing approach would be same.

Table 3.2 : Comparative Performance of Proposed Approach on Key Generation and Encryption Time

Length of Plain Text	Genetic Algorithm Based 2D Chaotic Map Approach	Proposed BBBC Based Approach
10	0.0973	0.0581
50	0.4556	0.2649
100	0.9987	0.7407
500	20.2894	11.6950
1000	92.6471	54.3559



3.5 CONCLUSIONS

This chapter proposes an integrated BBBC and 2D Chaotic map approach for data encryption. In this chapter, we optimized the chaotic map's initial parameters with the BBBC algorithm's help to produce the complex and unpredictable key. We compared the Performance of the proposed approach with the existing 2D chaotic map and genetic algorithm approach. For comparison purposes, we tested it on different character-sized text. We observed from the results that the proposed approach outperformed the existing one on all sized text.

Chapter – 4

DATA SECURITY IN CLOUD: A NEW SECURE USER AUTHENTICATION FRAMEWORK

4.1 INTRODUCTION

Recent developments in ubiquitous and context-aware computing have sparked a wave of innovation, giving rise to many applications. Smart healthcare, smart city initiatives, smart transportation systems, and many more have emerged, revolutionizing how users interact with the world. Promising technologies, including cloud computing and the Internet of Things (IoT), have benefited from the proliferation of these applications. IoT, in particular, is steadily advancing towards creating integrated environments that cater to intelligent services for humanity. Its vision is establishing connectivity for everything, requiring minimal storage and computational capabilities. Through the seamless integration of heterogeneous devices spatially dispersed and interconnected through networks, IoT adapts to the diverse demands of users and services. This transformative technology represents the future of connectivity and reachability, where devices become intelligible, recognizable, locatable, and controllable through the Internet, leveraging technologies like RFID, wireless LAN, and other means. As the digital frontier continues to expand, the fusion of ubiquitous computing, context-awareness, cloud computing, and IoT ushers in a new era of possibilities. The complexity and diversity of these innovations promise a landscape teeming with burstiness, combining both elaborate and concise expressions to captivate users all across the globe. The convergence of technologies fuels the drive towards intelligent solutions, revolutionizing various industries and empowering individuals with transformative digital experiences.

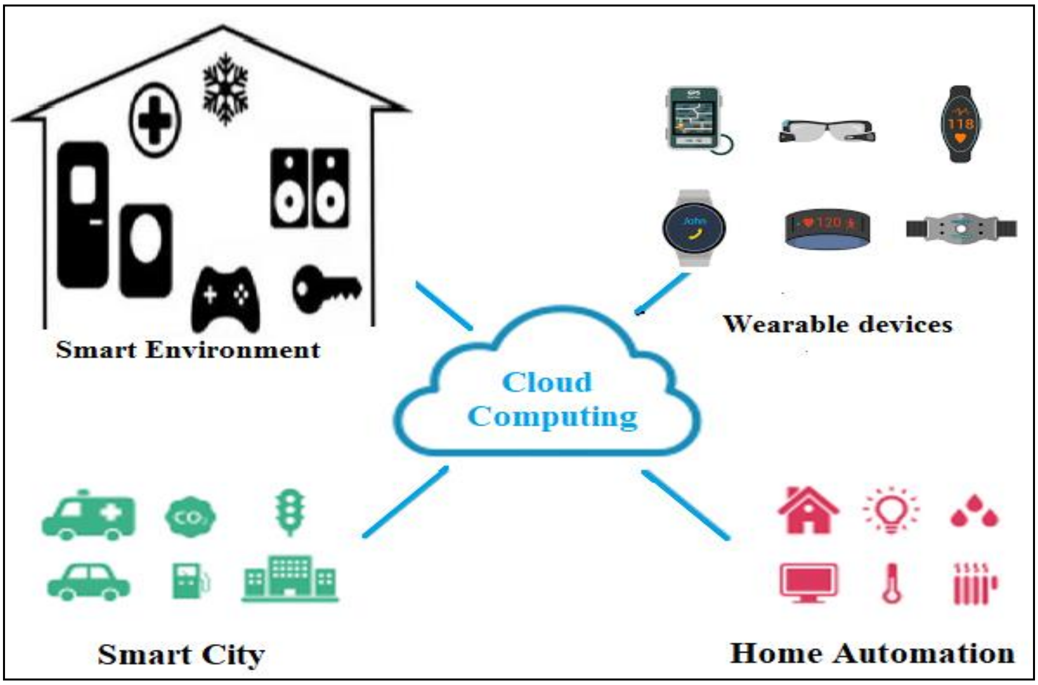


Figure 4.1. Cloud-IoT Environment

The cloud-IoT environment is depicted in Figure 4.1.

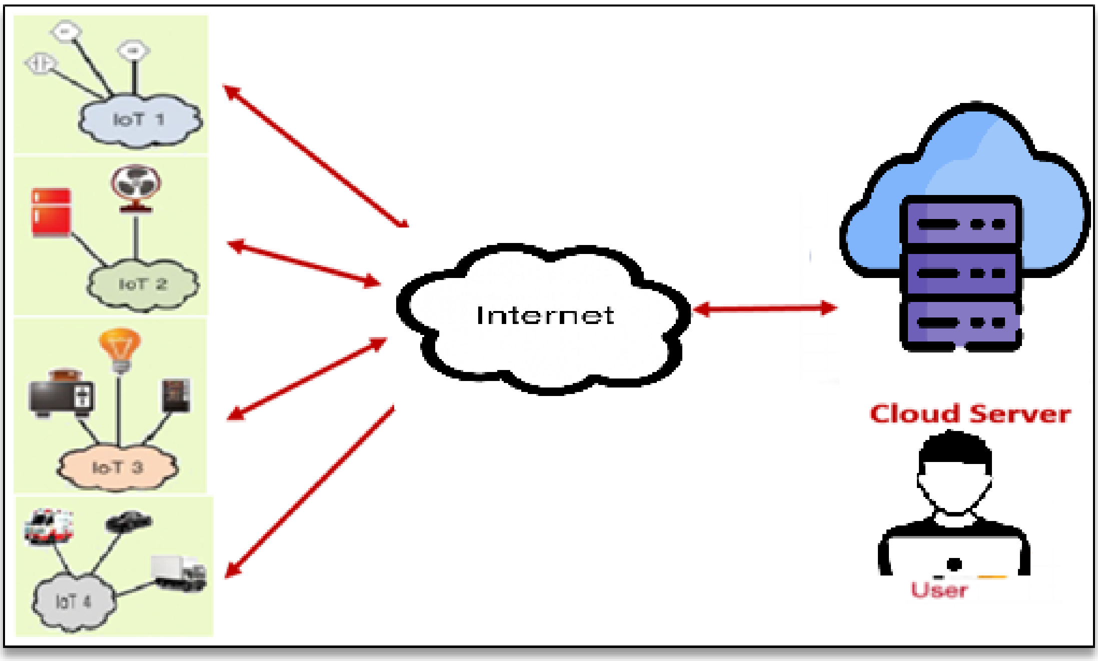


Figure 4.2. Authentication Framework

The realm of data in era of global computing and the IoT is a captivating tapestry woven from diverse smart devices – sensors, mobile devices, actuators –

orchestrating a symphony of ubiquitous services for users worldwide. The possibilities are vast and compelling, from healthcare to automobiles, surveillance to security, industrial appliances to safer mining production, and traffic management to ambient-assisted living. However, a huge concern looms large amongst this technological marvel – the IoT environment's data flood caused by these smart gadgets. This torrential flow of information presents a colossal challenge for standalone power-constrained IoT devices, rendering them inadequate to handle such an overwhelming data influx. The clever answer is to upload the created data to the cloud for long-term archival. Cloud computing emerges as the bedrock of the envisioned IoT and the future Internet, offering the ultimate conduit to connect, manage, and track the IoT landscape. It serves as a pivotal technology, paving the way for the realization of IoT's ambitious objectives. The intricate dance between IoT and cloud computing finds them deeply interdependent, each propelling and supporting the other's boundless potential. In this captivating symphony of technology, complexity and diversity converge, giving rise to an intricate narrative of perplexity and burstiness. The interplay of ideas and innovations creates a vibrant mosaic, shaping the trajectory of the IoT landscape and opening doors to unprecedented possibilities on the horizon. The mutual dependence between IoT and cloud computing sets the stage for a harmonious future where the orchestration of data and services transcends boundaries and touches the lives of billions around the globe.

However, the private information gathered by IoT devices is kept in the cloud and accessible to users from any location at any time. This leads to the potential risk of data threat. Remote users must be authenticated before giving access to resources and data. There is a need to secure data stored in the cloud using a cryptographic mechanism. Several authentication mechanisms have been proposed in the literature to secure the data stored in cloud. The most typical approach for two communicating parties to authenticate each other is by using a previously shared password. Communication parties calculate a session key to encrypt subsequent communications using this shared secret. Because most user-chosen passwords are restricted to the user's domain, an attacker or privileged insider has the best chance of stealing the user's password. As a result, dictionary attacks can be used to compromise password-based authentication systems. Existing security measures are insufficient to ensure the bare minimum level of security in the cloud-IoT ecosystem. Limitations of existing schemes are as below:

a) Replay attacks, denial of service attacks, insider attacks, user impersonation attacks, and offline password guessing assaults are examples of significant network attacks that were mostly ineffectual against most of the tactics.

b) Since the sensors have limitations on their battery life, memory, and computing power, the existing systems' high calculation costs make them unsuitable for environments with scarce resources.

c) Most of the solutions were unable to provide user privacy and mutual authentication.

d) Majority of existing authentication mechanisms are not designed for Internet scale and are not suited to meet the requirements of safety-critical components.

Multi-factor authentication is a workable option for assuring security and privacy in IoT networks due to the speed at which smart devices communicate to the Internet. This chapter presents a framework for securing the data stored on the cloud envrionment.

Section 4.2 of this chapter discusses the proposed cloud data security approach. The comparative performance of the suggested multi-factor user authentication approach is shown in Section 4.3. The formal verification of the suggested approach using AVISPA is covered in Section 4.4. Section 4.5 concludes the chapter.

4.2 PROPOSED DATA SECURITY APPROACH

This section proposes a new framework for data security in the cloud. Figure 4.1 depicts the proposed scheme's operational architecture.

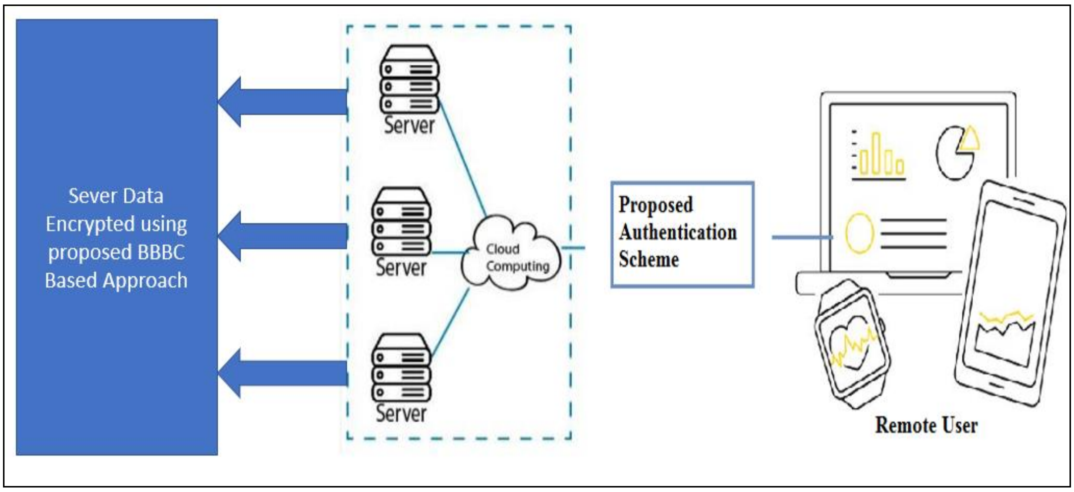


Figure 4.3: Proposed Framework for data security in the cloud.

As shown in Figure 4.3, the proposed framework works in 2 phases. Phase 1 of the proposed approach consists data encryption module. The phase stores the encrypted data on the server using BBBC (Big Bang – Big Crunch) based data encryption approach. The BBBC-based data encryption approach is already discussed in Chapter 3 of this thesis. Phase 2 of the suggested framework uses a multi-factor user authentication system to secure the cloud-based data. Figure 4.3 shows the workflow of the proposed user authentication scheme. The following phases make up the multi-factor user authentication technique, which is secure against well-known security exploits:

(a) Registration
(b) Login
(c) Authentication
(d) Smart card revocation

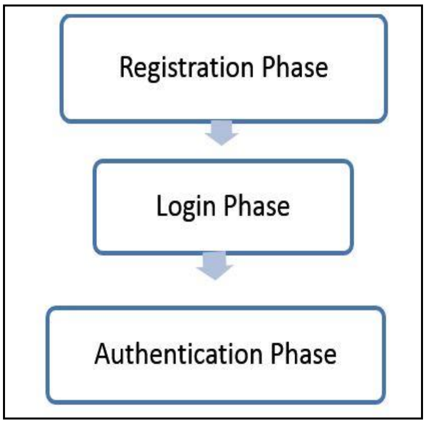


Figure 4.4. Workflow of proposed scheme

The parameters computed in the proposed scheme are computed by the user and server, respectively. Users can connect to the server using a smartphone or any terminal, such as a laptop, smart card reader, etc. These devices compute these parameters and then send them to the server at a remote location using the internet. In turn, the cloud server also calculates parameters. After calculating, the server stores the required parameter in memory and communicates the rest.

The proposed scheme includes the entities as below:

a) ***Remote User*****:** This is the person who wants to use the cloud server's features. The remote user is attempting to access any distant location's resources. The primary task is to gain access to cloud server services as and when requested.

b) ***Remote Server*****:** The requests of users are handled by the cloud server. The cloud server grants access to resources and services. The cloud server is remote but provides access to all users trying to access the cloud services.

c) ***Smart Card*****:** Temper-proof plastic card which has limited memory and processing capacity. The microcontroller chip in the smart card can manage data in its memory and perform on-card processing activities. It offers multiple-factor authentication to confirm the distant user's identity. One of the most practical methods for safeguarding private information on an unsecured public network is the smart card. Table 4.1 lists all notations used by the proposed approach.

Table 4.1. Notations

Symbols	Meaning
U_i	I^{th} number user
SR	Server
Id_i	Identity of user
SId_i	Identity of server

Symbols	Meaning
PW_i	User Password
Boi	Biometric of user
SC	Smart card
R_1,R_2,R_3	Random nonces
P,Q	Secret keys of the server
T_1,T_2,T_3	Time stamps
T	The permissible time interval for the allowed delay
S_k	Session key
H(.)	Hash operation
||	Concatenation operation
$\oplus$	XOR operation

4.2.1 Registration Phase

This is the initial phase of the proposed scheme. In the registration phase, the remote user registers itself with the server. Without registration, no user can access the services of the server. In the suggested technique, a user Ui submits a request for registration to the server SR for the purpose of registration. To register successfully, the user U_i performs the steps as given below. Figure 4.5 depicts the registration process of the scheme.

Step 1: The proposed scheme permits a user to select login credentials of their choice. For enhance security, the scheme employs unique biometrics of the user. The user U_i selects Id_i, password PW_i and sends their biometric BO_i at the cloud sensor. U_i produces a random nonce R_1 and computes $MBO_i = H(R_1 \| BO_i)$, $MUB_i = H(Id_1 \| BO_i)$, and $A_i = H(Id_i \| PW_i \| MUB_i)$ and sends the message $\{Id_i, A_i\}$ to the remote server SR via a secure channel.

Step 2 : SR calculates $B_i = H(MId_i \| P)$, using the private key *P*, $C_i = H(B_i)$, $D_i = C_i \oplus H(A_i \| Id_i)$, $E_i = H(A_i \| C_i) \oplus H(P)$, $F_i = B_i \oplus H(H(P) \| Q)$ and $G_i = A_i \oplus Id_i$. SR stores {A_i, D_i, E_i, F_i, H(·)} into the smart card and is issued to the user U_i via a secure channel.

Step 3 : User U_i stores MUB_i into smart card SC. Now, SC stores {A_i, D_i, E_i, F_i, H(·), MUB_i} into it.

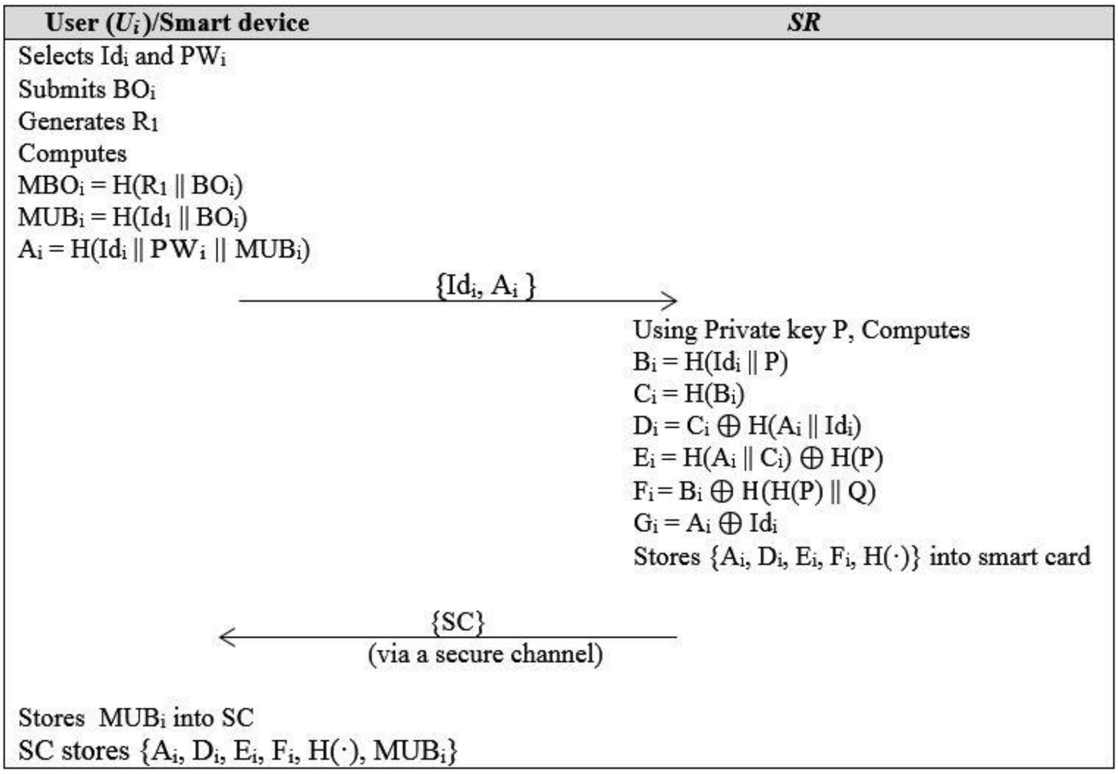


Figure 4.5 : Registration Process

4.2.2 Login Phase

A user Ui sends a login request to the server to access its services during the login phase of the suggested data security approach. The steps for the login process is given as below:

Step 1: The user U_i enters his smart card into the reader and enters the identity Idi', password PWi', and biometric imprint BOi' to the sensor at current timestamp T_1.

Step 2 : At current timestamp T_1' and smart card SC verifies if $(T1' - T1) \leq \triangle T$?. If the condition fails, the process is aborted. Otherwise, a process continues. SC computes $Ai' = H(Idi' \| PWi' \| MUBi')$ and $Gi' = Ai' \oplus Idi'$. It verifies if $G_i = G_i$?

and stored A_i = A_i' ?. If the condition satisfies, the process continues. Else, it terminates the session.

Step 3 : At current timestamp T_2, SC generates random nonce R_2 and extracts $C_i = D_i \oplus H(A_i \parallel Id_i)$, $H(P) = E_i \oplus H(A_i \parallel C_i)$, $Auth_1 = C_i \oplus R_2 \oplus H(H(P) \parallel SId_i)$, $Auth_2 = H(H(P) \parallel SId_i) \parallel C_i \parallel R_2 \parallel T_2)$. It sends message {$Auth_1$, $Auth_2$, T_2, F_i} to the server.

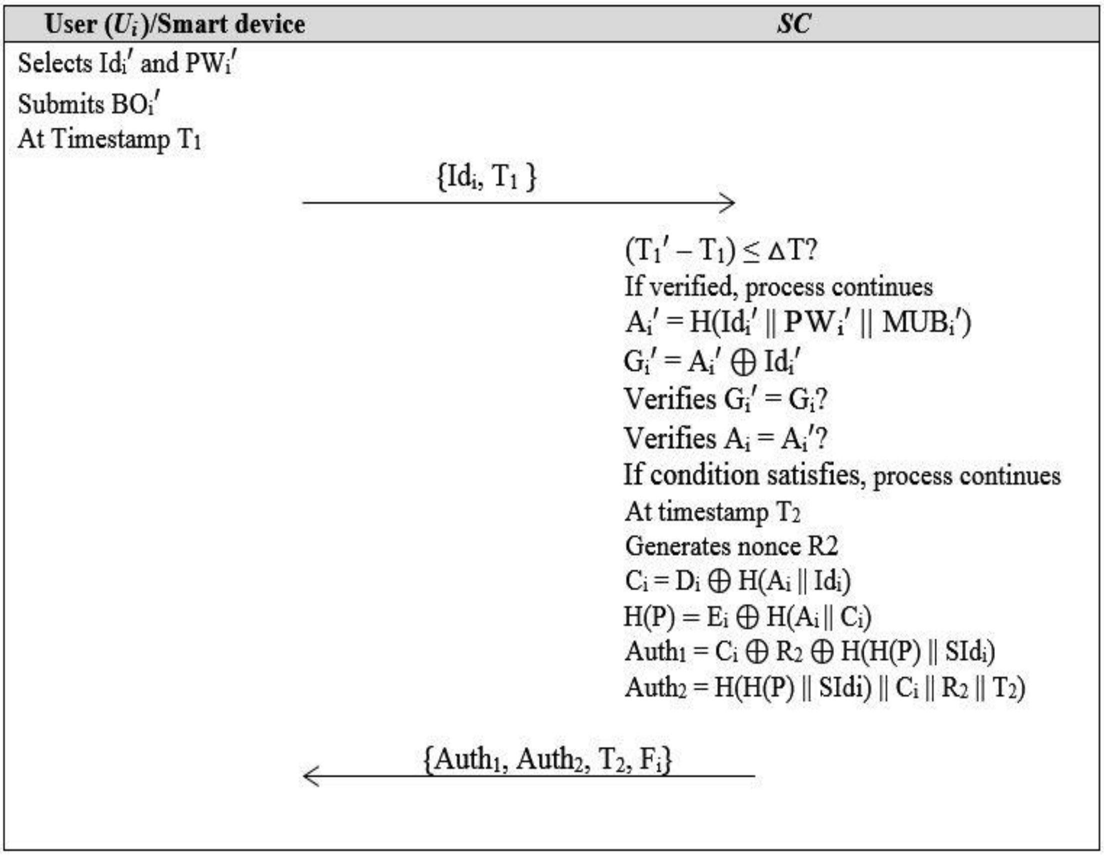


Figure 4.6. Login process

4.2.3 Authentication Phase

The suggested approach's authentication step enables mutual authentication between the server and the user. After successful mutual authentication, the suggested method generates a shared secret key. The steps involved in authentication are as follows:

Step 1: After getting {$Auth_1$, $Auth_2$, T_2, F_i}, SR producess recent timestamp T_2 and checks if $(T_2 – T_2) \leq \triangle T$?. This condition confirms resilience against replay attacks. If the given condition is false, the authentication process is terminated. Else, if the condition is true then SR extracts $Bi = H(H(P) \| Q) \oplus Fi$ and $R_2 = Auth1 \oplus H(Bi) \oplus H(H(P) \| SIdi)$ to compute $Auth_2 = H(H(P) \| SIdi) \| Ci \| R_2 \| T_2)$. If $Auth_2 = Auth_2$?. If it holds, the process continues. Else, it terminates the session.

Step 2: Further, SR generates R_3 at current timestamp T_3 computes $Auth_3 = R_3 \oplus H(SId_i \| R_2 \| T_2)$, $Auth_4 = H(SId_i \| R_2 \| R_3 \| T_2 \| T_3)$. SR sends $\{Auth_3, Auth_4, T_3\}$ to user U_i.

Step 3: Upon receiving the message $\{Auth_3, Auth_4, T_3\}$ at current timestamp T_3 , U_i verifies if $(T_3 – T_3) \leq \triangle T$?. If the condition fails, the session is terminated. Otherwise, U_i extracts $R_3 = Auth_3 \oplus H(SIdi \| R_2 \| T_2)$ and computes $Auth_4 = H(SIdi \| R_2 \| R_3 \| T_2 \| T3)$. It then verifies if Auth4 = Auth4. The process advances to the next stage if the verification is successful, at which point the user authenticates the remote server. Otherwise, Ui aborts the authentication process.

Step 4: At current timestamp T_4, U_i calculates $Auth_5 = H(H(P) \| SId_i) \| R_3 \| T_4)$ and a secret session key $S_K = H(H(H(P) \| SId_i) \| R_2 \| R_3)$ and $Auth_6 = H(S_K \| R_2 \| R_3)$. Then, it sends message $\{Auth_5, Auth_6, T_4\}$ to S_i.

Step 5: Upon receiving the message $\{Auth_5, Auth_6, T_4\}$, the SR first verifies the timestamp's authenticity. SR generates the current timestamp T_4. SC verifies if $(T_4 – T_4) \leq \triangle T$?. If the condition fails, the session is terminated. Otherwise, SC computes $Auth_5 = H(H(P) \| SIdi) \| R_3 \| T_4)$. It checks if $Auth_5 = Auth_5$?. If verification holds true, the user Ui is authenticated, and the process continues. Otherwise, the session is terminated.

Step 6: SR computes $SK = H(H(H(P) \| SIdi) \| R_2 \| R_3)$, $Auth6 = H(SK \| R_2 \| R_3)$. It verifies if $Auth_6 = Auth_6$?. The session key SK is confirmed if the condition is true. All messages are encrypted using the session key SK following mutual authentication. .Proposed authentication scheme is depicted in Figure 4.8.

4.2.4 Smartcard Revocation Phase

In this stage, the user recovers a smart card that has been lost, stolen, or for which they do not want to use the server's services.. The required steps are:

Step 1: User Ui enters Idi, password PWi and submits their biometric BOi at the sensor. Ui generates random nonce R_1 and calculates MBOi = H(R_1 || BOi), MUBi = H(Id_1 || BOi).

Step 2: SR verifies validity of the smartcard and calculates Gi = H(Idi || PWi || MUBi) ⊕ Idi. If stored $G_i = G_i$?, then SR asks the user to surrender his smartcard.

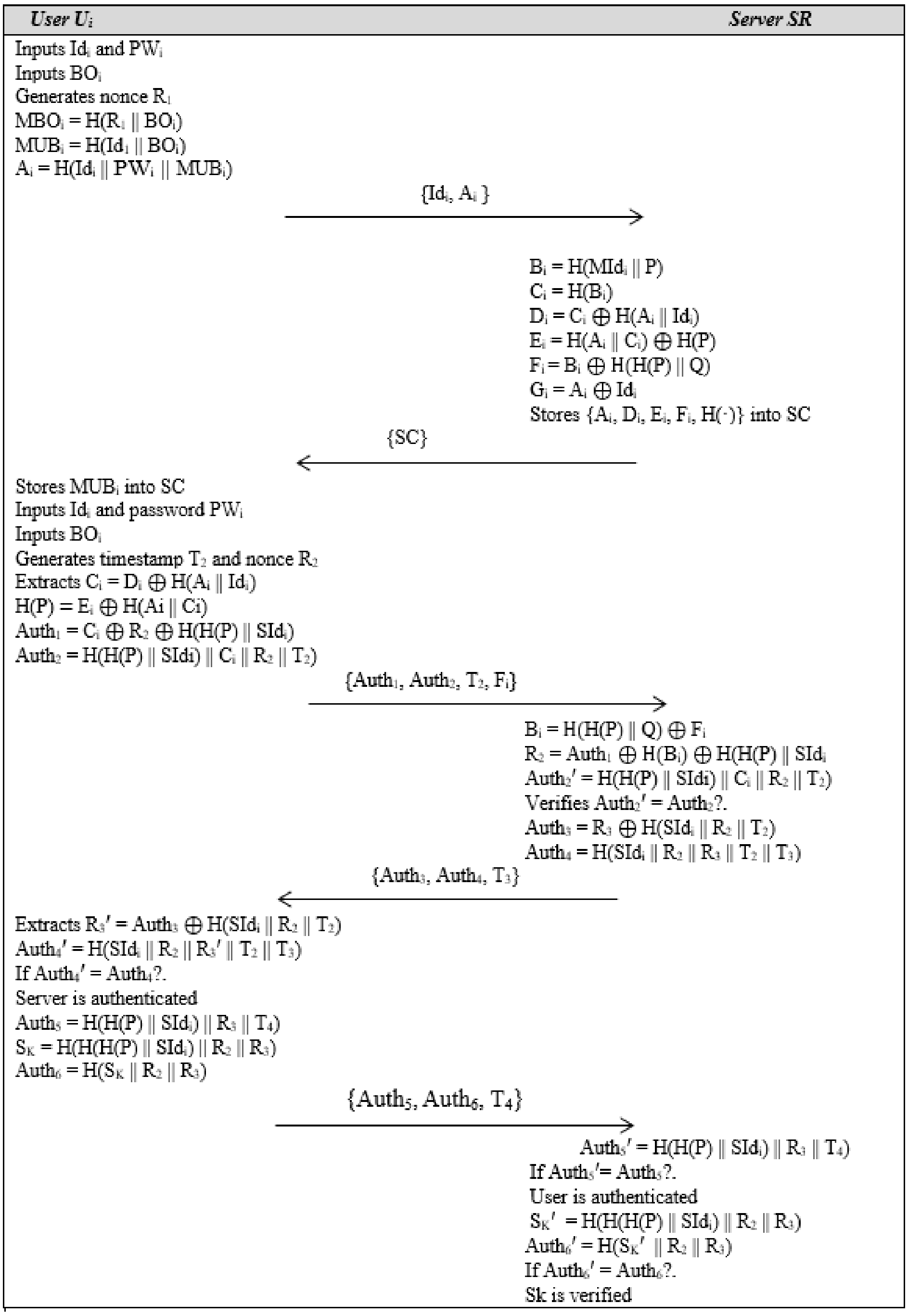


Figure 4.7. Authentication phase

4.3 COMPARATIVE PERFORMANCE OF PROPOSED MULTI-FACTOR USER AUTHENTICATION SCHEME

For performance analysis purposes, we evaluated the proposed approach and existing data security approaches in terms of computation cost. T_h and T_E indicate the cost required to compute hash and encryption, respectively. The suggested scheme is more effective than existing methods, as shown in Table 4.2 and 4.3.

Table 4.2: Cost Comparison of different phases

Schemes	Registration	Login	Authentication
Song [58]	$2T_h$	$1\ T_E + 2\ T_h$	$10\ T_h + 4\ T_E$
Wen & Li [54]	$5\ T_h$	$9\ T_h$	$22\ T_h$
Kumari et al. [56]	$4\ T_h$	$10\ T_h$	$16\ T_h$
Nikooghadam et al. [57]	$1\ T_E + 2\ T_h$	$1\ T_E + 2\ T_h$	$3\ T_E + 3\ T_D + 6\ T_h$
Chandrakar and Om, 2018	$5\ T_h$	$1\ T_E + 7\ T_h$	$3\ T_E + 16\ T_h$
Lwamo et al. [61]	$1\ T_E + 5\ T_h$	$1\ T_E + 6\ T_h$	$3\ T_E + 3\ T_D + 9\ T_h$
Sharma & Kalra [62]	$5\ T_h$	$3\ T_h$	$5\ T_E + 10\ T_h$
Proposed Data Security Approach	$7\ T_h$	$5\ T_h$	$12\ T_h$

Table 4.3 : Comparative performance with existing schemes

Schemes	Impersonation Attacks	Online password guessing attack	Insider attack	Server spoofing attack	Parallel session attack	User anonymity
Song [58]	No	Yes	No	Yes	No	No
Wen & Li [54]	Yes	No	Yes	No	No	Yes
Kumari et al. [56]	No	No	No	Yes	No	Yes

Schemes	Impersonation Attacks	Online password guessing attack	Insider attack	Server spoofing attack	Parallel session attack	User anonymity
Nikooghadam et al. [57]	No	No	Yes	Yes	No	No
Chandrakar and Om, 2018	No	No	No	No	No	Yes
Lwamo et al. [61]	No	No	Yes	Yes	No	No
Sharma & Kalra [62]	Yes	Yes	Yes	No	No	Yes
Proposed Data Security Approach	Yes	Yes	Yes	Yes	Yes	Yes

4.4 VALIDATION OF PROPOSED APPROACH USING AVISPA

For security analysis purposes, we adopted the suggested technique in AVISPA (Automated Validation of Internet Security Protocols and Applications). According to simulation results, the proposed method is protected against man-in-the-middle and replay attacks. [111]. Figures 4.8, 4.9, and 4.10 show the role of the user, server, environment, and OFMC output.

```
role user (Ui, SR : agent, % Ui is the user, SR is the server
          h : hash_func,
          SyKus : symmetric_key,
          SND, RCV : channel(dy))
played_by Ui
def=
local State : nat,
Idi, PWi, BOi, MBOi, MUBi, P,: text,
Ai, Bi,Ci, Di, Ei, Fi, Gi Auth1, Auth2, Auth3, Auth4, Auth5 : text,
R1, R2, R3, T1, T2, T3 Skey, AuthSkey : text
Mu: hash_func

const alice_bob_r2, alice_bob_t1, alice_bob_t3,
bob_alice_t2, bob_alice_r3,
subs1, subs2, subs3 : protocol_id

init State := 0
transition
1.  State = 0 /\ RCV(start) = | >
    State' := 1 /\ R1' := new()
                /\ MBOi' := h(R1'.BOi)
                /\ MUBi' := h(Idi'.BOi')
                /\ Ai' := h(Id'.PWi'.MUBi')
                /\ SND({Idi', Ai'}_SyKus)
                /\ secret({Id'}, sub1, Ui)
% receives smart card SC from the server securely

2. State = 1 /\ RCV({Di'.Ei'.Fi'. Mu(P'.Q').U'}_SyKus) =|>
% Login and authentication phase
  State' := 2 /\ secret({P'}, sub2, {SR})
             /\ Ci' := xor(Di'.h(Ai'.Idi')
             /\ h(P') := xor(Ei'.h(Ai'.Ci'))
             /\ R2' := new()
             /\ T2' := new()
             /\ Auth1' := xor(Ci'.R2'.h(h(P').SIdi'))
             /\ Auth2' := xor(h(h(P').SIdi').Ci'.R2'.T2')
             /\ SND(Auth1'.Auth2'.T2'.Fi')
             /\ witness(Ui, SR, alice_bob_r2, R2')
             /\ witness(Ui, SR, alice_bob_t1, T2')
% receive authentication message {Auth3, Auth4, T3} from server
3. State=2 /\ RCV{Auth3'. Auth4'.T3'}_SyKus = | >
   State' := 3 /\ T3' := new()
              /\ R3' := xor(Auth3'. h(Sidi'.R2'.T2'))
              /\ Auth4' := h(SIdi'.R2'. R3'.T2'. T3')
              /\ Auth5' := h(h(P).SIdi'.R3'. T4')
              /\ Sk' := h(h(h(P).SIdi').R3'. T4')
              /\ Auth6' := h(Sk'. R2'.R3')
              /\ SND(Auth5'. Auth6.T4')
              /\ witness(Ui, SR, alice_bob_t3, T3')
              /\ request(SR, Ui, bob_alice_t2, T2')
              /\ request(SR, Ui, bob_alice_r2, R2')
end role
```

Figure 4.8 : User role

```
role server (Ui, SR : agent, % Ui is the user, SR is the server
            h : hash_func,
            SyKus : symmetric_key,
            SND, RCV : channel(dy))
played_by SR
def=
local State : nat,
Idi, PWi, BOi, MBOi, MUBi, P,: text,
Ai, Bi,Ci, Di, Ei, Fi, Gi Auth1, Auth2, Auth3, Auth4, Auth5 : text,
R1, R2, R3, T1, T2, T3 Skey, AuthSkey : text
Mu: hash_func

const alice_bob_r2, alice_bob_t1, alice_bob_t3,
bob_alice_t2, bob_alice_r3,
subs1, subs2, subs3 : protocol_id

init State := 0
transition
% receive registration request message from the user
1. State = 0 /\ RCV(h(MID')) =|>
State' := 1 /\ P' := new()
              /\ Bi' := h(Midi'.P')
              /\ Ci' := h(Bi')
              /\ Di' := xor(Ci'.h(Ai', Id'))
              /\ Ei' := xor(h(Ai'.Ci').h(P))
              /\ Fi' := xor(Bi'.h(h(P').Q'))
              /\ Gi' := xor(Ai'.Idi')
              /\ SND({Di'.Ei'.Fi'. }_SyKus)
% sends smart card
              /\ secret({Idi'}, sub1, Ui)
              /\ secret({ P', Q'}, sub2, {SR})
% Login and authentication phase

2. State = 1 /\ RCV({Auth1', Auth2', T2'.Fi'}_SyKus) =|>
  State' := 2 /\ R2' := new()
              /\ R3' := new()
              /\ R2' := xor(Auth1', h(Bi').h(h(P')).Sid')
              /\ Auth3' := xor(R3'.h(Sidi'.R2'.T2'))
              /\ Auth4' := h(SId'.R2'.R3'.T2'.T3')
              /\ SND({Auth3'.Auth4'.T3'}_SyKus)
% send authentication response message to the user
              /\ witness(SR, Ui, bob_alice_t2, T2')
              /\ witness(SR, Ui, bob_alice_r3, R3')

3. State = 2 /\ RCV({AuthSkey.T3'}_SyKus =|>
   State' := 3 /\ request(Ui, SR, alice_bob_t1, T1')
              /\ request(Ui, SR, alice_bob_r2, R2')
              /\ request(Ui, SR, alice_bob_t3, T3)
end role
```

Figure 4.9 : Server role

```
role environment()
def=
const ui, sr: agent,
h, mu : hash_func,
sykus : symmetric_key
nidi, ti, ts : text,
alice_bob_ti, bob_alice_ts, alice_bob_alpha, bob_alice_beta,
subs1, subs2, subs3 : protocol_id
intruder_knowledge = { h, mu, midi, u, m, r1, auth1, auth2,
auth3, authskey, auth4, auth5, t2, t3 }
composition
        session(ui, sr, sykus, h)
        /\ session(i, sr, sykus, h)
        /\ session(ui, i, sykus, h)
end role

goal
   secrecy_of subs1
   secrecy_of subs2
   secrecy_of subs3
   authentication_on alice_bob_ti
   authentication_on alice_bob_alpha
   authentication_on bob_alice_ts
   authentication_on bob_alice_beta
end goal
environment()
```

Figure 4.10 : Role environment

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web−interface−computation/
./tempdir/workfilevOpMGm.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.21s
visitedNodes: 38 nodes
depth: 4 plies
```

Figure 4.11: The result of the analysis using OFMC of the proposed scheme

4.5 CONCLUSIONS

This chapter proposes a complete framework to secure data in cloud environment. The proposed framework works in two phases i.e. data encryption and user authentication. The data encryption approach encrypts data on the server side using BBBC based algorithm. The user authentication phase includes a multifactor mechanism for data security in the cloud environment. In this approach, we considered multiple factors instead of single-user authentication factors for cloud data security. The multiple factors we considered for the authentication mechanism are passwords, smart cards, and biometrics. The multiple factors for the user authentication scheme ensure more data security on the cloud. For comparison's sake, we contrast the suggested strategy with the other seven currently on the market. The performance findings demonstrate that the suggested user authentication system performs better than all current methods.

Chapter – 5

AN EFFICIENT TWO-FACTOR DATA SECURITY APPROACH FOR THE CLOUD ENVIRONMENT

An astonishingly large number of people are now using the internet because of the recent rapid advancements in wireless and mobile communication technology. Gaze upon the wondrous changes happening all around us, brought about by smart homes, smart cities, and so much more. The smart devices, all connected in the Internet of Things, generate loads of data, making it grow faster than ever before. This tremendous surge in data becomes the driving force behind what we call the Cloud paradigm. As defined by the National Institution of Standards and Technology, cloud computing is a model that lets you access computer resources like networks, servers, storage, applications, and services whenever and wherever you need them. It's like a magical shared pool of resources that can be quickly set up and taken down with little effort and interaction from those in charge. Think of it as a style of computing where super powerful IT capabilities are delivered as services to customers outside the system, all using Internet technology [112-114].

The significant features of the cloud, such as the minimum cost involved, highly elastic, ubiquitous access to services, scalability, and cheap data storage, have shifted the mass towards the cloud. Three varieties of the deployment paradigm are available: public, private, and hybrid. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the three service models for cloud computing.

Cloud computing facilitates services to users at a low cost. It efficiently offers users virtual computing services such as processing, software, hardware and storage. The data generated from smart devices is stored in the cloud. Users can retrieve their data at any time, anywhere across the globe. Shifting their data to the cloud offers advantages such as: a) permanent storage of their data; b) fast retrieval at any time and at any place; c) no need for actual purchasing of resources; d) minimal maintenance required for resources. This platform is not only suitable for organizations but also for individual users. They can easily access their data using smartphones, laptops, etc., sitting at any remote location.

The immense popularity of the cloud has created a profound marketplace for cloud providers. Cloud providers must consider the security aspect as it is of vital importance. The biggest threat to this paradigm is data security. Data security has emerged as a significant hindrance prohibiting users from shifting to the cloud as third parties store and manage the data. Cloud providers must ensure the security of servers. There must not be a leak of any secret user data stored on the servers. With the increasing computational power, attackers have become more computationally efficient and try different attacks to break through the servers to gain access to the stored data.

Cloud and IoT have become powerful paradigms to envision intelligent identification and management. IoT comprises several low-cost and low-power sensors. These sensors are in wireless communication with one another. They are used to monitor a particular area's environmental conditions using data gathered from sensor nodes. IoT applications are widely used in healthcare, intelligent transportation, and environmental monitoring. Three parties make up IoT networks: users, gateway nodes, and sensor nodes. To gather data and sense the area, sensor nodes are placed there. Open networks are used to transmit this detected data to the gateway node. The cloud stores this information for subsequent use. All businesses, sectors of the economy, and industries need this information.

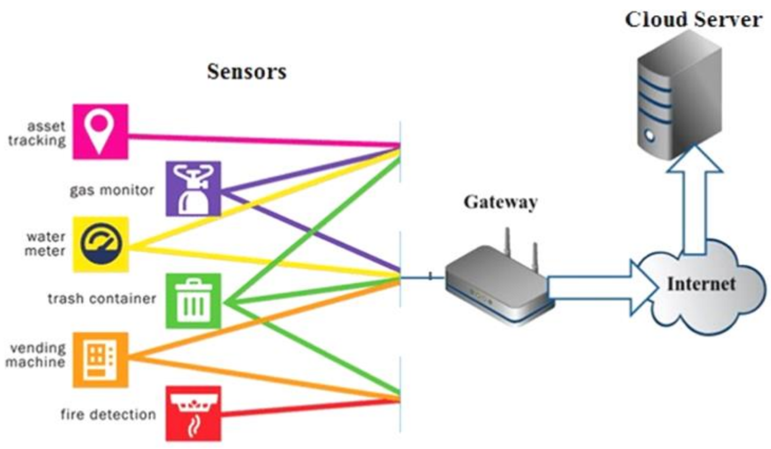


Figure 5.1. The basic framework of WSNs in Cloud-IoT applications

The basic framework for cloud IOT applications is shown in Figure 5.1. In this chapter, we'll explore a new framework for a Cloud environment. In this cloud environment all the sensor nodes and the gateway node are connected through the Internet. Cloud envrionment has many uses and is important in the Internet of Things (IoT). Here's the interesting part: In this setup, a user can access any sensor node that's part of the cloud through the gateway node. But, there's a challenge. Since communication happens in unreliable public places, intruders can sneak in and mess with the data. That's where user authentication comes in! It's a crucial factor in designing for such environments.

Moreover, the sensor nodes have some limitations. They don't have unlimited power or communication abilities [112-114]. So, the security mechanism we use for authenticating remote users must be lightweight and not too computationally heavy.

Several user authentication mechanisms have been proposed in the literature. Yeh et al. [115] presented an authentication protocol. The proposed protocol is based upon Elliptic Curve Cryptography (ECC). The results of the proposed approach show that it has high space complexity. Das et al. [116] and Xue et al. [117] discussed login credential-based and temporal authentication-based schemes for WSNs. Later, in two different papers, Xu and Wang [118] and Turkanovic and Hölbl [119] found that Xue et al. [117] failed to secure from forgery attacks. They proposed an efficient approach against the forgery attacks. Xue et al. [117] nullified the claims made by Li et al. [120]. They also found security issues in the discussed scheme. Turkanovic et al. [121] presented a novel authentication scheme for wireless ad-hoc WSNs. They presented a low computation approach that performs well on data security attacks. But Farash et al. [122], Ruhul and Biswas [123] found Turkanovic et al. [121]'s scheme is not perorming well on forgery attacks. Dolev et al. [123] evaluated the security performance of public key protocols and proposed a novel framework for analyzing their properties. The results of the proposed novel data security approach highlighted the significance of authentication to achieve secure communication.

Table 5.1 : Limitations in the Existing Literature

Existing schemes	Cryptanalysis By	Limitations
Das et al. [116]	Xu and Wang [118]	Forgery attack Impersonation attack
Xue et al. [117]	Turkanovic and Hölbl [119]	Forgery attack Information disclosure attack
Xue et al. [117]	Li et al. [120]	Weak authentication Prone to attacks
Turkanovic et al. [121]	Farash et al. [122]	Forgery attack Password guessing attack
	Ruhul and Biswas [123]	Offline guessing attack No user anonymity

Section 5.1 of this chapter proposes a secure user authentication approach. Section 5.2 shows the security analysis of the proposed scheme. Section 5.3 presents the results obtained on implementing the scheme using AVISPA. Section 5.4 concludes the chapter.

5.1 PROPOSED KEY AGREEMENT APPROACH

This section presents a secure remote user authentication approach for cloud environments. The phases of the proposed approach are as given below:

a) Pre-deployment phase

b) Registration phase

c) Authentication phase

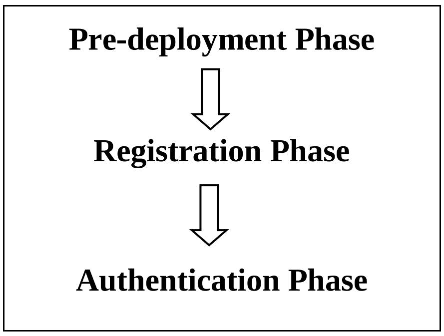


Figure 5.2. Workflow of the proposed scheme

The proposed approach consists of the remote user, gateway node, and sensor node, similar to an IoT network. These entities are represented as U_t, GW, and SN, respectively. Table 5.1 shows the notations of the proposed approach.

Table 5.2: Notations

Symbol	Meaning
U_t	t^{th} user
SN	Sensor node
GW	Gateway node
ID_t	Unique identity of user U_t
X	Secret parameter known only to SN
PS_t	Strong user password
SM	Smart card
R_1, R_2, R_3	Secret random nonces
SK_{SN}	Calculated session key by SN
SK_U	Calculated session key by U_t
$H(\cdot)$	Hash operation
$\|\|$	Concatenation operation
$\oplus$	XOR operation

5.1.1 Pre-deployment Phase

The proposed approach's pre-deployment phase facilitates the gateway and sensor nodes to establish secure connections.

Step 1: The GW nodes submit their identity IDGW, pseudo-identity MIDGW to SN through a secure channel.

Step 2: Further, SN calculates C1 = H(MIDGW || IDSN || X), C2 = H(IDGW || X) stores IDGW and transmits {C1, C2, IDSN} to GW.

Step 3: GW stores {C1, C2, IDSW, IDGW, IDSN}.

5.1.2 Registration Phase

This phase permits the user to register using his smart card. Without registration, no user can avail of the services.

Step 1: Ut selects their identity IDt, PSt. Ut generates random nonce R1 and computes masked identity MIDt = H(R1 || IDt), MPSt = H(R1 || PSt), and transmits {IDt, MIDt} to SN.

Step 2: SN verifies submitted IDt. If IDt is invalid, the process will be terminated. Else, SN computes A1 = H(MIDt || IDSN || X), A2 = H(IDt || X), stores IDt in its database, and communicates {M1, M2, IDSN} to Ut using a secure channel.

Step 3 : Ut calculates B1 = A1 ⊕ MPSt, B2 = A2 ⊕ H(IDt || MPSt), B3 = R1 ⊕ H(IDt || PSt) and stores {B1, B2, B3, MIDt, IDSN} in the smart card.

User		***SN***
Selects ID_t and PS_t		
Generates R_1		
Computes $MID_t = H(R_1 \| ID_t)$ $MPS_t = H(R_1 \| PS_t)$		
	$\{ID_t, MID_t\}$ →	
		Verifies IDt is unallocated Computes $A_1 = H(MID_t \| ID_{SN} \| X)$ $A_2 = H(ID_t \| X)$ Stores IDt in database
	← $\{M_1, M_2, ID_{SN}\}$	
(via a secure channel)		
$B_1 = A_1 \oplus MPS_t$ $B_2 = A_2 \oplus H(ID_t \| MPS_t)$ $B_3 = R_1 \oplus H(ID_t \| PS_t)$ SC stores $\{B_1, B_2, B_3, MID_t, ID_{SN}\}$ in SC		

Figure 5.3 : Registration phase

5.1.3 Authentication Phase

Step 1 : When Ut wish to access the services, Ut inserts smart card and enters {IDt, PSt}. Ut generates a random R2 and fresh pseudo-identity MIDtnew, calculates Dt = B3 ⊕ H(IDt ‖ PSt), MPSt = H(PSt ‖ Dt), A1= B1 ⊕ MPSt, A2 = B2 ⊕ H(IDt ‖ MPSt), E1 = A1 ⊕ R2, E2 = H(R2 ‖ MIDt ‖ IDSN) ⊕ IDt, E3 = A2 ⊕ H(IDt ‖ MPSt) ⊕ MIDtnew ⊕ H(R2 ‖ IDt), E4 = H(IDt ‖ MIDt ‖ MIDtnew ‖ R2 ‖ E3). Ut transmits {MIDt, E1, E2, E3, E4} to SN.

Step 2 : GW chooses fresh MIDGWnew, random nonce R3, calculates E5 = C1 ⊕ R3, E6 = H(R3 ‖ IDGW ‖ IDSN) ⊕ IDGW, E7 = C2 ⊕ MIDGWnew ⊕ H(R3 ‖ IDGW), E8 = H(MIDGW ‖ IDGW ‖ MIDGWnew ‖ R3 ‖ E7). GW transmits {MIDt, E1, E2, E3, E4, IDGW, E6, E7, E8} to SN.

Step 3 : SN calculates R2 = E1 ⊕ H(MIDt ‖ IDSN ‖ X), IDt = E2 ⊕ H(R2 ‖ MIDt ‖ IDSN), MIDtnew = E3 ⊕ H(Idt ‖ X) ⊕ H(R2 ‖ IDt). It checks IDt and E4 = H(IDt ‖ MIDt ‖ MIDtnew ‖ R2 ‖ E3)?. If true, R3 = E5 ⊕ H(IDGW ‖ IDSN ‖ X), IDGW = E6 ⊕ H(R3 ‖ IDGW ‖ IDSN), IDGWnew = E7 ⊕ H(IDGW ‖ X) ⊕ H(R3 ‖ IDGW), verifies IDGW and E8 = H(IDGW ‖ IDGW ‖ IDGWnew ‖ R3 ‖ E7)?. If it fails, session is terminated.

Step 4: Else, SN generates random RSN to calculate SKSN = H(R2 ⊕ R3 ⊕ RSN), E9 = H(IDGWnew ‖ IDSN ‖ X) ⊕ H(R3 ‖ IDGWnew), E10 = H(IDGWnew ‖ R3 ‖ IDGW) ⊕ H(R2 ‖ RSN), E11 = H(SKSN ‖ E9 ‖ E10 ‖ H(IDGW ‖ X)), E12 = H(MIDtnew ‖ IDSN ‖ X) ⊕ H(R2 ‖ MIDtnew), E13 = H(MIDtnew ‖ R2 ‖ MIDt) ⊕ (R3 ⊕ RSN), E14 = H(SKSN ‖ E12 ‖ E13 ‖ H(IDt ‖ X)) and transmits {E9, E10, E11, E12, E13, E14} to GW.

Step 5: GW calculates (R2 ⊕ RSN) = E10 ⊕ H(IDGWnew ‖ R3 ‖ IDGW), SKGW = H(R3 ⊕ R2 ⊕ RSN), verifies E11 = H(SKGW ‖ E9 ‖ E10 ‖ C2)?. If true, GW computes C1new = E9 ⊕ H(R3 ‖ IDGWnew) and replaces C1 with C1new and IDGW with IDGWnew. Further, sends {E12, E13, E14} to Ut.

Step 6 : SM calculates (R3 ⊕ RSN) = E13 ⊕ H(MIDtnew || R2 || MIDt), SKU = H(R2 ⊕ RGW ⊕ RSN). It validates E14 = H(SKU || E12 || E13 || A2)?. If true, SM proceeds B1new = E12 ⊕ H(R2 || MIDtnew) ⊕ MPSt. It replaces B1 with B1new and MIDt with MIDtnew.

U_t	***GW***	***SN***
Inputs ID_t and PS_t Generates random R_2 $D_t = B_3 \oplus H(ID_t \parallel PS_t)$ $MPS_t = H(PS_t \parallel D_t)$ $A_1 = B_1 \oplus MPS_t$ $A_2 = B_2 \oplus H(ID_t \parallel MPS_t)$ $E_1 = A_1 \oplus R_2$ $E_2 = H(R_2 \parallel MID_t \parallel ID_{SN}) \oplus ID_t$ $E_3 = A_2 \oplus H(ID_t \parallel MPS_t) \oplus MID_{tnew} \oplus H(R_2 \parallel ID_t)$ $E_4 = H(ID_t \parallel MID_t \parallel MID_{tnew} \parallel R_2 \parallel E_3)$ $V_3 = H(V_1 \parallel V_2 \parallel Ni \parallel T_1)$		
$\{MID_t, E_1, E_2, E_3, E_4\}$ →		
	Chooses a random nonce R_3 $E_5 = C_1 \oplus R_3$ $E_6 = H(R_3 \parallel ID_{GW} \parallel ID_{SN}) \oplus ID_{GW}$ $E_7 = C_2 \oplus MID_{GWnew} \oplus H(R_3 \parallel ID_{GW})$ $E_8 = H(MID_{GW} \parallel ID_{GW} \parallel MID_{GWnew} \parallel R_3 \parallel E_7)$	
	$\{MID_t, E_1, E_2, E_3, E_4, ID_{GW}, E_6, E_7, E_8\}$ →	
		$R_2 = E_1 \oplus H(MID_t \parallel ID_{SN} \parallel X)$ $ID_t = E_2 \oplus H(R_2 \parallel MID_t \parallel ID_{SN})$

$MID_{tnew} = E_3 \oplus H(Id_t \| X) \oplus H(R_2 \| ID_t)$

$R_3 = E_5 \oplus H(ID_{GW} \| ID_{SN} \| X)$

$ID_{GW} = E_6 \oplus H(R_3 \| ID_{GW} \| ID_{SN})$

$ID_{GWnew} = E_7 \oplus H(ID_{GW} \| X) \oplus H(R_3 \| ID_{GW})$

$SK_{SN} = H(R_2 \oplus R_3 \oplus R_{SN})$

$E_9 = H(ID_{GWnew} \| ID_{SN} \| X) \oplus H(R_3 \| ID_{GWnew})$

$E_{10} = H(ID_{GWnew} \| R_3 \| ID_{GW}) \oplus H(R_2 \| R_{SN})$

$E_{11} = H(SK_{SN} \| E_9 \| E_{10} \| H(ID_{GW} \| X))$

$E_{12} = H(MID_{tnew} \| ID_{SN} \| X) \oplus H(R_2 \| MID_{tnew})$

$E_{13} = H(MID_{tnew} \| R_2 \| MID_t) \oplus (R_3 \oplus R_{SN})$

$E_{14} = H(SK_{SN} \| E_{12} \| E_{13} \| H(ID_t \| X))$

$\{E_9, E_{10}, E_{11}, E_{12}, E_{13}, E_{14}\}$ ←

$E_{10} \oplus H(ID_{GWnew} \| R_3 \| ID_{GW})$

$SK_{GW} = H(R_3 \oplus R_2 \oplus R_{SN})$

$C_{1new} = E_9 \oplus H(R_3 \| ID_{GWnew})$

Replaces C_1 with C_{1new}

$\{E_{12}, E_{13}, E_{14}\}$ ←

$E_{13} \oplus H(MID_{tnew} \| R_2 \| MID_t)$

$SK_U = H(R_2 \oplus R_{GW} \oplus R_{SN})$

Validates $E_{14} = H(SK_U \| E_{12} \| E_{13} \| A_2)$

$B_{1new} = E_{12} \oplus H(R_2 \| MID_{tnew}) \oplus MPS_t$

Replaces B_1 with B_{1new} and MID_t with MID_{tnew}

Figure 5.4 : Authentication phase

5.2 SECURITY ANALYSIS

The security comparison with the related schemes shows that our scheme achieves all security attributes and is resistant to attacks. Table 5. 2 shows the comparison of security features.

Table 5.3. Security feature comparison

Features	**Yeh et al. [115]**	**Das et al. [116]**	**Xue et al. [117]**	**Turkanovic et al. [121]**	**Farash et al. [122]**	**Proposed scheme**
Replay attack	Yes	No	No	Yes	Yes	Yes
Privileged insider attack	No	No	No	No	Yes	Yes
Password guessing attack	No	No	No	No	No	Yes
Server **impersonation** attack	No	No	No	No	No	Yes
Hidden server attack	No	No	No	No	No	Yes
Resists user anonymity	No	No	No	No	Yes	Yes
Impersonation attack	No	No	No	No	No	Yes
Mutual authentication	Yes	No	Yes	Yes	Yes	Yes
Forward secrecy	No	Yes	Yes	Yes	Yes	Yes

5.3 EXPERIMENTAL RESULTS

We employed the Automated Validation of Internet Security Protocols and Applications (AVISPA) for simulation and performance analysis. It is frequently used to check the integrity of security protocols. HLPSL (High-Level Protocol Specification Language) is used by AVISPA to verify the robustness of protocols. The architecture of AVISPA is shown in Figure 5.4. For our proposed scheme, it has been simulated on OFMC (On-the-fly Model-Checker). The results obtained are shown in Figure 5.5.

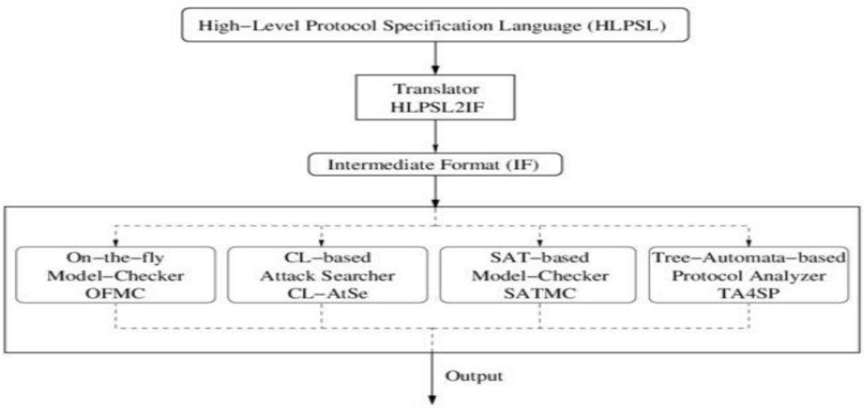


Figure 5.5 : AVISPA Architecture

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web−interface−computation/
./tempdir/workfilevOpMGm.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.31s
visitedNodes: 179 nodes
depth: 11 plies
```

Figure 5.6 : Simulation results on OFMC

5.4 CONCLUSIONS

This chapter presents a secure two-factor user authentication scheme for data security on the cloud. The proposed scheme is lightweight. This approach uses a hash function. Thus, it is suitable for practical applications. The proposed scheme is robust and efficient. The scheme has been formally verified by a simulation tool. The proposed scheme can be integrated with BBBC-based data encryption and decryption module to provide a complete data security framework. We observed that the proposed scheme outperforms existing data security schemes from comparison results. It has low computation cost due to two factors for user authentication on the cloud.

Chapter – 6

CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSIONS

In this chapter, we conclude our research work along with the future scope of this work. In this thesis, We suggested an approach to protect the data in the cloud setting. The proposed framework consists of two phases. Phase 1 of the proposed framework encrypts and decrypts the data. We proposed Big Bang – Big Crunch Based data encryption approach for data encryption. We compared the performance of the proposed data encryption approach with the existing Genetic Algorithm-based 2D Chaotic Approach. From the performance results, we observed that the proposed approach outperformed the existing approach. Phase 2 of the proposed framework is used to secure data in the cloud environment. For phase 2 of the framework, we proposed two data security schemes. Scheme 1 is the multifactor-based data security scheme, and scheme 2 is the light-weighted data security scheme for the cloud. We can integrate any one scheme with the proposed BBBC-based data encryption approach for our proposed data security framework. We observed From performance results that the proposed schemes were performing well compared to existing approaches.

Chapter 1 Presents the motivation behind the research work. This chapter discusses data security issues and different classical approaches to data encryption. The problem formulation and objectives are presented in this chapter.

Chapter 2 presents an up-to-date review of relevant literature. The literature review is organized into two parts. Part 1 of this chapter presents different data encryption approaches available in the literature. Part 2 of this chapter discusses different data security approaches for cloud environments.

Chapter 3 Proposes an integrated BBBC and 2D Chaotic map approach for data encryption. In this chapter, we optimized the chaotic map's initial parameters with the BBBC algorithm. In the proposed approach, BBBC algorithm produces the complex and unpredictable key. We compared the Performance of the proposed approach with the existing 2D chaotic map and genetic algorithm approach. For comparison purposes, we tested it on different character-sized text. We observed from the results that the proposed approach outperformed the existing one on all-sized text.

Chapter 4 Proposes a multifactor data security approach for a cloud environment. In this approach, we considered multiple factors instead of single user authentication factors for cloud data security. The multiple factors we considered for the authentication mechanism are passwords, smart cards, and biometrics. The multiple factors for the user authentication scheme ensure more data security on the cloud. We compare the proposed approach with the existing 7 available approaches for comparison purposes. From performance results, we observe that the proposed user authentication scheme outperforms all existing approaches.

Chapter 5 Proposes a secure two-factor user authentication scheme for data security on the cloud. The proposed scheme is lightweight as it uses a hash function, thus, suitable for practical applications. The proposed scheme is robust and efficient. The scheme has been formally verified by a simulation tool. The comparison shows that the proposed scheme outperforms existing schemes than existing schemes. It has low computation cost due to two factors for user authentication on the cloud.

6.2 FUTURE SCOPE

This thesis presented a complete framework to secure the data from unauthorized users. The proposed framework works in two phases. In the first phase, it secures the server from unauthorized users using a hashing-based approach. The first phase limits unauthorized users from illegally access to the data. It is almost impossible to bypass server security using this proposed approach. In the second phase, We encrypted our data using an integrated BBBC algorithm and 2D chaotic maps approach. In data encryption, we transform the data into a complex and secure format that can only be read by that person with decryption key. The integrated Big Bang Big Crunch (BBBC) algorithm and 2D chaotic maps approach can provide more security to data, restricting unauthorized users from accessing the data even if they can bypass the security provided on the server side. In this thesis, the proposed approach was tested on simple text data. In the future, we can test the performance of the proposed approach on different types of data like images, voices, and datasets. Further, new nature-inspired computing-based parallel processing search & optimization approaches can be proposed to optimize the parameters of existing encryption approaches efficiently.

REFERENCES

[1] Shaikh, Rizwana, and M. Sasikumar, "Data classification for achieving security in cloud computing", Procedia computer science 45 (2015), pp. 493-498.

[2] Sana, M. U., Li, Z., Javaid, F., Liaqat, H. B., & Ali, M. U., (2021), "Enhanced Security in Cloud Computing Using Neural Network and Encryption", IEEE Access, 9, pp. 145785-145799.

[3] Ruiter, J., & Warnier, M., (2011), "Privacy regulations for cloud computing: Compliance and implementation in theory and practice", Computers, privacy and data protection: an element of choice (pp. 361-376), Dordrecht, Springer Netherlands.

[4] Arora, R., Parashar, A., & Transforming, C. C. I., (2013), "Secure user data in cloud computing using encryption algorithms", International journal of engineering research and applications, 3(4), pp. 1922-1926.

[5] Kim, M., Mohindra, A., Muthusamy, V., Ranchal, R., Salapura, V., Slominski, A., & Khalaf, R., (2016), "Building scalable, secure, multi-tenant cloud services on IBM Bluemix", IBM Journal of Research and Development, 60(2-3), pp. 8-1.

[6] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[7] "Trust Your Data With Security, Privacy", IBM https://www.ibm.com/cloud/security [Accessed: 25-Jan-2019].

[8] Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and access management as security-as-a-service from clouds. Procedia Computer Science, 79, 170-174.

[9] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing", 5th International Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, 2010.

[10] Rao, R. V., & Selvamani, K., Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48, 2015, pp. 204-209.

[11] D. Bruneo, “CloudWave: Where adaptive cloud management meets DevOps”, 2014, IEEE Symposium on Computers and Communications (ISCC), pp. 1-6, 2014.

[12] F. Benedetti, A. D. Cocco, C. Marinelli, and L. Pichetti, “Cloud-Wave: Where adaptive cloud management meets DevOps”, 2014 IEEE Symposium on Computers and Communications (ISCC), pp.1-6, 2014.

[13] G. Da Cunha Rodrigues, “Monitoring of Cloud Computing Environments: Concepts, Solutions, Trends, and Future Directions”, Proceedings of the 31st Annual ACM Symposium on Applied Computing, pp. 378-383, 2016.

[14] Z. Chen, and J. Yoon, “CloudWave: Where adaptive cloud management meets DevOps”, 2014 IEEE Symposium on Computers and Communications (ISCC), pp. 1-6, 2010.

[15] “(ISC)2® and Cloud Security Alliance”, Cloud Security Alliance.[Online]. Available, https://cloudsecurityalliance.org/articles/isc2-and-cloud-ecurityalliance-introduce-new-cloud-security-certification/ [Accessed: 25-Jan-2019].

[16] Sharma, G., & Kalra, S. (2019). “A lightweight user authentication scheme for cloud-IoT based healthcare services”, *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *43*, 619-636.

[17] Mell P, Grance T (2018) SP 800-145, “The NIST Definition of cloud computing”, CSRC (online) Csrc.nist.gov, https://csrc.nist.gov/publications/detail/sp/800-145/fnal.

[18] Heiser J., “What you need to know about cloud computing security and compliance”, Gartner, Research, ID Number: G00168345, 2009.

[19] Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA (2017), “Optimal virtual network function placement in multi-cloud service function chaining architecture”, Comput Commun 102:1–16

[20] Yu S, Wang C, Ren K, Lou W (Mar 2010) “Achieving secure, scalable, and fine-grained data access control in cloud computing”, In: Proceedings of the IEEE INFOCOM

[21] Akshaya MS, Padmavathi G (2019), “Taxonomy of security attacks and risk assessment of cloud computing”, In: Peter J, Alavi A, Javadi B (eds) Advances in big data and cloud computing. Advances in intelligent systems and computing, vol 750. Springer, Singapore

[22] Subramanian N, Jeyaraj AJC, Engineering E (2018), “Recent security challenges in cloud computing”, Comput Electr Eng 71:28–42

[23] Bernard Golden. “Defining private clouds”, 2009 /http://www.cio.com/ article/ 492695/Defining_Private_Clouds_Part_OneS

[24] Singh, S., & Sharma, A., “Cryptosystems in Asymmetric Cryptography for Securing Data at various Levels”, 2020, *Delving*.

[25] Sharma, E. R., & Singh, S. (2019, April), “Reforming Cyber Security with Coding”, In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, pp. 1-6, IEEE.

[26] Sharma, A., Jha, P., & Singh, S. (2021), “Data Control in Public Cloud Computing: Issues and Challenges”, *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, *14*(2), 564-579.

[27] Li, H., & Zhang, Y. (2021), “Research on Data Security Technology in Cloud Computing Environment”, Journal of Physics: Conference Series, 1825(1), 012044. doi: 10.1088/1742-6596/1825/1/012044

[28] Matta, P., Arora, M., & Sharma, D., “A comparative survey on data encryption Techniques: Big data perspective”, Materials today: proceedings, 46, 2021, pp. 11035-11039.

[29] Kumar, Sunil, et al. “Applying The Modular Encryption Standard To Mobile Cloud Computing To Improve The Safety Of Health Data”, Journal of Pharmaceutical Negative Results, 2022, pp. 1911-1917.

[30] Siva Kumar, D. V. N., & Santhi Thilagam, P., “Searchable encryption approaches: attacks and challenges”, Knowledge and Information Systems, 2019, vol. 61, pp. 1179-1207..

[31] Morales-Sandoval, M., Cabello, M. H., Marin-Castro, H. M., & Compean, J. L. G. (2020), “Attribute-based encryption approach for storage, sharing and retrieval of encrypted data in the cloud”, IEEE Access, 8, 170101-170116.

[32] Gai, K., Qiu, M., & Zhao, H. (2017), “Privacy-preserving data encryption strategy for big data in mobile cloud computing”, IEEE Transactions on Big Data, 7(4), pp. 678-688.

[33] Chen, W., Chen, G., Zhao, Y., & Zhang, J., “Security vulnerability and encryption technology of computer information technology data under big data environment”, Journal of Physics: Conference Series , Vol. 1800, No. 1, 2021, pp. 012012, IOP Publishing.

[34] Reddy, N. C. S., Madhuravani, B., & Sneha, D. P., “An approach for efficient and secure data encryption scheme for spatial data”. SN Computer Science, 1(3), 2020, pp. 117

[35] Pooja Verma et. al., “Multi Encryption Approach for Privacy Preserving Authentication over VANETs.”, Journal of Emerging Technologies and Innovative Research, 7(9), 2020, pp. 189-194.

[36] Aljawarneh, S., Yassein, M. B., & Talafha, W. A. A., “A multithreaded programming approach for multimedia big data: encryption system”, Multimedia Tools and Applications, 77, 2018, pp. 10997-11016.

[37] M. Sri Lakshmi et. al. (Year). “A Hybrid Approach with Watermark Encryption for Digital Data Protection.”, International Journal of Research 5(4), 2018, pp. 1851-1854

[38] Priya Matta, Minit Arora, Deepika Sharma (2021). “A comparative survey on data encryption Techniques: Big data perspective.” Journal Name, Volume(Issue), Page numbers.

[39] Dr. B. Sunil Kumar, J. Jayalakshmi, V. Muniraj Naidu (2018). “Execution of data encryption strategy in mobile cloud computing.”, Journal of Emerging Technologies and Innovative Research, 5(7), pp. 1315-1319

[40] Siva Kumar, D. V. N., & Santhi Thilagam, P., “Searchable encryption approaches: attacks and challenges”, Knowledge and Information Systems, 2019, vol. 61, pp. 1179-1207.

[41] Miguel Morales-Sandoval, Melissa Hinojosa Cabello, Heidy M. Marin-Castro, José Luis González Compeán (2020). “Attribute-Based Encryption Approach for Storage, Sharing, and Retrieval of Encrypted Data in the Cloud.” Journal Name, Volume (Issue), Page numbers.

[42] Keke Gai, Meikang Qiu, Hui Zhao (2021). “Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing.” Journal Name, Volume (Issue), Page numbers.

[43] Chen Weijie, Guodong Chen, Yanheng Zhao, Jinghua Zhang (2021). “Security vulnerability and encryption technology of computer information technology data under big data environment.” Journal Name, Volume (Issue), Page numbers.

[44] N. Chandra Sekhar Reddy, B. Madhuravani, D. P. Sneha (2020). “An Approach for Efficient and Secure Data Encryption Scheme for Spatial Data.” Journal Name, Volume (Issue), Page numbers.

[45] Pooja Verma, Rohit Rathore (2020). “Multi Encryption Approach for Privacy Preserving Authentication over VANETs.” Journal Name, Volume(Issue), Page numbers.

[46] Shadi Aljawarneh, Muneer Bani Yassein, We'am Adel Talafha (2018). “A multithreaded programming approach for multimedia big data: encryption system.” Journal Name, Volume (Issue), Page numbers.

[47] M. Sri Lakshmi, Vallamkonda Sai Manogna, Ediga Usha Rani (2018). “A Hybrid Approach with Watermark Encryption for Digital Data Protection”, Journal Name, Volume (Issue), Page numbers.

[48] Author(s) (Year). "Efficient Time-Oriented Latency-Based Secure Data Encryption for Cloud Storage", Journal Name, Volume (Issue), Page numbers.

[49] Wang YY, Liu JY, Xiao FX, Dan J. , "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer communications. 2009 Mar 4;32(4):583-5.

[50] Chen, D., & Zhao, H. (2012, March), "Data security and privacy protection issues in cloud computing", In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.

[51] Liu, X., Zhang, Y., Wang, B., & Yan, J. (2012), "Mona: Secure multi-owner data sharing for dynamic groups in the Cloud", *IEEE transactions on parallel and distributed systems*, *24*(6), 1182-1191.

[52] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014), "Security and privacy for storage and computation in cloud computing. *Information sciences"*, *258*, 371-386.

[53] Dong, X., Yu, J., Zhu, Y., Chen, Y., Luo, Y., & Li, M. (2015), "SECO: Secure and scalable data collaboration services in cloud computing", *computers & security*, *50*, 91-105.

[54] Wen F, Li X., "An improved dynamic ID-based remote user authentication with key agreement scheme", Computers & Electrical Engineering. 2012 Mar 1;38(2):381-7.

[55] Chang YF, Tai WL, Chang HC, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update" International Journal of Communication Systems. 2014 Nov;27(11):3430-40.

[56] Kumari S, Khan MK, Li X., "An improved remote user authentication scheme with key agreement", Computers & Electrical Engineering. 2014 Aug 1;40(6):1997-2012.

[57] Nikooghadam M, Jahantigh R, Arshad H., "A lightweight authentication and key agreement protocol preserving user anonymity", Multimedia Tools and Applications. 2017 Jun 1;76(11):13401-23.

[58] Song R (2010), "Advanced smart card-based password authentication protocol", Computer Standards & Interfaces 32(5):321-5.

[59] Xu J, Zhu WT, Feng DG (2009), "An improved smart card based password authentication scheme with provable security", Comput Stand Interfaces 31(4):723-8.

[60] Chen BL, Kuo WC, Wuu LC (2014), "Robust smart-card-based remote user password authentication scheme", International Journal of Communication Systems 27(2):377-89.

[61] Lwamo NM, Zhu L, Xu C, Sharif K, Liu X, Zhang C., "SUAA: A secure user authentication scheme with anonymity for the single & multi-server environments", Information Sciences. 2019 Mar 1;477:369-85.

[62] Sharma, G., & Kalra, S. (2021), "A robust multi-factor remote user authentication scheme for cloud-IoT services", *International Journal of Information and Computer Security*, *16*(3-4), 272-291.

[63] Odelu V, Das AK, Goswami A (2014), "A secure effective key management scheme for dynamic access control in a large leaf class hierarchy", Information Sciences 269:270-85.

[64] Yao, Y., Zhang, L., Yi, J., Peng, Y., Hu, W., & Shi, L. (2016, September), "A framework for big data security analysis and semantic technology", In *2016 6th International Conference on IT Convergence and Security (ICITCS)* (pp. 1-4). IEEE.

[65] Aldossary, S., & Allen, W. (2016), "Data security, privacy, availability, and integrity in cloud computing: issues and current solutions", *International Journal of Advanced Computer Science and Applications*, *7*(4), 485-498.

[66] Lin, J., & Liu, L. (2019, July), "Research on security detection and data analysis for the industrial internet", In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 466-470). IEEE.

[67] Sun, P. J. (2019), "Privacy protection and data security in cloud computing: a survey, challenges, and solutions", *IEEE Access*, *7*, 147420-147452.

[68] Yadav, D., Shinde, A., Nair, A., Patil, Y., & Kanchan, S. (2020, May). "Enhancing data security in Cloud using Blockchain", In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 753-757). IEEE.

[69] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. (2021), "CryptoGA: a cryptosystem based on genetic algorithm".

[70] "Virtualization and the Software-Defined Data Center", VMwareIN Virtualization and the Software-Defined Data Center, VMwareIN, VMWare. [Online]. Available", https://www.vmware.com/ solutions/ software-defined-datacenter/in-depth.html [Accessed: 25-Jan- 2019].

[71] "What is Software Defined Datacenter(SDDC)? - VMWare Insight. [Online]. Available", http://vmwareinsight.com/Articles/2017/9/5800931/What-is-Software-Defined-Datacenter-SDDC [Accessed: 25-Jan-2019].

[72] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing", p. 7. [http://dx.doi.org/10.6028/NIST.SP.800-145]

[73] L. Columbus, "Cloud Computing Market Projected To Reach $411B By 2020", Forbes.[Online].Available,https://www.forbes.com/sites/louiscolumbus/2017/10/18/cloudcomputing-market-projected-to-reach-411b-by-2020/ [Accessed: 25-Jan-2019].

[74] M. Ali, S.U. Khan, and A.V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Inf. Sci., vol. 305, pp. 357-383, 2015. [http://dx.doi.org/10.1016/j.ins.2015.01.025]

[75] "Economic Impact of Cybercrime." [Online]. Available", https://www.csis.org/analysis/economic-impact-cybercrime [Accessed:25-Jan-2019].

[76] "Gartner Predicts a Record Year for Security Spending in 2018", Protegrity, p. 08-Dec-2017.

[77] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-ofthe-art and research challenges", J. Internet Serv. Appl., vol. 1, no.1, pp. 7-18, 2010. [http://dx.doi.org/10.1007/s13174-010-0007-6]

[78] D. Puthal, B.P.S. Sahoo, S. Mishra, and S. Swain, "Cloud Computing Features, Issues, and Challenges: A Big Picture", 2015 International Conference on Computational Intelligence and Networks, pp. 116-123, 2015. [http://dx.doi.org/10.1109/CINE.2015.31]

[79] Gup8ta, S., & Chaudhary, A. (2021). "Data Security in Cloud Computing: A Comprehensive Review", IEEE Access, 9, 18165-18189. doi: 10.1109/access.2021.3053062

[80] Alqahtani, S. M., & Alqahtani, M. A. (2021), "A Review of Data Security and Privacy in Cloud Computing", Journal of Information Security, 12(1), 1-17. doi: 10.4236/jis.2021.121001

[81] Li, H., & Zhang, Y. (2021), "Research on Data Security Technology in Cloud Computing Environment", Journal of Physics: Conference Series, 1825(1), 012044. doi: 10.1088/1742-6596/1825/1/012044

[82] Kumar, S., & Singh, V. K. (2021), "Data Security Challenges in Cloud Computing: A Review", International Journal of Computer Science and Information Security, 19(2), 1-9.

[83] Li, W., Li, Y., & Chen, J. (2021), "A Survey of Data Security and Privacy Protection in Cloud Computing", Journal of Physics: Conference Series, 1768(1), 012021. doi: 10.1088/1742-6596/1768/1/012021

[84] Alharbi, A., Alshammari, F., & Alqahtani, M. (2020), “A Review of Data Security Techniques in Cloud Computing Environments”, Journal of King Saud University - Computer and Information Sciences, 32(11), 1303-1312. doi: 10.1016/j.jksuci.2020.07.007

[85] Zhang, X., Wang, H., & Wu, Y. (2020), “A Review of Data Security and Privacy Protection in Cloud Computing Environment”, Journal of Physics: Conference Series, 1667(1), 012015. doi: 10.1088/1742-6596/1667/1/012015

[86] Kumar, S., & Singh, V. K. (2020), “A Review of Data Security Techniques in Cloud Computing Environment”, International Journal of Advanced Research in Computer Science and Software Engineering, 10(9), 104-109.

[87] Alshahrani, M., & Alshehri, S. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”. Journal of Information Security and Applications, 62, 102890. doi: 10.1016/j.jisa.2021.102890

[88] Singh, N., & Singh, S. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Comprehensive Review”, Journal of Ambient Intelligence and Humanized Computing, 12(5), 5101-5121. doi: 10.1007/s12652-021-03203-6

[89] Raza, S., & Khan, M. K. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Ambient Intelligence and Humanized Computing, 12(4), 4229-4247. doi: 10.1007/s12652-021-03171-x

[90] Li, Y., & Zhang, Y. (2020), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Ambient Intelligence and Humanized Computing, 11(9), 3979-3998. doi: 10.1007/s12652-020-02540-3

[91] Alharbi, A., Alshammari, F., & Alqahtani, M. (2020), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A

Review”, Journal of King Saud University - Computer and Information Sciences, 32(11), 1293-1302. doi: 10.1016/j.jksuci.2020.07.006

[92] Alghamdi, R., & Alghamdi, M. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Cybersecurity, 7(1), tyaa038. doi: 10.1093/cybsec/tyaa038

[93] Zhang, Y., & Li, Y. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Cybersecurity, 7(1), tyaa046. doi: 10.1093/cybsec/tyaa046

[94] Zhang, Y., & Li, Y. (2020), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Ambient Intelligence and Humanized Computing, 11(11), 4899-4919. doi: 10.1007/s12652-020-02649-6

[95] Alqahtani, M. A., & Alqahtani, S. M. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Comprehensive Review”, Journal of Information Security and Applications, 63, 102943. doi: 10.1016/j.jisa.2021.102943

[96] Liu, X., & Chen, H. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Cybersecurity, 7(1), tyab016. doi: 10.1093/cybsec/tyab016

[97] Khan, M. K., & Raza, S. (2021)” Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of Cybersecurity, 7(1), tyaa040. doi: 10.1093/cybsec/tyaa040

[98] Alshahrani, M., & Alshehri, S. (2020). “Improving cloud computing data security Using Integrated Cryptographic Transformations: A Review”, Journal of King Saud University - Computer and Information Sciences, 32(12), 1473-1482. doi: 10.1016/j.jksuci.2020.09.005

[99] Alharbi, A., Alshammari, F., & Alqahtani, M. (2021), “Improving cloud computing data security Using Integrated Cryptographic Transformations: A

Review", Journal of Cybersecurity, 7(1), tyab003. doi: 10.1093/cybsec/tyab003

[100] Nidhi Shah "Data Security in Cloud Computing A Comprehensive Survey", Digvijay Mahida - 2018.

[101] Lynda Kacha, "An Overview on Data Security in Cloud Computing", Abdelhafid Zitouni - 2018.

[102] Bajirao Subhash Shirole, L.K. Vishwamitra, "Review Paper on Data Security in Cloud Computing Environment", 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020.

[103] Rajanikanth Aluvalu, V. Uma Maheswari, Krishna Keerthi Chennam, S. Shitharth, "Data Security in Cloud Computing Using Abe-Based Access Control", Architectural wireless networks solutions and security issues, Vol. 196, Springer, 2021, pp. 47-61

[104] Wang, X., Zhang, H., & Liu, Z, "A Novel 2D Chaotic Map and Its Application in Image Encryption", IEEE Transactions on Circuits and Systems for Video Technology, 31(4), 1309-1322.(2021).

[105] Lu, J., Yu, S., & Ho, D. W., "A novel 2D chaotic map and its application in color image encryption", Journal of Ambient Intelligence and Humanized Computing, 11(12), 5687-5703.(2020).

[106] Zhou, C., Zhang, Y., & Xu, Y., "An improved 2D chaotic map and its application in image encryption", International Journal of Bifurcation and Chaos, 30(12), 2050206.(2020).

[107] Tian, X., & Cui, L. A, "New 2D Chaotic Map and Its Application in Color Image Encryption", Entropy, 21(7), 657.(2019).

[108] Zhang, L., Li, Y., Zhang, Z., & Zhou, W., "An image encryption scheme based on a 2D chaotic map", Entropy, 20(2), 78.(2018).

[109] Das ML, Saxena A, Gulati VP., "A dynamic ID-based remote user authentication scheme", IEEE transactions on Consumer Electronics. 2004 Jul 6;50(2):629-31.

[110] Shah, S. H., Iqbal, A., & Shah, S. S. A. (2013, October), "Remote health monitoring through an integration of wireless sensor networks, mobile phones & cloud computing technologies", In *2013 IEEE Global Humanitarian Technology Conference (GHTC)* (pp. 401-405). IEEE.

[111] Xiong, Z., Sheng, H., Rong, W., & Cooper, D. E. (2012), "Intelligent transportation systems for smart cities: a progress review", *Science China Information Sciences*, *55*(12), 2908-2914.

[112] Mois, G., Sanislav, T., & Folea, S. C. (2016), "A cyber-physical system for environmental monitoring", *IEEE transactions on instrumentation and measurement*, *65*(6), 1463-1471.

[113] Yeh, H. L., Chen, T. H., Liu, P. C., Kim, T. H., & Wei, H. W. (2011), "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography", *Sensors*, *11*(5), 4767-4779.

[114] Das, A. K., Sharma, P., Chatterjee, S., & Sing, J. K. (2012), "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", *Journal of Network and Computer Applications*, *35*(5), 1646-1656.

[115] Xue, K., Ma, C., Hong, P., & Ding, R. (2013), "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks", *Journal of Network and Computer Applications*, *36*(1), 316-323.

[116] Xu, S., & Wang, X. (2013), "A new user authentication scheme for hierarchical wireless sensor networks", *Int. Rev. Comput. Softw*, *8*(6), 197-203.

[117] Turkanovic, M., & Holbl, M. (2013), "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks", *Elektronika ir Elektrotechnika*, *19*(6), 109-116.

[118] Li, C. T., Weng, C. Y., & Lee, C. C. (2013), "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks", *Sensors*, *13*(8), 9589-9603.

[119] Turkanović, M., Brumen, B., & Hölbl, M. (2014), "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notio", *Ad Hoc Networks*, *20*, 96-112.

[120] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment", *Ad Hoc Networks*, *36*, 152-176.

[121] Amin, R., & Biswas, G. P. (2016), "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks", *Ad Hoc Networks*, *36*, 58-80.

[122] Sharma, G., & Kalra, S. (2020), "Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications", *Journal of Ambient Intelligence and Humanized Computing*, *11*(4), 1771-1794.

LIST OF PUBLICATIONS

1. Sartaj Singh, Dr. Ashok Sharma, Pranay Jha "Data Control in Public Cloud Computing: Issues and Challenges". Paper published in benthamscience,17-06-2019, Volume 14, Issue 2 , 2021 (Scopus)

2. Sartaj Singh, Dr. Ashok Sharma, "Use of Cloud based Framework for remotely managing the storages in different Machines Using Web API." jetir.org, 26-11-2018,November 2018, Volume 5, Issue 11,UGC.

3. Sartaj Singh, Dr. Ashok Sharma, "Data Storage and Computation In Cloud: A Review." THINK INDIA, 07-Dec-19,Vol-22-Issue-17, ISSN 0971-1260, UGC Journal.

4. Sartaj Singh, Dr. Ashok Sharma, "Cryptosystems in Asymmetric Cryptography for Securing Data at various Level." THINK INDIA 07-Dec-19, Vol-22-Issue-17, ISSN 0971-1260 UGC Journal.

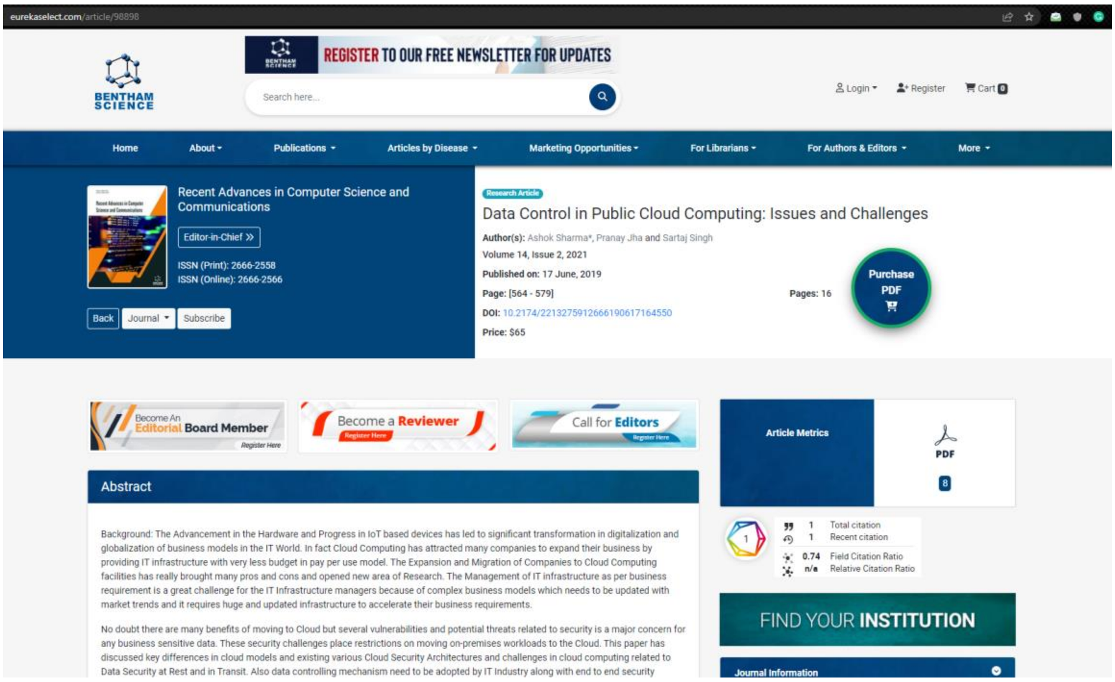
5. Sartaj Singh, Dr. Ashok Sharma "Cryptosystems in Asymmetric Cryptography for Securing Data at various Level." Refereed Journal Delving-Journal of Technology and Engineering Dec-20,Vol. 4 Issue 2 , ISSN 0975-5829 Refereed Journal.

6. Sartaj Singh, Dr. Amar Singh, "Data Security in Cloud Environment: A Comprehensive Survey & Open Challenges". International Conference on Innovation, Research and Challenges in Emerging Technologies (IRCET-2021) (Scopus).

7. Sartaj Singh, Dr. Amar Singh, Dr. Geeta, "Secure and Efficient User Authentication Scheme for Wireless Sensor Networks in Cloud-IoT applications". ICCTBM 20-21 January, 2022 International Conference On Smart Computing Technologies And Business Management Strategies, Chandigarh Business School Of Administration, Landran In collaboration with Perdana University, Malaysia (Scopus).

8. Sartaj Singh, Dr. Amar Singh, Dr.Geeta, “Robust Cloud-based IoT Authenticated key agreement scheme for Wireless Sensor Networks.” RACS-04-05 Nov. 2022 1st International Conference On Recent Advances In Computing Sciences 04-11-2022(Scopus).

9. Sartaj Singh, Dr. Amar Singh “An enhanced authentication key agreementy scheme for cloud based IoT in wireless sensor networks”. Paper published in International Journal of Electrical and Electronics Research on 23 October 2023.


eurekaselect.com/article/98898
REGISTER TO OUR FREE NEWSLETTER FOR UPDATES
BENTHAM SCIENCE
Search here...
Login
Register
Cart 0
Home
About
Publications
Articles by Disease
Marketing Opportunities
For Librarians
For Authors & Editors
More
Recent Advances in Computer Science and Communications
Editor-in-Chief
ISSN (Print): 2666-2558
ISSN (Online): 2666-2566
Back
Journal
Subscribe
Research Article
Data Control in Public Cloud Computing: Issues and Challenges
Author(s): Ashok Sharma*, Pranay Jha and Sartaj Singh
Volume 14, Issue 2, 2021
Published on: 17 June, 2019
Page: [564 - 579]
Pages: 16
DOI: 10.2174/2213275912666190617164550
Price: $65
Purchase PDF
Become An Editorial Board Member
Register Here
Become a Reviewer
Register Here
Call for Editors
Register Here
Article Metrics
PDF
8
Abstract
Background: The Advancement in the Hardware and Progress in IoT based devices has led to significant transformation in digitalization and globalization of business models in the IT World. In fact Cloud Computing has attracted many companies to expand their business by providing IT infrastructure with very less budget in pay per use model. The Expansion and Migration of Companies to Cloud Computing facilities has really brought many pros and cons and opened new area of Research. The Management of IT infrastructure as per business requirement is a great challenge for the IT Infrastructure managers because of complex business models which needs to be updated with market trends and it requires huge and updated infrastructure to accelerate their business requirements.
No doubt there are many benefits of moving to Cloud but several vulnerabilities and potential threats related to security is a major concern for any business sensitive data. These security challenges place restrictions on moving on-premises workloads to the Cloud. This paper has discussed key differences in cloud models and existing various Cloud Security Architectures and challenges in cloud computing related to Data Security at Rest and in Transit. Also data controlling mechanism need to be adopted by IT Industry along with end to end security
1 Total citation
1 Recent citation
0.74 Field Citation Ratio
n/a Relative Citation Ratio
FIND YOUR INSTITUTION
Journal Information

THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

A Study of Various Security Threatsin RSA

Sartaj Singh*, Ashok Sharma, Sandeep Kaur

**PhD Scholar, School of Computer Science and Engineering, LPU, Phagwara*

Associate Professor, School of Computer Science and Engineering, LPU, Phagwara

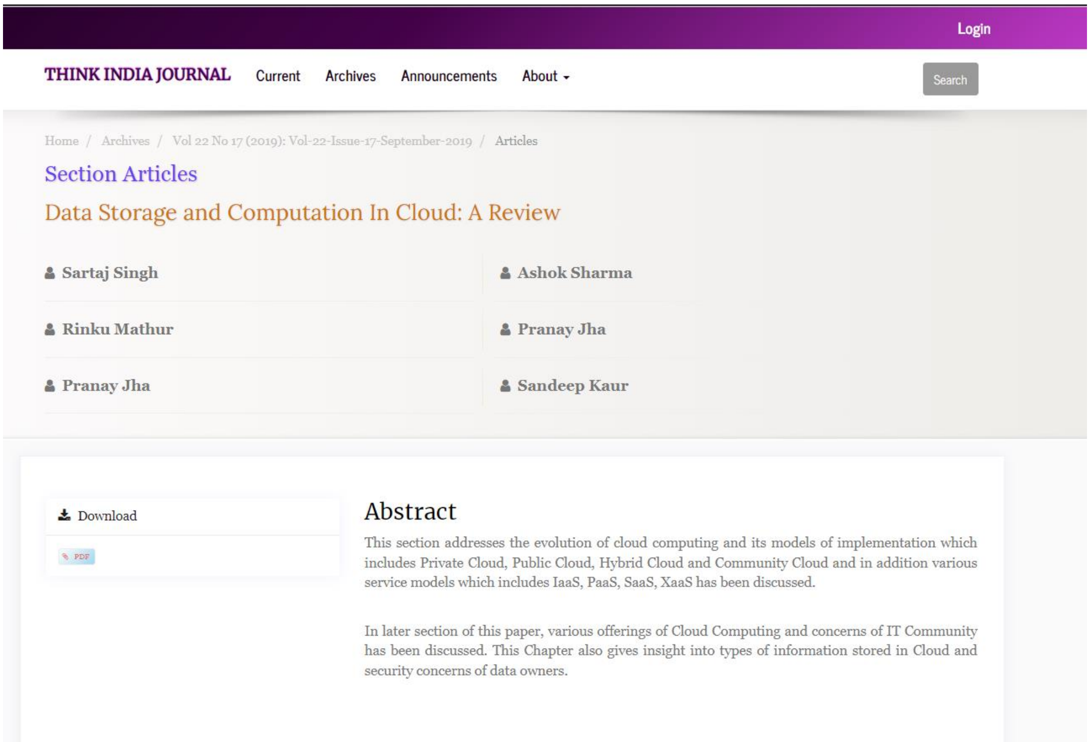
Assistant Professor, Guru Nanak College for Women, CharanKanwal, Banga

Abstract:

Data Security has been concern for all stakeholders no matters the customer types, organisations. Securing data in rest in cloud or somewhere else and even during the communication is always not trustworthy. The entire research in data security deals in these two cases only and no matter we claims a lot but very next moment leads us to another threats. In this paper we have examine the various threats found by various researchers in most adopted RSA algorithm.

Introduction

Cryptographic algorithm is deemed very important in cryptosystem for, as well as, maintaining authentic and confidential message. Encryption and decryption are the primary necessity for privacysecurity on the internet [18]. Creating secret keys Sk, is


Login

THINK INDIA JOURNAL Current Archives Announcements About

Search

Home / Archives / Vol 22 No 17 (2019): Vol-22-Issue-17-September-2019 / Articles

Section Articles

Data Storage and Computation In Cloud: A Review

Sartaj Singh

Ashok Sharma

Rinku Mathur

Pranay Jha

Pranay Jha

Sandeep Kaur

Download

PDF

Abstract

This section addresses the evolution of cloud computing and its models of implementation which includes Private Cloud, Public Cloud, Hybrid Cloud and Community Cloud and in addition various service models which includes IaaS, PaaS, SaaS, XaaS has been discussed.

In later section of this paper, various offerings of Cloud Computing and concerns of IT Community has been discussed. This Chapter also gives insight into types of information stored in Cloud and security concerns of data owners.

Delving

Journal of Technology and Engineering Sciences

An Open Access Journal

ISSN 0975-5829

December 2020

Vol. 4 Issue 2

Articles

PANIPAT INSTITUTE OF ENGINEERING & TECHNOLOGY

(Approved by AICTE, New Delhi & Affiliated to Kurukshetra University, Kurukshetra)

INTERNATIONAL CONFERENCE
ON
INNOVATION, RESEARCH AND CHALLENGES IN EMERGING TECHNOLOGIES (IRCET-2021)

CERTIFICATE

This is to certify that ***Mr. Sartaj Singh*** *from* ***LPU Phagwara*** *has presented a paper entitled* ***"Data Security in Cloud Environment: A Comprehensive Survey & Open Challenges"*** *in the International Conference on Innovation, Research and Challenges in Emerging Technologies (IRCET-2021) organized by Department of Information Technology and Department of Electronics & Communication Engineering at Panipat Institute of Engineering & Technology, Samalkha, Panipat on 19th -20th November, 2021.*

Conveners | Conference Chair | Director

CHANDIGARH GROUP OF COLLEGES

Building Careers. Transforming Lives.

PERDANA UNIVERSITY DU026(B)

ONLINE INTERNATIONAL CONFERENCE ON SMART COMPUTING TECHNOLOGIES AND BUSINESS MANAGEMENT STRATEGIES: (ICCTBM 2022)

CERTIFICATE OF PARTICIPATION

This is to certify that Dr. / Mr. / Ms. SARTAJ SINGH from LPU, PHAGWARA has presented a Research Paper titled SECURE AND EFFICIENT USER AUTHENTICATION SCHEME FOR WIRELESS SENSOR NETWORKS IN CLOUD-IOT APPLICATIONS in the International Conference held at Chandigarh Business School of Administration, Landran in collaboration with Perdana University, Malaysia on 20th & 21st January, 2022.

Dr. Tejinder Pal Singh Brar
Conference Convener

Dr. Ramandeep Saini
Conference Chair

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

RACS

SCHOOL OF COMPUTER APPLICATION

Certificate No. 255647

BEST PAPER AWARD

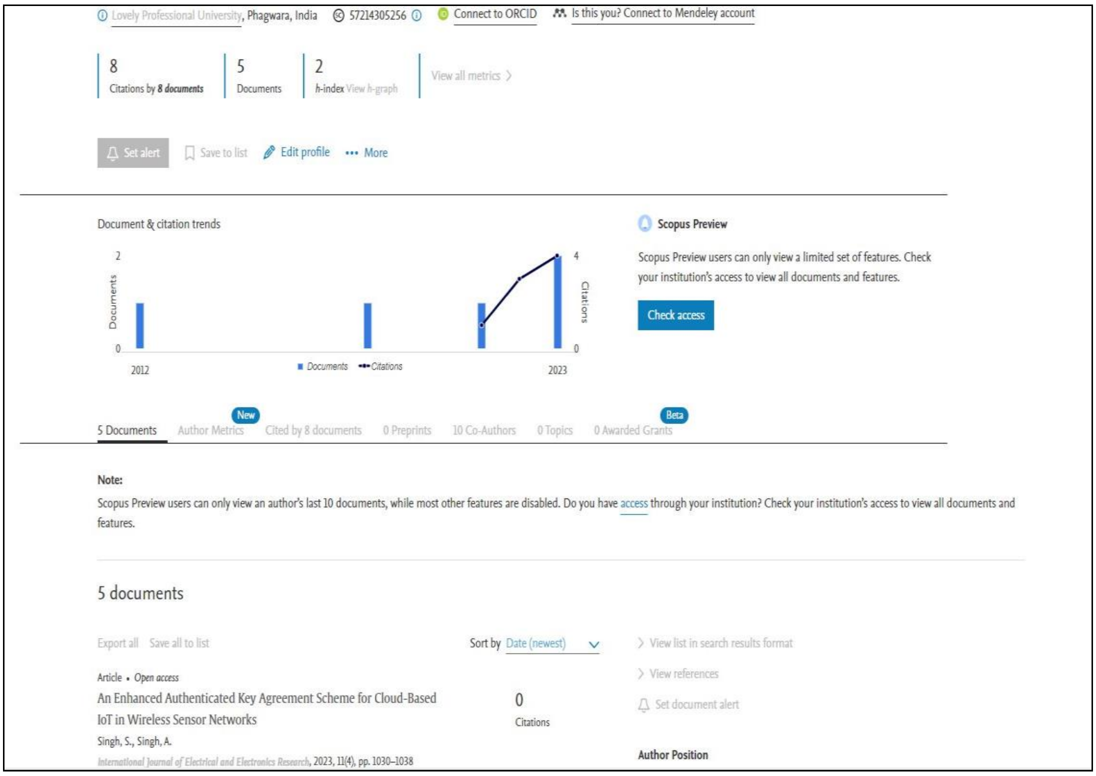
Presented to

Dr./Mr./Ms. **Sartaj Singh** of **Lovely Professional University** for his/her research paper entitled **"Robust Cloud-based IoT Authenticated key agreement scheme for Wireless Sensor Networks"** presented in the ***1st International Conference on Recent Advances in Computing Sciences (RACS-2022)*** held from 4th to 5th November 2022, organized by School of Computer Application at Lovely Professional University, Punjab.

Date of Issue : 05-11-2022
Place : Phagwara (Punjab), India

Debayan Ghosh

Prepared by (Administrative Officer-Records)	**Convener (RACS-2022)**	**Conference Chair (RACS-2022)**	**Session Chair (RACS-2022)**


Lovely Professional University, Phagwara, India 57214305256 Connect to ORCID Is this you? Connect to Mendeley account

8 Citations by 8 documents | 5 Documents | 2 h-index View h-graph | View all metrics >

Set alert Save to list Edit profile ••• More

Document & citation trends

Scopus Preview

Scopus Preview users can only view a limited set of features. Check your institution's access to view all documents and features.

Check access

5 Documents | Author Metrics New | Cited by 8 documents | 0 Preprints | 10 Co-Authors | 0 Topics | 0 Awarded Grants Beta

Note:

Scopus Preview users can only view an author's last 10 documents, while most other features are disabled. Do you have access through your institution? Check your institution's access to view all documents and features.

5 documents

Export all Save all to list Sort by Date (newest)

> View list in search results format

> View references

Set document alert

Article • *Open access*

An Enhanced Authenticated Key Agreement Scheme for Cloud-Based IoT in Wireless Sensor Networks

Singh, S., Singh, A.

International Journal of Electrical and Electronics Research, 2023, 11(4), pp. 1030–1038

0 Citations

Author Position