REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

ENHANCING CLOUD COMPUTING SECURITY USING THE CHAOS THEORY FOR CRYPTO SYSTEMS

Mustafa Ameer Sabri AWADH

Master's Thesis

Supervisor

Asst. Prof. Dr. Muhammad İLYAS

Istanbul, 2023

ENHANCING CLOUD COMPUTING SECURITY USING THE CHAOS THEORY FOR CRYPTO SYSTEMS

Mustafa Ameer Sabri AWADH

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

Istanbul, 2023

The thesis titled ENHANCING CLOUD COMPUTING SECURITY USING THE CHAOS THEORY FOR CRYPTO SYSTEMS prepared by MUSTAFA AMEER SABRI AWADH and
submitted on 08/08/2023 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

Asst. Prof. Dr. Muhammad ILYAS
Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Department of Computer Engineering, Altınbaş University	
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	
Asst. Prof. Dr. Jawad RASHEED	Department of Software Engineering, Nişantaşı University	

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis. Submission date of the thesis to Institute of Graduate Studies: / /

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Mustafa Ameer Sabri AWADH

Signature

DEDICATION

To begin with, I would want to praise and thank Allah, the Almighty, for providing me with the information, skills, and chance to conduct and successfully complete my research. Sincere thanks go out to my parents. They have been the driving force behind everything good that has happened to me, and their love is the foundation upon which everything rests. Now is the perfect time for me to thank my sister and brother for their love and support.

PREFACE

My adviser, Asst. Prof. Dr. Muhammad İLYAS, gave me the guidance, supervision, motivation, and help I needed to finish my studies, and I am very grateful to him for that. His perseverance, willingness to collaborate with me, critical criticism, and useful suggestions have significantly increased my comprehension and confidence. I value the time he spent reviewing my work and pointing out my mistakes. Last but not least, I'd want to thank everyone for their encouragement, prayers, and/or wise counsel.

ABSTRACT

ENHANCING CLOUD COMPUTING SECURITY USING THE CHAOS THEORY FOR CRYPTO SYSTEMS

AWADH, Mustafa Ameer Sabri

M.Sc,. Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Muhammad İLYAS

Date: August / 2023

Pages: 81

The safety of the information stored in the cloud has emerged as a primary worry in recent years alongside the expansion of cloud computing. Traditional encryption algorithms, such as Advanced Encryption Standard (AES), are susceptible to attacks, particularly when the keys are held on the cloud. This is because cloud providers encrypt data to protect it from unauthorized access. As a consequence of this, there is a requirement for an updated encryption method that offers a higher level of protection for data stored in the cloud. In this thesis, a modified version of the AES algorithm is proposed as a solution to the problem of ensuring the safety of cloud data by improving the key management and encryption procedure. In order to protect the secrecy, integrity, and authenticity of data stored in the cloud, a modified version of the AES algorithm makes use of a hybrid key management technique. This strategy combines the benefits of symmetric and asymmetric encryption. A randomized encryption procedure is also a part of the method. This process helps to ensure that the ciphertext is completely unique and makes it more difficult for adversaries to break the encryption. Using a cloud- based system, the purpose of this paper is to analyze the efficiency as well as the safety of a modified version of the AES algorithm. The evaluation will include a comparison of the modified AES algorithm with typical encryption algorithms, such as AES and RSA, in terms of security, efficiency, and scalability. [CDATA[The evaluation will include a comparison of the modified AES algorithm with traditional encryption algorithms, such as AES and RSA. The findings of the evaluation will illustrate the efficacy of the modified AES algorithm in preventing illegal access to cloud data and preserving the confidentiality and safety of cloud-based systems.

Keywords: AES , Cloud Computing , Encryption , Chaotıc Map, Cryptography.

TABLE OF CONTENTS

Pages

LIST OF TABLE

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AES	:	Advanced Encryption Standard
IoT	:	Internet of Things
ECC	:	Elliptic Curve Cryptography
DSA	:	Digital Signature Algorithm
DH	:	Diffie-Hellman
DES	:	Data Encryption Standard
3DES	:	Triple Data Encryption Standard
GDPR	:	General Data Protection Regula tio
HIPAA	:	Health Insurance Portability and Accountability Act
CMRC	:	Chaotic-map Research Cryptosystem
DPA	:	Differential Power Analysis Virtualization
VCM	:	Cryptography Machine
EMTACA	:	Enhanced Mutual Trusted Access Control Algorithm
SLA	:	Service Level Agreement
SaaS	:	Software as a Service
PaaS	:	Platform as a Service
IaaS	:	Infrastructure as a Service
AWS	:	Amazon Web Services
GCP	:	Google Cloud Platform
CRM	:	Customer Relationship Management
IAM	:	Identity and Access Management

VPNs : Virtual Private Networks

PII : Personally Identifiable Information

NIST : National Institute of Standards and Technology

1. INTRODUCTION

1.1 INTRODUCTION

This use of cryptographic techniques is referred to as "cryptography," and the term "cryptography" is used to refer to this use of cryptographic methods. The use of cryptographic methods to secure data that is either being sent to or stored in the cloud is referred to as "cryptography," and the term "cryptography" is used to refer to this use of cryptographic methods. The term "cloud computing" refers to a category of information technology in which resources like as processing power, storage space, and application software are made available on demand over the internet. Cloud computing is also known as "utility computing." Another name for this type of information technology is "the cloud." Cryptography is a vital component of cloud computing because it provides a mechanism to guarantee the secrecy, integrity, and authenticity of data that is being exchanged or stored on the cloud. This makes cryptography an indispensable part of cloud computing. This is due to the fact that cryptography supplies a method for keeping the data secure. As a consequence of this, encryption has developed into an important component of cloud computing. Computing environments that make use of the cloud are subject to a wide variety of security risks, some of which include the loss of data, access to the data that was not permitted, and theft of the data. The employment of cryptography affords an additional layer of protection against potential dangers such as these, and so should be considered. When applying cryptography in cloud computing, some of the cryptographic activities that need to be carried out include encryption, hashing, digital signatures, and key management. These are just a few examples. Among the other activities involved in cryptography is hashing. The data that needs to be protected can be encrypted so that it is transformed into a format that cannot be read by utilizing a key that is kept a secret. This allows the data to be transformed into a format that cannot be read. The data can then be transformed into a format that cannot be read as a result of this. The original data are utilized in order to generate a digest that is of a particular length. The purpose of hashing is to verify that the generated digest is accurate by employing a length that is predetermined. Digital signatures are a form of authentication that can be used to confirm the sender's identity as well as detect anyattempts to manipulate the data. A vendor of digital services is responsible for supplying these signatures. This enables the process of assuring the validity and integrity of data to make use of digital signatures, which was not previously possible. The process of encrypting and

decrypting data calls for the utilization of cryptographic keys, which are required to be protected by the utilization of key management in order to fulfill the requirements of the process. The use of cryptography in cloud computing provides a method for securing data that is stored on the cloud by guaranteeing the data's confidentiality, integrity, and validity. This methodology for data security is made possible by the use of cryptography in cloud computing. The utilization of encryption in cloud computing might provide a solution to this problem. It is absolutely necessary in order to protect the privacy of data that is stored in the cloud, in particular in settings where multiple users and applications use the same resources. [5].

1.2 CRYPTOGRAPHY

The study of processes that can guarantee that information transported across a network will remain private, unchanged, and unmodified is referred to as cryptography. This branch of knowledge is sometimes referred to as the study of several techniques th<at can keep a secret. The investigation of information security can also be referred to as research on information security, which is a word that is used in some contexts. The word kryptos may be translated as "hidden" or "secret," and the word graphein can be translated as "writing." Both of these words are from the Ancient Greek language. The modern definition of the term "cryptography" when it is used as a noun originates from the merging of these two different ideas. People have used cryptography at all periods in time throughout history, from ancient times right up until the present day, to secure sensitive information such as military plans, trade secrets, and personal details. Cryptography has been utilized by people from ancient times right up until the present day. This practice dates all the way back to the period of the ancients (prehistoric era). Encryption and decryption are the two fundamental procedures that can be used to deconstruct any cryptographic activity into its component elements. Encryption and decryption are the two fundamental processes that can be utilized to decrypt any message. Using ciphers, which are combinations of letters and numbers, is one method for accomplishing this goal. The goal of encryption is to render the original message unintelligible and unreadable by transforming the plaintext of the message into the ciphertext. This is accomplished by replacing the plaintext with the ciphertext. The plaintext is jumbled up in order to achieve this goal. This is accomplished by changing the plaintext of the message into the ciphertext instead of displaying it. Before you are able to read the

ciphertext, the first step that needs to be taken is to decrypt the ciphertext. The original message, which is hidden in the ciphertext, can only be read by those individuals who have been given the correct decryption key and have been told that they can be trusted with it. Other people will not be able to read the original message since it is encrypted. The basic goal of cryptography is to restrict access to information so that it can be understood by no one other than those who are specifically designated to receive it. This is accomplished by encoding messages in a way that is unintelligible to anybody other than those individuals. One method that can be used to accomplish this objective is to encrypt the information in such a way that they are the only ones who can decipher it. There are many distinct kinds of encryption, the most common of which are symmetric key encryption and public key encryption. There are also numerous other kinds of encryption. Nevertheless, these are only two of the many conceivable variants that are available. In addition to this, there are a large number of distinct sorts of technologies that are used for encrypting information. When data is encrypted using a symmetric key, the key that is used for the encryption operation is the same key that is used for the decryption method. The safety of the data is ensured as a result of this action. It is essential for both parties—the sender and the recipient—to keep the location of the key a secret in order to ensure that both parties can preserve their respective levels of privacy. This can be accomplished by both sides keeping the location of the key a secret from one another. When encrypting data with a public key, one of the keys is made available to the entire public, while the other key is held under the highest level of confidence possible. It is not required to impose any restrictions on the diffusion of the public key; nevertheless, the private key must always be held in a location that is inaccessible and secure. After the communication has been encrypted using the recipient's public key, the only thing that can decrypt it is the recipient's private key, which is kept secret. After the message has been encoded utilizing the recipient's public key, the message can then be decrypted utilizing the recipient's private key. While a message is being transmitted via a network, the use of cryptography can help to ensure a number of different things, one of which is that the message is authentic. This is one of the objectives that the study of cryptography strives to realize as part of its mission. The authenticity of messages can be "fingerprinted" in a digital sense by utilizing cryptographic hashing algorithms. This enables the authenticity of the communications to be established in a way that was not previously feasible. Because the hash value will also change if the message is altered in any manner, it will be much simpler

to identify any efforts at manipulation. This is because any change to the message will cause the hash value to shift. Because of this, it is now much simpler to recognize any effort at manipulation. One of the most important jobs that can be done with the assistance of cryptography is authentication, which is also one of the most difficult. In order to successfully carry out this function, it is essential to verify the identity of the message's sender and to check that the information contained in the message has not been altered in any way while it is being sent. In addition to this, it is important to make sure that the message has not been changed in any manner, since this could be a sign of possible malicious intent. Digital signatures are a versatile kind of verification that may be applied in a variety of different scenarios. They can be used to authenticate digital documents. They can be utilized for the verification of transactions conducted either online or offline. As a result of this, they are an effective instrument for determining whether or not objects are genuine. After the message is hashed and combined with a value, a digital signature can be created by encrypting the value with the sender's private key, followed by encrypting the result with the message itself. This process is called a two-step encryption. This procedure is carried out numerous times till the signature is finished. If the recipient makes use of the public key that was supplied by the sender, then they will have the ability to decipher the digital signature that was left behind by the sender. Before agreeing to receive the communication, the recipient will have the opportunity to confirm the sender's identity using this method. The process of generating cryptographic keys and then ensuring that those keys continue to be secure and confidential once they have been generated is referred to as key management. The formulation of the cryptographic keys is the initial step in this process. Maintaining the secrecy of cryptographic keys is an absolutely essential step toward ensuring that the system will operate as intended at all times. Management of encryption keys is an essential component of data security. The study of processes that can guarantee that information transported across a network will remain private, unchanged, and unmodified is referred to as cryptography. This branch of knowledge is sometimes referred to as the study of several techniques that can keep a secret. The investigation of information security can also be referred to as research on information security, which is a word that is used in some contexts. Cryptography is utilized in a variety of settings, including but not limited to electronic transactions, online banking, and cloud computing, amongst other applications, to protect the financial and personal information of customers who are doing transactions online. This

security is offered in a wide range of contexts, including but not limited to online banking, cloud computing, and online financial dealings.

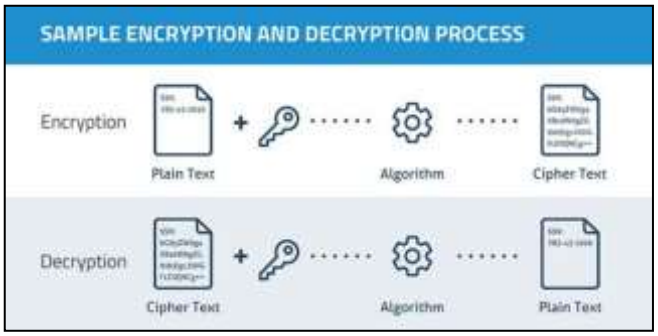

Figure 1. 1: Encryption/Decryption Process [11].

1.2.1 Security Algorithm

The application of a wide variety of mathematical methods is at the core of the field of study known as cryptography. The primary goal of this field is to protect the confidentiality of data and information while it is being sent. Cryptography is a method of information protection that makes use of something called a security algorithm. This strategy involves adhering to a set of predetermined regulations and operating procedures at all times. In the course of this conversation, I'm going to go over a few of the most common cryptographic security mechanisms that are now being utilized. These are techniques that protect information using encryption. The abbreviation AES refers to the phrase "Advanced Encryption Standard." The Advanced Encryption Standard, more commonly referred to as AES and in some places referred to simply as AES, is a form of symmetric encryption that is widely deployed for the purpose of maintaining the security of data in a wide variety of contexts. This encryption method was developed in the 1990s and has since become the industry standard. The use of online banking, online shopping, and the online sharing of files are all instances of these types of circumstances. Due to the fact that AES is a block cipher, the data is encrypted in discrete chunks of a size that has been predetermined before the encryption process begins. This dimension is subject to modification at any time. The Advanced Encryption Standard, also known as AES, is widely recognized as one of the most trustworthy encryption algorithms currently available. It is possible to use keys of 128, 192, or 256 bits in length. The RSA algorithm is a form of encryption that makes use of public-key cryptography. As a result of this technology, it is now possible to have confidential discussions and to create digital signatures. Both the encryption and decryption processes that use RSA need to make

use of a public key in addition to a private key for the operations to be successful. Under no circumstances are the general public made aware of these keys and where they can obtain them. The safety of the private key is never put at risk, despite the fact that anybody can publish and distribute the public key. This is because the protection of the private key is always given the utmost importance. The already difficult task of decryption is made considerably more difficult by the fact that the RSA algorithm is based on the mathematical idea of prime factorization. When employing the symmetric encryption method known as Blowfish, the length of a key can be anywhere from 32 bits all the way up to 448 bits in its entirety. This length range is possible because Blowfish uses a symmetric encryption algorithm. File-sharing services and online financial transactions are only two examples of the many places where the well-known Blowfish algorithm for encrypting data is put to use. Blowfish encryption is utilized not just in these but also in a variety of other settings. The fact that the block cipher known as Blowfish is both easy to use and secure has contributed significantly to its widespread acceptance. The family of SHA-2 cryptographic hash functions is utilized extensively in a variety of applications, including data encryption and electronic signatures, amongst others. Hashing the data that are provided as input results in a value that is formed using SHA- 2 and has a size that has been established in advance. Because of this, it is now much easier to validate the data and make certain that it is an accurate representation of the situation. Hash widths ranging from 224 bits all the way up to 512 bits are supported by SHA-2. The greatest hash width that SHA-2 can support is 512 bits, however it can support hash widths of any size. The method of public-key encryption known as elliptic curve cryptography (elliptic curve cryptography, or ECC for short) uses elliptic curves as the fundamental building block of the system. ECC is frequently used in programs that require encryption that is both lightweight and speedy for the purposes of protecting communication and establishing digital signatures. ECC is regularly used in programs that require encryption that is both lightweight and quick. ECC is a suitable choice for mobile devices and other low-power devices since it provides the same level of security as RSA but requires a smaller key size. This makes it an ideal choice for devices that have limited power resources. Because of this, it is an excellent option for use in public-key cryptography. Because ECC provides the same amount of safety, this is the explanation for why this is the case. The Diffie-Hellman protocol is a mechanism for exchanging keys that is used in the process of building a secure channel of communication between two parties.

The protocol was named after the two individuals who developed it. This procedure was given its current name in honor of the two researchers who initially invented it. The Diffie-Hellman protocol is one that permits two parties to safely swap a secret key despite the fact that their connection is not being protected. This is possible because the protocol is named after the two people who developed it. The names of the two mathematicians who contributed to its development were selected as a way to thank them. Virtual private networks (VPNs) and SSL/TLS are two examples of technologies that rely on encrypted communication to function properly. The Diffie-Hellman algorithm is utilized to a significant degree in both of these groups of applications. The usage of security algorithms is essential to the field of cryptography because these algorithms offer a dependable technique of preserving the confidentiality of sensitive data. As a result, the utilization of security algorithms is essential to the field of cryptography. These procedures, which make use of methods such as encrypting, decrypting, hashing, and exchanging keys, make it possible to guarantee the data's authenticity, integrity, and secrecy. In addition, the data's integrity can be maintained. Methods are utilized by these various procedures as well. The requirements of the application will be used to determine the speed, efficiency, and safety criteria of the algorithm that must be selected. [13].

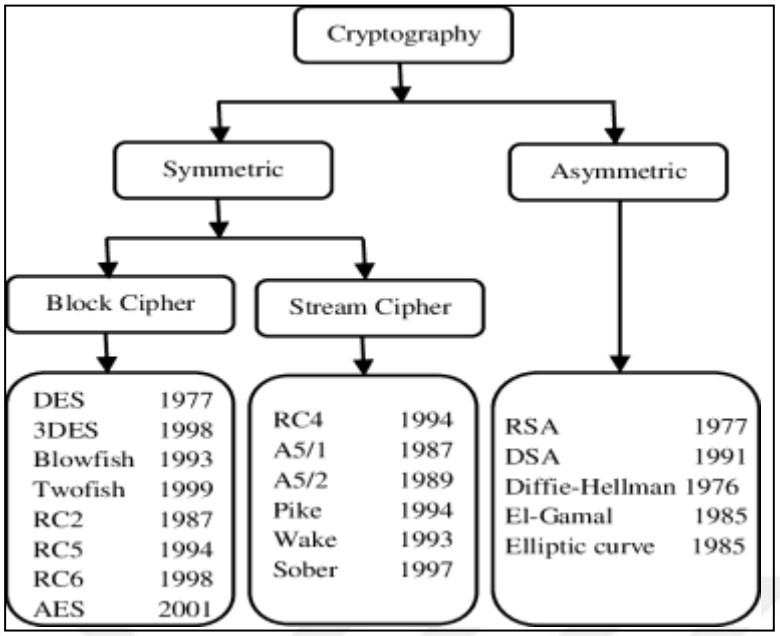

Figure 1. 2: Classification of Algorithms [13].

1.2.2 Asymmetric Algorithm

A method known as asymmetric cryptography, which is also known as public-key cryptography, can be used to encrypt and decrypt data. Other names for this type of encryption include public-key cryptography. This approach encrypts and decrypts data by utilizing two keys that are independent from one another but are mathematically related to one another. The independence of the keys does not affect the effectiveness of the encryption or decryption. Both of these keys are used, but only one of them is disclosed to the general public. However, the public key can be retrieved by anyone who makes a request for it, and the person who has the secret key will always maintain total control over the public key. The use of symmetric cryptography is less secure than the use of asymmetric cryptography because it needs the use of the same key for both encryption and decryption. Asymmetric cryptography uses different keys for each operation. It is commonly used for secure communication as well as digital signatures as a result of the increased level of security that it provides. In asymmetric cryptography, the generation of a key, the process of encrypting data, and the process of decrypting data each make use of their own individual algorithms. This ensures that no two sets of encrypted data can be read by the same set of decryption methods. This article provides an explanation of several of the asymmetric algorithms that are now used most frequently in cryptography. Asymmetric algorithms are becoming increasingly important in the field of cryptography. The science of

cryptography is beginning to place an increased emphasis on asymmetric algorithms due to their growing significance. The well-known asymmetric method RSA uses the mathematical process of prime factorization as its primary structural component. This is because the factorization of prime numbers is the most secure kind of encryption. One example of an asymmetric approach is presented here. When utilizing the RSA algorithm, the utilization of two very large prime integers is required in order to generate a public key as well as a private key for use in the procedure. Hackers will have a harder time deciphering the encryption method that is now being utilized as a result of this action being taken. It is normal practice to use the RSA cryptographic method for both the production of digital signatures and the encryption of messages. This approach may be found in most modern computers. The term "elliptic curve cryptography" (ECC) is used the vast majority of the time to refer to the type of cryptography that makes use of public keys and is founded on elliptic curves. ECC is a suitable choice for mobile devices and other low-power devices since it provides the same level of security as RSA but requires a smaller key size. This makes it an ideal choice for devices that have limited power resources. Because of this, it is an excellent option for use in public-key cryptography. Because ECC provides the same amount of safety, this is the explanation for why this is the case. The Digital Signature Algorithm (DSA) is an example of a public-key algorithm that is frequently utilized for the purpose of producing digital signatures. When utilizing DSA, a pair of keys will be generated: one will be public and will be used for validating signatures, and the other will be private and will be used for signing messages. The public key will be used for validating signatures, and the private key will be used for signing messages. The public key will be used to validate signatures, while the private key will be used to sign messages. Both keys are required for the process. The Digital Signature Algorithm (DSA) is founded on the fundamental concept of discrete logarithm, which serves as the algorithm's underlying mathematical foundation. This serves as the basis upon which the DSA is built. The Diffie-Hellman (DH) algorithm is a technique for exchanging keys that is used to construct a safe line of communication between two different parties. This line of communication is established by using the Diffie-Hellman (DH) algorithm. Ron Rivest and Martin Hellman are credited with the development of this method. The Diffie- Hellman protocol is one that permits two parties to safely swap a secret key despite the fact that their connection is not being protected. This is possible because the protocol is named after the two people who developed it. The names of the two

mathematicians who contributed to its development were selected as a way to thank them. Both secure communication protocols (SSL/TLS) and virtual private networks (VPNs) make considerable use of DH as a key cryptographic building block. "Virtual private network" is what is meant to be referred to when using the abbreviation VPN.

1.2.3 Symmetric Algorithm

A form of cryptography known as "symmetric cryptography" is one in which the encryption and decryption processes make use of the same key. This form of cryptography was developed in the 1960s. Exactly the same steps are taken to encrypt and decrypt messages when using this particular method of encryption. This particular kind of encryption got its name from the symmetric key arrangement, which also served as the source of its inspiration. Due to the fact that the key may only be used to decode the communication if the owner of the key is aware of its location, it is of the utmost significance that both parties maintain the communication's confidentiality. Because it can encrypt and decrypt data quickly and effectively, symmetric cryptography is extensively used for secure communication and the storing of data. This is due to the fact that it can do both functions with relative ease. Symmetric cryptography makes use of a wide variety of methods and processes in order to encrypt and decrypt data. These are necessary steps in the process. Because of this, there is a larger capacity for flexibility. Within the confines of this part, we will discuss and evaluate a selection of the symmetric algorithms that are now seeing the most widespread application in the field of cryptography. These algorithms are used on an almost daily basis. The term "Advanced Encryption Standard," which is abbreviated as "AES," refers to a type of symmetric encryption technology that can be applied in a wide variety of settings. This category includes a wide variety of applications, some examples of which include online banking and shopping as well as the transfer of files between users. Due to the fact that AES is a block cipher, the data is encrypted in discrete chunks of a size that has been predetermined before the encryption process begins. This dimension is subject to modification at any time. The Advanced Encryption Standard, also known as AES, is widely recognized as one of the most trustworthy encryption algorithms currently available. It is possible to use keys of 128, 192, or 256 bits in length. In the past, a number of businesses depended on a kind of encryption called Data Encryption Standard (DES), which was symmetric in design and was regarded for its reliability. Since it uses a block cipher with a

key size that is not exceptionally large (only 56 bits), the Data Encryption Standard (DES) is a form of encryption that is considered to be one of the less secure options available. In recent years, the more secure and up-to- date method of encryption known as AES has gradually begun to displace the older and more vulnerable DES algorithm in popular use. When employing the symmetric encryption method known as Blowfish, the length of a key can be anywhere from 32 bits all the way up to 448 bits in its entirety. This length range is possible because Blowfish uses a symmetric encryption algorithm. File-sharing services and online financial transactions are only two examples of the many places where the well-known Blowfish algorithm for encrypting data is put to use. Blowfish encryption is utilized not just in these but also in a variety of other settings. The fact that the block cipher known as Blowfish is both easy to use and secure has contributed significantly to its widespread acceptance. The symmetric encryption method known as Triple DES (3DES) employs three keys rather than just one, making it a more secure alternative to the DES method than the latter. DES is an abbreviation for the Data Encryption Standard. Due to the fact that the block cipher that 3DES utilizes has a key size of 168 bits, it is a well-liked choice for the security of data in a wide variety of different sorts of applications. This is because of the fact that 168 bits is the maximum size that a key may be. One example of this type of application is the use of the internet to conduct financial transactions and shop. In the modern world, symmetric cryptography may be found being used in a variety of scenarios, including encrypted communication as well as online banking and shopping. These are only some of the many applications that can be found for it; there are many others. Because of the speed with which it can encrypt and decode data, symmetric cryptography is an excellent option for use in contexts involving real-time data transmission and communication. This is because it can encrypt and decode data. The requirements of the application in terms of speed, efficiency, and security should serve as a reference for choosing the suitable symmetric approach to employ in the process. [14].

1.2.4 Chaotic Map Cryptosystem

The Chaotic Map Cryptosystem is a way of encrypting data transfers that uses the characteristics of chaotic systems in order to ensure that data remains private. This type of encryption was developed in order to combat the problem of data leakage. The exploitation of chaotic system characteristics allows for the successful completion of this task. The extraordinary sensitivity of chaotic systems to the conditions under which they are first activated is one of the characteristics that define these kinds of systems. This suggests that even a modest shift in those parameters can have a significant impact on the results that are produced by the system. If one makes use of this characteristic of chaotic systems, it is feasible to generate a key for encrypting and decrypting data that is both truly random and unpredictable. This can be accomplished by using chaotic systems. It is possible to encrypt and decrypt data with the usage of this key. The Chaotic Map Cryptosystem consists of a plaintext message, a chaotic map, and a secret key. These three elements work together to decipher messages. To put together this system, you are going to need each and every one of these components. Utilizing a chaotic map makes it feasible to produce a secret encryption key starting with a random number sequence. This can be accomplished by using the map. This key can be used to encrypt as well as decrypt information. Both functions are possible with it. After the plaintext communication has been encrypted using a private key, the message that has been encrypted is then sent across a channel that is not believed to be particularly secure. This occurs after the encryption of the plaintext communication. In order for the recipient to understand the communication, they will need to make use of the identical chaotic map as well as the hidden key. The following is a list of the kinds of actions that take place within the confines of the Chaotic Map Cryptosystem: The method of generating the secret key required for encryption and decryption makes use of a chaotic map. This map is used to produce a random series of integers, which are then utilized in the process of creating the secret key. This key is necessary in order to read or write data that has been encrypted. The data can't be read or written without it. It is possible to produce the top-secret key by seeding the chaotic map with a value and then traveling iteratively over the map. This process is described in more detail in the next paragraph. This procedure can be carried out an unlimited number of times as required. To encrypt a message, it must first be broken up into blocks, and then the private key must be XORed with each block in turn. This process must be repeated until the message is encrypted. Only after that would it be possible to

comprehend the message. Before being sent across a channel that is not secure, the communication is encrypted, and the recipient of the message is the only one who can decrypt it once it has been delivered to them. After the message has been sent without error, it will next be decrypted making use of the same scrambled map and secret key that were utilized in the prior stage of the procedure. It is possible to decode the original message and reconstruct it in its plaintext form by applying XOR to each encrypted message block together with the private key. This allows for the message to be reconstructed. The Chaotic Map Cryptosystem is an example of a type of cryptography known as symmetric-key cryptography. This is due to the fact that the key is utilized in both the encryption and decryption procedures. The key is utilized in both stages of symmetric-key cryptography, which is why the technology was given its current name. The Chaotic Map Cryptosystem relies heavily on the randomization and unpredictability of the chaotic map as core building blocks. This enables the system to maintain a high level of security despite its decentralized architecture. Before the chaotic map can produce a series of numbers that can be said to be truly random and unexpected, a considerable deal of thinking needs to go into the process of building it. This is because randomness and predictability are closely related. [15].

1.3 PROBLEM STATEMENT

The growing use of cloud computing has resulted in the emergence of a new and significant challenge, and that challenge is ensuring the security of data that is stored in the cloud. Even while cloud services encrypt data in order to prevent unauthorized access, older encryption technologies like the Advanced Encryption Standard (AES) can be cracked by hackers. This is because AES was purposefully created to be vulnerable to attack. This is especially true in the event that the keys corresponding to these techniques are also kept on the cloud in some fashion. It is vital to make use of the most up-to-date encryption technology in order to protect the privacy of one's data while it is being stored in the cloud. Only this will ensure that one's information is not viewed by unauthorized parties. This thesis provides a modified version of the AES algorithm as a technique of improving key management and encryption, and thus a method of resolving the security weaknesses that are present in cloud storage and computing environments. There are now a great deal of security holes in the cloud. By employing a hybrid key management technique that combines the most advantageous aspects of symmetric and asymmetric encryption, the most recent version of the AES

algorithm protects the confidentiality of data stored in the cloud in addition to the data's integrity and veracity. The data stored in the cloud are protected using this method. This is only possible thanks to the utilization of asymmetric cryptography, which is what makes this a possibility. To ensure that the ciphertext is actually one of a kind and to make it more difficult for would-be hackers to decode the information, the approach additionally incorporates a random encryption technique. This is done to verify that the ciphertext is truly unique. In order to arrive at a conclusion on the overall performance of the modified AES algorithm, the goal of this thesis is to conduct an inquiry into how effectively and securely it operates in a cloud context. This will allow the conclusion to be drawn on the overall performance of the algorithm. The evaluation will include a comparison of the modified AES technique with standard encryption algorithms such as AES and RSA in terms of security, efficiency, and scalability. Specifically, the comparison will look at how well the modified AES technique protects data. In order to successfully complete these comparisons, the most widely used encryption strategies will be applied. The results of the test will reveal how well the upgraded AES algorithm secures data that is stored in the cloud as well as the confidentiality and safety of cloud-based infrastructures.

1.4 RESEARCH QUESTIONS

Some questions that illustrate the problem discussed in this research:

How does the modified AES approach stack up in terms of security, efficiency, and scalability in comparison to other tried-and-true algorithms such as RSA and AES? In comparison to other, more traditional ways of key management, how much of an improvement in cloud data security may be anticipated from the implementation of a hybrid key management approach that makes use of a modified version of the AES algorithm? How does the randomization of the encryption process in the upgraded version of the AES algorithm guarantee that the ciphertext is truly unique, and how does it prevent assaults such as known plaintext attacks and chosen plaintext attacks? How well does the updated AES algorithm function with the many various components of cloud computing, such as the many distinct cloud service providers, different types of data, and different storage systems? In comparison to traditional encryption methods, how does the updated AES algorithm affect the amount of time required to process data and the number of resources that are consumed by cloud-based systems? In an architecture that is built on the web, how does the modified

AES algorithm address the problem of key management and distribution? The AES algorithm is used to encrypt data that is stored in the cloud. Recent enhancements to this method have lessened a number of dangers, including data breaches, insider assaults, and cyberattacks. Data protection requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) need strict adherence to specified criteria. How does the upgraded AES algorithm guarantee that this will happen in a cloud-based system? The algorithm for the updated AES needs to have some improvements made to it so that it can better defend against potential dangers, such as those posed by quantum computers and machine learning. What other steps can be done to ensure success in this endeavor? When it comes to the identification of users and the control of their access in the cloud, how does the updated AES algorithm affect the usability of the system and the user experience?

1.5 AIMS, OBJECTIVES AND CONTRIBUTIONS

The aim of this thesis is to investigate the effectiveness of a hybrid cryptosystem that combines Advanced Encryption Standard (AES) and Chaotic-map research cryptosystem (CMRC) for secure communication in the presence of various security threats. The thesis aims to address the challenges of existing encryption techniques by proposing a novel hybrid cryptosystem that leverages the strengths of both AES and CMRC to ensure the confidentiality, integrity, and authenticity of data in different applications, such as cloud computing, wireless sensor networks, and Internet of Things (IoT).

Objectives:

a. To conduct a comprehensive literature review of existing encryption techniques and their limitations, particularly in the context of cloud computing, wireless sensor networks, and IoT.
b. To propose a novel hybrid cryptosystem that combines AES and CMRC to address the limitations of existing encryption techniques and ensure the confidentiality, integrity, and authenticity of data in different applications.
c. To develop a prototype implementation of the proposed hybrid cryptosystem and evaluate its performance and security in different scenarios, such as different key sizes, data types, and network topologies.
d. To compare the performance and security of the proposed hybrid cryptosystem with

existing encryption techniques, such as AES, CMRC, and RSA, in terms of throughput, latency, energy consumption, and security level.

e. To investigate the robustness of the proposed hybrid cryptosystem against different security threats, such as side-channel attacks, differential power analysis (DPA), and brute-force attacks, and propose countermeasures to enhance its security.

f. To evaluate the usability and user experience of the proposed hybrid cryptosystem, particularly in the context of IoT and wireless sensor networks, and propose improvements to enhance its usability and user experience.

g. To demonstrate the effectiveness and applicability of the proposed hybrid cryptosystem in different applications, such as cloud computing, wireless sensor networks, and IoT, and provide recommendations for further research and development.

Overall, the thesis aims to contribute to the field of cryptography by proposing a novel hybrid cryptosystem that can provide a higher level of security and performance in different applications. The thesis also aims to advance the understanding of the strengths and limitations of existing encryption techniques and provide insights into the design and implementation of secure communication systems.

2. RELATED WORK

2.1 INTRODUCTION

Cloud computing is a widely used paradigm that allows users to access shared resources, such as computing power, storage, and applications, over the Internet. Cloud computing has many benefits, such as scalability, cost-effectiveness, and flexibility, but it also poses significant security challenges, particularly in terms of data privacy and confidentiality. Cryptography is a critical component of cloud security, as it enables secure communication and data protection. In this literature review, we will discuss the use of state-of-the-art methods for cryptography in cloud computing.

State-of-the-art methods for cryptography in cloud computing:

a. Homomorphic Encryption: Homomorphic encryption is a state-of-the-art encryption technique that allows computation to be performed on encrypted data without decrypting it. Homomorphic encryption enables secure computation and data sharing in the cloud without revealing the underlying data. Homomorphic encryption has many potential applications in cloud computing, such as secure data analysis and secure computation outsourcing. However, homomorphic encryption is still in its early stages of development, and it is not yet widely used in practice due to its high computational overhead.

b. Attribute-Based Encryption: Attribute-based encryption is a state-of-the-art encryption technique that allows access control to be enforced on encrypted data. Attribute-based encryption enables fine-grained access control in the cloud by encrypting data based on attributes, such as user roles and permissions. Attribute- based encryption has many potential applications in cloud computing, such as secure data sharing and outsourcing. However, attribute-based encryption is still in its early stages of development, and it is not yet widely used in practice due to its complexity and scalability issues.

c. Searchable Encryption: Searchable encryption is a state-of-the-art encryption technique that allows search queries to be performed on encrypted data without revealing the underlying data. Searchable encryption enables secure data search and retrieval in the cloud without compromising data privacy. Searchable encryption has many potential applications in cloud computing, such as secure data sharing and outsourcing. However, searchable encryption is still in its early stages of development, and it is not yet widely

used in practice due to its high computational overhead and security limitations.

d. Proxy Re-Encryption: Proxy re-encryption is a state-of-the-art encryption technique that allows an intermediate party to transform encrypted data from one key to another key without revealing the underlying data. Proxy re-encryption enables secure data sharing and outsourcing in the cloud by allowing data owners to delegate access to their data without compromising data privacy. Proxy re- encryption has many potential applications in cloud computing, such as secure data sharing and outsourcing. However, proxy re- encryption is still in its early stages of development, and it is not yet widely used in practice due to its complexity and scalability issues.

2.2 RELATED WORKS

[7] is a paper that delves into the topic of encrypting the data that is stored in the cloud.

[1] This study's objective is to gain an understanding of the cryptographic methods that are available to ensure the confidentiality of files even while they are being stored in the cloud. This will be accomplished by gathering relevant information. In this piece, we will discuss asymmetric and symmetric techniques, which are two of the most common approaches to encrypting and decrypting information, respectively. Asymmetric techniques were developed in the 1960s, and symmetric techniques were developed in the 1970s. This article provides a step-by-step guide to encrypting data using the AES and DES methods. The steps are presented in the order in which they should be performed. The RC-2 Encryption Algorithm is yet another of the methods that are going to be covered in this article. [8] and

[2] collaborated on the writing of an article that was published under the title "Data Security in Cloud Computing Using AES." In this piece, we will go over the potential risks that are associated with utilizing cloud computing, as well as the preventative measures that can be implemented to eliminate those potential risks. An implementation of the Advanced Encryption Standard (AES) was developed as a data security algorithm, and a website serving as an application for data security was developed at the same time as the paper that discussed the use of AES for data security in cloud computing. In the context of the HEROKU cloud, both of these were brought up for discussion. Research and Design of Cryptography Cloud framework [3] was the title of a paper that was published in [9], and it discussed the various cryptographic frameworks that are used in cloud computing. The paper was titled Research and Design of Cryptography Cloud framework.In addition, they discussed the utilization of public and private keys for the purposes of encryption and decryption, as well as the operation of a virtualization

cryptography machine (VCM), as well as the various strategies that are utilized to guarantee the safety of data that is stored in the cloud. This is a research paper that goes into great detail about cloud cryptography. It covers everything from its design and implementation to the function that virtual cryptographic machines (VCMs) play in the process. Which business provides services that are associated with cryptography? In addition, a framework for CC is proposed, which gives the impression that the authors intend to provide users with cryptographic services that are in line with the cloud computing model. This is the result of the work that was done by Ahmad.S.A., whose paper titled "Hybrid Cryptography Algorithm in cloud computing"[4] discussed the use of a hybrid approach, also known as the combination of two different encryption techniques, in order to increase the level of safety that the data has. This was done in order to improve the level of safety that the data has. At a time when data malfunctions are becoming an increasingly common occurrence, this hybrid approach is an innovative method for protecting sensitive data. In his review paper, he discussed not only the methods that he himself had used, but also the methods that had been used by other researchers. In other words, he didn't just talk about the methods that he had used. Because of this, we were able to form a more comprehensive understanding of cryptographic algorithms. This article provides a comprehensive analysis that compares and contrasts a number of different hybrid approaches. Pandey suggested they write a paper with the working title "Data Security in Cloud-Based Applications." In this paper [5,] which can be found here, he discussed the security threats that we are currently up against. Located here. He suggested employing the AES method as a means of resolving the problem as a means of finding a solution. An algorithm for a block cipher that makes use of private keys is referred to as the Advanced Encryption Standard (also abbreviated as AES). Within the scope of this study, each and every facet of the AES procedure was dissected and dissected into its component parts. In it, he also discussed the three security patterns that are required to deliver adequate data protection. This was included in the aforementioned document. Filtering, encryption, and permission are the three security patterns that make up this pattern. An algorithm with the abbreviation "Enhanced Mutual Trusted Access Control Algorithm" (EMTACA) was suggested in the aforementioned reference number [10]. [6] Customers who use cloud services and cloud service providers both benefit from the use of this method, which makes them feel more secure when using cloud services. This article provides evidence that the confidentiality, integrity, and availability of data were all preserved, which are the three pillars of data security that are considered to be of the utmost significance. The purpose of this paper is to make a suggestion for a system that incorporates the EMTACA algorithm, which has the potential to improve reputation-based, guaranteed, and trusted cloud services for users who are working in an environment that makes use of cloud computing. The authors of [11] express their concerns regarding the security of storing data in the cloud. There are some suggestions provided in order to strengthen the protection afforded to

cloud-based databases. This method utilizes multiple encryption algorithms, such as Triple Data Encryption Standard (DES), an arbitrary number generator (Random Number Generator), and RSA, in order to achieve a higher level of security; however, as a direct consequence of this, the method's performance is negatively impacted. The authors of "12" arrive at the conclusion that a hybrid algorithm might be able to partially meet these criteria, which they state as a possibility in their conclusion. The research conducted by the authors is centered on determining how something like this could be accomplished during the transfer of extremely sensitive data, such as information pertaining to the military or financial transactions. We were able to avoid the problems that are normally associated with RSA Security by employing a hybrid strategy for the protection of the data stored in the cloud(13).

Both the RSA and the Feistel Cipher Algorithm were put to use during both of the phases of the encryption procedure. The risk of a man-in-the-middle attack has been significantly mitigated as a direct result of the application of two separate algorithms across two separate stages of the process. In [14], it is suggested that the use of encryption during transmission can help to alleviate some of the concerns regarding the disclosure of data. This makes use of both the RSA algorithm and the hash function to ensure that data is only transmitted over the channel in an encrypted form. RSA is an acronym for the Secure Authentication and Key Exchange. It is possible to differentiate between various encryption algorithms based on the degree to which they protect data from being stolen or compromised in some other way, as well as the rate at which they carry out their tasks and the level of efficiency with which they do so. Both symmetric and asymmetric key algorithms are viable options for data encryption while it is being transmitted, and both are just as effective as the other. Within the context of both the Traditional Algorithms and the Proposed Algorithms, the authors of [15] examined the benefits and drawbacks of both Symmetric Key Cryptography and Asymmetric Key Cryptography. This was done in the context of both sets of algorithms. They have also conducted an evaluation of the effectiveness of the cryptanalysis methods that have been used. Blowfish, RSA, Advanced Encryption Standard (AES), and Data Encryption Standard (DES) are among the encryption algorithms that have been evaluated to determine which one provides the highest level of security for cloud data. At this very moment, the outcomes of these examinations are being analyzed. [14] and [16] present a demonstration of an evaluation of symmetric and asymmetric algorithms, with the primary focus being on the evaluation of symmetric algorithms. The purpose of this analysis is to determine which algorithm should be applied to cloud-based applications and services that call for the encryption of link data. This article provides a concise comparative outline and comparison of cryptographic algorithms, with a particular emphasis on the Symmetric approach that should be used for Cloud-based applications and services that require link data and encryption. In particular, the article focuses on how this approach should be implemented. In addition to that, a comparison

of the various cryptographic algorithms is included in the paper. The most important difference between AES and DES is discussed in [17], along with the limitations of AES. You'll find the comparison discussed here in the same section. The inference that can be made is that AES might be easier to implement in either low-level or high-level programming languages. This is the conclusion that can be drawn. Blowfish, Advanced Encryption Standard (AES), and Data Encryption Standard (DES) were the three symmetric-key cryptography algorithms that were evaluated and compared in terms of their performance in [28]. The performance of the algorithms in a variety of different settings was evaluated by taking into account how they responded when presented with a diverse set of data loads. This allowed for an accurate assessment of how well the algorithms performed in each of the settings. In the study that is outlined in [18], a comparison of the efficiency of various encoding and decoding algorithms was carried out on hardware that exhibited a variety of processing speeds. This was done in order to determine which algorithm was the most effective. In addition, the size of the file was changed in order to guarantee that the results would be reliable. It has been demonstrated that the AES (Rijndael) algorithm has the highest throughput and the quickest execution time when compared to other hardware processors. This is the case because the algorithm uses the Rijndael cipher.

2.3 CONCLUSION

Cryptography plays a critical role in cloud security, and there are various traditional and state-of-the-art methods that can be used to secure cloud computing environments. Traditional methods, such as AES and RSA, are widely used and studied, and they are considered secure for cloud computing applications. State- of-the-art methods, such as homomorphic encryption, attribute-based encryption, searchable encryption, and proxy re-encryption, offer many potential benefits, but they are still in their early stages of development, and further research is needed to improve their efficiency, scalability, and security. Future works should focus on developing hybrid methods that combine the strengths of traditional and state-of-the-art methods to provide

3. MATERIALS AND METHODS

3.1 INTRODUCTION

This chapter provides an introduction to the idea of cloud computing and a discussion of the current security concerns that influence data that is networked and stored on the cloud. Lightweight cryptography and the associated cryptographic systems are broken down in detail, along with their definitions and some brief explanations.

3.2 CLOUD COMPUTING

The concept of cloud computing refers to the utilization of a decentralized network of remote servers, as opposed to storing, administering, and processing data and applications on a local server or on an individual computer. Cloud computing, in its most basic form, refers to a concept that enables on-demand, internet-based access to a variety of information technology services and resources, including servers, data storage, databases, programs, and applications. The widespread use of cloud computing has resulted in a shift in the manner in which individuals and businesses make use of available computing resources:

a. Scalability: Cloud computing enables businesses to scale up or down their computing resources depending on their needs. This allows them to respond quickly to changes in demand and avoid overprovisioning or underprovisioning their resources.
b. Cost-effectiveness: Cloud computing enables businesses to save costs on hardware, software, and infrastructure by outsourcing their computing needs to cloud providers. Cloud providers typically charge based on usage, which allows businesses to only pay for what they need.
c. Flexibility: Cloud computing enables businesses to access their computing resources from anywhere with an internet connection. This allows employees to work remotely and collaborate in real-time from different locations.
d. Reliability: Cloud computing enables businesses to access high-quality computing resources that are managed and maintained by cloud providers. Cloud providers typically have redundant systems and backup facilities to ensure high availability and data protection.

e. Security: Cloud computing enables businesses to access secure computing resources that are protected by encryption, firewalls, and other security measures. Cloud providers typically have dedicated security teams and compliance standards to ensure the confidentiality, integrity, and availability of their customers' data.

f. The three most common categories of cloud services are:

g. Infrastructure as a Service (IaaS): IaaS offers remote access to physical or virtual servers, storage, and networking components. The cloud allows users to host and administer their own servers, apps, and services.

h. Second, Platform as a Service (PaaS) is a service that allows you to build, test, and release software in the cloud. Users can focus on application development and deployment instead of worrying about the underlying technology stack.

i. Third, SaaS (Software as a Service) delivers programs via the web. Software applications can be accessed and used by users without requiring users to install or manage any software on their own devices.

Cloud computing also has some challenges, including data privacy and security concerns, vendor lock-in, and regulatory compliance issues. However, these challenges can be mitigated by implementing appropriate security measures, selecting reliable cloud providers, and ensuring compliance with data protection regulations.

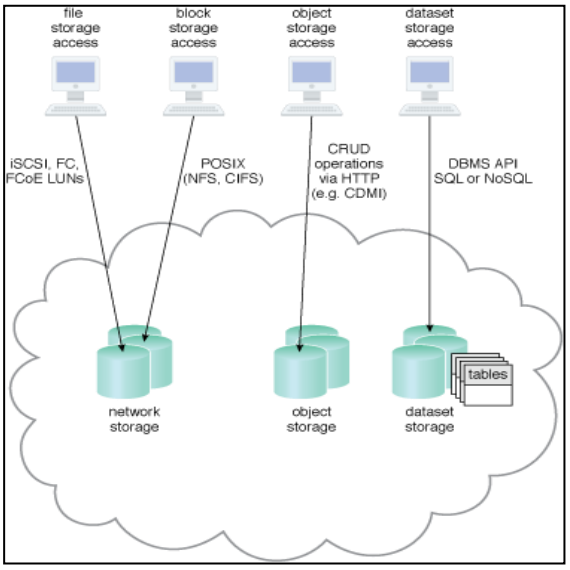

Figure 3. 1: Cloud Computing Mechanism [11].

3.2.1 Cloud Computing Characteristics

Cloud computing has several characteristics that distinguish it from traditional computing. The key characteristics of cloud computing are:

Advantage #1: Users may access servers, storage, and apps whenever they need them without having to wait for or contact with cloud service providers. Users can allocate and reallocate resources on demand, and they'll only be charged for what they really utilize.

Second, users may access their data and programs from any location with an internet connection and a variety of mobile devices thanks to cloud computing.

Thirdly, cloud computing enables cloud service providers to pool computing resources like servers, storage, and networks in order to allocate those resources in a way that is both efficient and flexible. In this way, people can safely share the same space without compromising their own safety.

The ability to swiftly and easily increase or decrease the amount of available computer resources in response to fluctuations in demand is a key benefit of cloud computing. Because of this, companies can respond rapidly to shifts in demand and avoid either over- or under-allocating resources.

Cloud computing's metered service means that users only pay for the processing power they actually consume. Businesses may now better manage their finances and expenses as a result of this.

To guarantee high availability and data security, cloud computing employs redundant systems and backup facilities, providing a high level of resilience. This allows companies to safeguard their data and apps against loss and make a full recovery in the event of a disaster.

Cloud computing's multi-tenancy feature enables numerous users to safely and securely share the same set of hardware resources. This allows cloud service providers to make better use of their resources while keeping costs down for their customers.

Cloud computing's SLA ensures a predetermined threshold of uptime, performance, and safety for its users. This lets organizations check in with their cloud service providers to make sure they're delivering the promised level of service and hold them to their word when they don't.

For these reasons, cloud computing has emerged as a viable alternative to more

conventional methods of data processing. The ability to swiftly and easily increase or decrease the amount of available computer resources is a major benefit of cloud computing for organizations. This helps to keep their applications and data available and recoverable at all times.

3.2.2 Computer Cloud Deployments

The term "computer cloud deployments" is the one that is intended to be used when referring to the process of putting resources from cloud computing to use and administering them. In order to better understand cloud deployments, we may break them down into three distinct categories, which are as follows: A "public cloud deployment" is the situation in which a cloud service provider makes its servers, data storage, and software accessible to anybody who has access to the internet. This type of deployment is known by the name "public cloud deployment." This deployment model is also sometimes referred to by the phrase "open cloud." If the user has access to the internet, they are able to make use of shared server space and other computer resources from any location; however, they will only be charged for the amount of time that they spend making use of these services. Users of a public cloud don't need to be concerned about the underlying infrastructure because the cloud provider is the one who controls and maintains it. Users of a private cloud do need to be concerned about the underlying infrastructure. One of the most prevalent sources of annoyance among cloud customers is eliminated as a result of this change. In the field of cloud computing, an infrastructure is said to be a "private cloud" when it serves the needs of just one organization and all of the cloud's resources are utilized by that one business. This is due to the fact that only one business is making use of the cloud's accumulated resources. This particular type of cloud is referred to as a "private cloud" by its common name. It is possible for the IT staff of an organization or an external provider to oversee the construction and maintenance of a private cloud, regardless of whether the private cloud is housed on-premises or in a data center. It does not matter where the private cloud is physically located, as this is always the case. In addition to enabling more detailed administration of data and computing resources, private cloud deployments provide superior flexibility and security options than their public cloud equivalents do. The cost of using private clouds is typically much higher than that of public ones. Hybrid cloud deployments, in which public and private cloud resources are used together, are becoming an increasingly popular choice for modern organizations to

serve the computing needs of their customers. These deployments combine public and private cloud resources. When it comes to scalability, adaptability, and security, hybrid cloud deployments provide businesses the best of both public and private cloud environments in one convenient package. Hybrid cloud deployments provide organizations with the best of both public and private cloud settings. This is due to the fact that hybrid cloud deployments integrate the best aspects of both public and private cloud operating systems. For example, a firm might store and operate data and applications that are not as sensitive on the public cloud, while the organization's more sensitive information would be stored and run on a private cloud.

Because of this, the company would be in a position to make use of both of the many cloud storage options that are currently accessible. In addition, cloud installations can be categorized in accordance with the services that they offer, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), in that order. IaaS, which stands for infrastructure as a service, is a paradigm of service delivery that enables cloud service providers to virtualize a wide variety of computational resources and make them available to their clients. This style of service delivery is referred to as "the cloud." These resources include not only servers but also storage space and network connections as well. "platform as a service," sometimes abbreviated as "PaaS," refers to the fact that cloud service providers make available a platform that may be used for the development, testing, and distribution of software. This concept is also abbreviated as "PaaS." "platform as a service" is what "PaaS" refers to when written out as an abbreviation.

In a SaaS deployment, cloud providers offer software applications over the internet. Choosing the right cloud deployment model depends on an organization's computing needs, security requirements, and budget. Public cloud deployments are ideal for organizations that require scalability, flexibility, and cost-effectiveness. Private cloud deployments are ideal for organizations that require greater control over their computing resources and data. Hybrid cloud deployments are ideal for organizations that require a combination of public and private cloud resources to meet their computing needs.

3.2.3 Cloud computing service models

Figure 3.2 illustrates how cloud computing deployment can be conceptualized into three distinct levels, each of which is further detailed below:

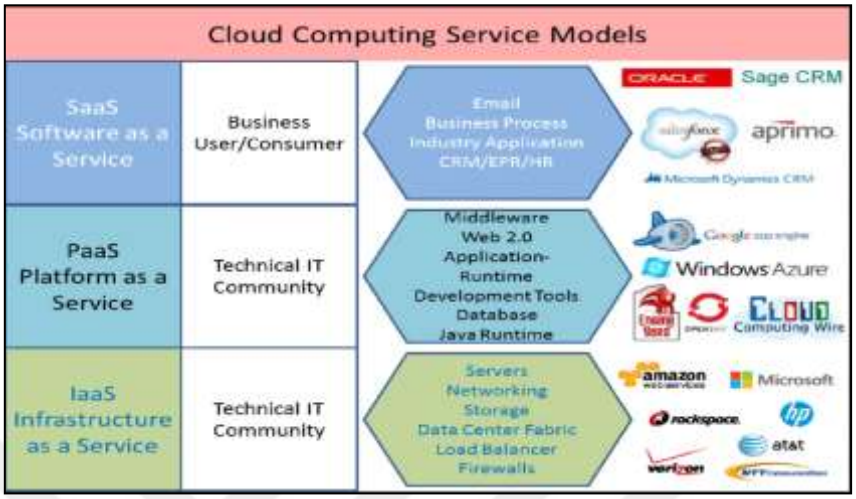

Figure 3. 2: Cloud Computing Service Models [21].

The service model of a cloud provider is the framework that the provider employs in order to categorize the many cloud services that they make available to their clientele as well as the manner in which those services are structured. The delivery of cloud services can often be broken down into one of three primary models, which are as follows: The acronym "IaaS" refers to "infrastructure as a service." Customers have access to virtualized server farms, data centers, and networks when they use a platform known as Infrastructure as a Service (IaaS). When utilizing a cloud platform, users have the ability to configure and manage their own applications and services in their own environments. When users make use of Infrastructure as a Service (IaaS), they are provided with a significant amount of flexibility over the process of constructing and personalizing the computing environments that they work in. Companies that provide infrastructure as a service include the likes of Amazon Web Services, Microsoft Azure, and Google Cloud Platform, amongst a great deal of other options. A technology known as "Platform as a Service" (PaaS) is what makes it possible to design apps that run on the Internet, test those applications, and then finally deploy such applications. Customers are freed from the burden of worrying about the underlying infrastructure, allowing them to devote their full attention to the process of developing and distributing applications. The vast majority of companies that supply PaaS to businesses also provide their clients with databases, middleware, and development environments that are preconfigured and ready to

use right away. PaaS gives its users a great level of flexibility and variety, which makes it easy for them to develop and deploy new apps. PaaS also makes it possible for them to do so with minimal effort. Heroku, IBM Cloud, and Oracle Cloud Platform are just a few examples of companies that offer platform-as-a-service to its customers. The term "software as a service," also abbreviated as "SaaS," refers to a model in which users obtain access to software through a subscription-based model. Customers are able to make use of the program without having to download it, set it up, or keep it maintained on their end. All of these tasks are handled by the service provider. SaaS providers make available a wide variety of software goods, including e-mail, apps to enhance productivity, and platforms for customer relationship management. These are only some of the software products that may be accessed. SaaS provides customers with a high degree of convenience and accessibility, allowing them to access software applications from anywhere with an internet connection. Examples of SaaS providers include Salesforce, Google Workspace, and Microsoft Office 365. Choosing the right cloud service model depends on an organization's computing needs, expertise, and budget. IaaS is ideal for organizations that require a high degree of control over their computing resources and want to customize and configure their systems as needed. PaaS is ideal for organizations that want to develop and deploy applications quickly and easily without worrying about the underlying infrastructure. SaaS is ideal for organizations that want to access and use software applications without having to manage them on their own devices [24].

3.3 CLOUD COMPUTING SECURITY

The term "cloud computing security" refers to the collection of safeguards and protocols that are put into place in order to shield cloud computing systems, applications, and data against unauthorized access, data breaches, and other types of cybercrime and other security concerns. Cloud computing security is also referred to as "cloud computing safety." Security in cloud computing is a very serious topic because to the large volumes of sensitive data that are stored in environments that are referred to as "the cloud." As a direct consequence of this, cloud-based computer systems are regularly the targets of malicious cyberattacks. The following is a list of some of the most essential issues of cloud computing security, in the order of their importance:

Safeguarding of Data The protection of data in cloud computing is an essential component of the service's comprehensive security, but it is also one that is frequently neglected. Cloud service providers employ a variety of security measures, including encryption, access controls, and other safeguards, in order to prevent data from being accessed in an unauthorized manner and from becoming compromised. Businesses need to take further steps and implement additional security protocols, such as multi- factor authentication, in order to guarantee the integrity of their data and prevent it from being compromised. The Administration of Identities and Requests for Access: IAM stands for "identity and access management," which refers to the process of regulating and managing access to cloud resources. This approach is also abbreviated as "IAM." IAM ensures that only approved users are able to access cloud resources and that those authorized users' access is restricted to only the resources that they require. IAM also ensures that only authorized users are able to access cloud resources. IAM also allows businesses the capacity to monitor and keep track of user actions, which enables them to identify and prevent unwanted access to their systems. Security of the Network: Network security is an additional crucial component of cloud computing safety. Cloud service providers protect the cloud network from any potential cyberattacks by putting in place a variety of security precautions, including firewalls, intrusion detection systems, and other preventative measures. When it comes to the matter of safeguarding their network connections to the cloud, businesses are required to take further care and implement additional security measures such as virtual private networks (VPNs). Compliance & rules: Cloud service providers are obligated to adhere with a range of regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), in order to safeguard the personal information and privacy of its clients. In order for businesses to avoid the risk of facing legal and financial penalties, it is necessary for them to ensure that the cloud service providers that they contract with meet all of the prerequisites. Reconstruction after Disasters and the Continuity of Operations in Businesses The security of cloud computing needs to take into consideration issues relating to disaster recovery and business continuity. Cloud service providers frequently offer backup and recovery services as a preventative measure against the loss of data in the event of a cataclysmic event or an extended power outage. This is done as a safety measure. In addition to developing and putting into action business continuity and disaster recovery plans, companies should do so in order to ensure that their

operations can continue even in the case of an interruption. In a nutshell, the purpose of cloud computing security is to prevent unauthorized access to cloud computing systems, applications, and data while also preventing data breaches. This can be accomplished by installing a number of technical protections, in addition to policies and processes. To ensure the data they store in the cloud is kept private and prevent unwanted access to it, it is imperative for organizations to implement a comprehensive security policy that addresses all aspects of cloud computing security. Only then can they be sure that their data is protected. These security domains can be connected with additional service delivery modules that contain all security concerns for the infrastructure, including the network, host, and application layers, as shown in Figure 3.3 of the Computing Security Architecture for the Cloud. This is possible thanks to the cloud's modular design. [26].

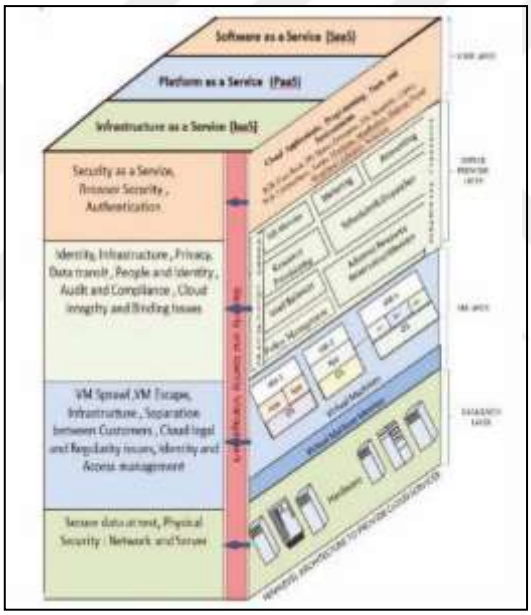

Figure 3. 3: Cloud Computing Security Architecture[26].

3.4 CHAOTIC MAP

Mathematical models that represent the behavior of complex systems over the course of time are called chaotic maps. These models are sometimes referred to as nonlinear dynamical systems. Nonlinear maps are chaotic maps that do not follow a linear relationship between the variables that are input and the variables that are output. Instead, chaotic maps display behavior that is convoluted and hard to predict. This behavior is very sensitive to the system's initial conditions and to even minute disturbances. It is common practice to construct chaotic maps using discrete-time iterative equations, which are used to chart the

development of a system over a period of time. The equations contain a number of variables and factors that are responsible for determining how the system will behave. The distinctive qualities of chaotic maps, such as sensitivity to beginning conditions, non-periodicity, and topological mixing, are what distinguish them from other types of maps. The trait of chaotic maps known as sensitivity to beginning circumstances describes the phenomenon in which seemingly insignificant shifts in the parameters of the system at the outset can have a significant impact on the ultimate result. This attribute is commonly referred to as the "butterfly effect," and it describes a phenomenon in which the flapping of the wings of a butterfly in one area of the planet can potentially generate a storm in another part of the world. Non-periodicity is a feature of chaotic maps that describes the way in which the system does not repeat itself in a predictable fashion over the course of time. This is in contrast to the behavior of periodic systems. Instead, chaotic maps display a behavior pattern that is convoluted, erratic, and difficult to forecast. The term "topological mixing" is used to describe a characteristic of chaotic maps in which the system displays complicated and unpredictable behavior that mixes together several regions of the state space. This phenomenon is frequently referred to as a "smoothing" of the state space, which describes the process by which various regions become indistinguishable over the course of time. Applications of chaotic maps can be found in a variety of domains, including physics, engineering, economics, and encryption, among others. In the field of cryptography, chaotic maps are put to use for a variety of purposes, including the generation of random numbers and the encryption and decryption of data. Due to the unpredictable nature of their behavior, chaotic maps are an excellent tool for the development of safe encryption algorithms that are resistant to attack. In general, chaotic maps are effective mathematical models that can be used to represent the behavior of complicated systems throughout the course of time. Because of their one-of-a-kind characteristics, they can be put to use in a variety of contexts, including cryptography [27].

3.5 HYBRID TECHNIQUE

Combining the strengths of symmetric and asymmetric encryption, hybrid cryptography is a method that may encrypt and decrypt data in a manner that is not only more secure but also more effective. This is accomplished by utilizing a cryptographic approach known as hybrid cryptography. In hybrid cryptography, the data is encrypted using a symmetric encryption

method, and the symmetric key that is used for encryption is sent securely using an asymmetric encryption algorithm. This enables the data to be kept private while it is being transmitted. The following activities are typically included in the process of hybrid cryptography:

a. Key generation: It is the sender's responsibility to provide a symmetric encryption key, which is subsequently used in the process of encrypting the data.
b. In addition, in order to execute asymmetric encryption, the sender will supply a pair of keys, one public and one private, to the recipient. The data is encrypted when the sender applies the symmetric encryption key to the data before sending it. This happens before the data is sent.
c. Encoding of the secret key the symmetric encryption key is then encrypted by the sender with the recipient's public key using symmetric encryption. This ensures that no one other than the receiver, who owns the associated private key, is able to access the encrypted content or decrypt the symmetric key in order to read it. The recipient is the only one who possesses the private key.
d. The data will be transmitted, and the sender will provide the recipient with both the encrypted data and the encrypted symmetric key.
e. Decryption of the data takes place when the recipient uses their own private key to decrypt the symmetric encryption key. After that, they decrypt the data by using the symmetric key that they previously decrypted. When compared to employing either symmetric or asymmetric encryption on their own, hybrid cryptography offers a number of benefits. However, in order to encrypt vast volumes of data quickly and effectively, symmetric encryption calls for the safe exchange of the encryption key.

Symmetric encryption is both faster and more efficient. Asymmetric encryption is less efficient than symmetric encryption when it comes to encrypting huge volumes of data, but it is more safe due to the fact that it requires two separate keys. Hybrid cryptography is a method that encrypts and decrypts data using two different approaches, yet the result is a system that is both more safe and more efficient. It makes it possible to encrypt vast volumes of data quickly and easily using symmetric encryption, while at the same time ensuring that the exchange of encryption keys is carried out in a secure manner using asymmetric encryption. As a consequence of this, hybrid cryptography is frequently utilized in programs that require both efficacy and security, such as online transactions and secure communication

conducted over the internet. [28].

3.6 DATA CLASSIFICATION

Data classification in cloud computing cryptography is the process of categorizing data based on its sensitivity level or importance. Data classification is an important aspect of cloud computing security because it helps organizations determine the appropriate level of protection needed for their data and enables them to implement the necessary security measures. The following are some common data classification categories: Public Data: Public data refers to data that is intended for public consumption, such as marketing materials, press releases, and public announcements. Public data does not require any special security measures and can be freely shared with anyone. Internal Data: Internal data refers to data that is used within an organization, such as internal reports, memos, and documents. Internal data may contain sensitive information that is not intended for public consumption but does not pose a significant risk to the organization if it is compromised. Confidential Data: Confidential data refers to data that is highly sensitive and requires strict security measures, such as financial data, personally identifiable information (PII), and intellectual property. Confidential data must be protected from unauthorized access, and access to it must be restricted to only authorized personnel. Restricted Data: Restricted data refers to data that is highly sensitive and requires the highest level of security measures, such as classified government data, trade secrets, and highly sensitive personal information. Restricted data requires strict access control measures, including physical and logical security controls, and must be protected from unauthorized access at all times. Data classification is important in cloud computing because it enables organizations to determine the appropriate level of security measures needed to protect their data. For example, public data may not require any special security measures, while confidential and restricted data require strict access control measures, encryption, and other security measures to ensure their confidentiality and integrity., Figure 3.4 shows Architecture of data classification [29].

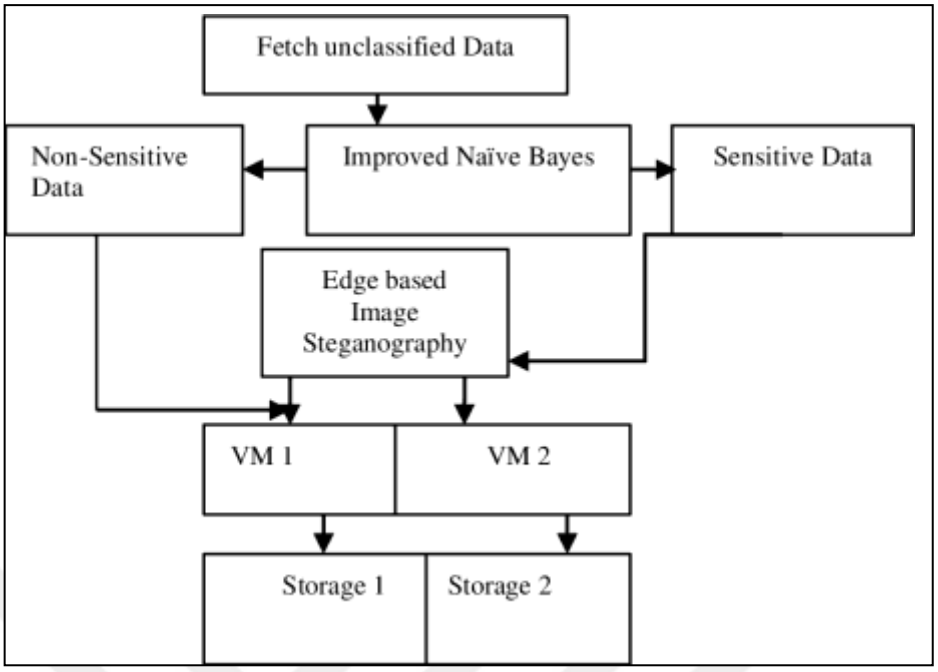

Figure 3. 4: Architecture of Data Classification Application [29].

Classifying data entails determining how important various pieces of information are, how they should be protected, and where they should be kept. [30].

3.7 RELEVANT CRYPTOGRAPHIC SYSTEM BACKGROUND

This section provides a brief description most common data encryption techniques, first DES, 3DES, BLOWFISH then the AES cryptosystem as it adapts to the proposed AES/chaotic-map cryptosystem as it is inspired by it.

3.7.1 Des

The Data Encryption Standard (DES) is an algorithm for symmetric-key encryption that was initially developed by IBM in the 1970s. It was named after the acronym for the acronym for Data Encryption Standard. The acronym for the Data Encryption Standard inspired the naming of this standard's acronym. The National Institute of Standards and Technology (NIST), which can be found in the United States of America, was ultimately the organization that was responsible for standardizing the Data Encryption Standard.

The Data Encryption Standard (DES) is a well-known method that is used for the purpose of encrypting data in order to keep it from being accessed by unauthorized parties. The goal of this protection is to prevent the data from being read by these parties. This is done with

the intention of ensuring the security of the data. The Data Encryption Standard (DES) is a technique for encrypting and decrypting data. It operates on data blocks that are 64 bits long and requires a key that is 56 bits long in order to encode and decrypt data. Multiple iterations of a pair of mathematical processes called as substitution and permutation are required for the process of encrypting data. Both the data that is supposed to be encrypted and the key are subjected to these actions before encryption can begin. Both the size of the key that is being used and the technique of encryption that is being applied can have an effect on the number of rounds of operations that are required to decrypt a message. [C]ombining these two factors can reduce the amount of time needed to decipher a message. The Data Encryption Standard (DES) is currently utilized in a vast variety of applications, some of which include, but are not limited to, monetary transactions, data storage, and communication networks. Other applications that make use of DES include medical records, government documents, and classified information. However, due to developments in computer power as well as an increase in the number of threats to data security, the DES encryption algorithm's security has been compromised, and it is no longer recognized as a secure encryption method. This is because of the fact that there has been an increase in the number of threats to data security. This is as a result of the interaction of these two elements working together. The Data Encryption Standard (DES), also known as the Advanced Encryption Standard (AES), is a technique of encryption that was developed as a direct response to the complaints that were raised against the DES. This approach is notable for the improved level of safety that it provides. Advanced Encryption Standard, often known as AES, is a more secure technique of encryption than Data Encryption Standard, also known as DES. This is due to the fact that AES employs a block size of 128 bits and a variable key size of 128, 192, or 256 bits. The Advanced Encryption Standard (AES) has supplanted the Data Encryption Standard (DES) as the go-to encryption method in a wide variety of applications worldwide. DES was the previous encryption method of choice. Encrypting data via a system such as the Data Encryption Standard (DES) is a standard method that can be utilized to reduce the likelihood of unauthorized individuals gaining access to sensitive information. The Data Encryption Standard (DES) is a method of cryptography that encrypts data with symmetric keys. This method was developed in the 1970s. The Data Encryption Standard (DES) was formerly thought to be a trustworthy method of encryption; however, this impression has shifted in recent years as computing power has expanded and new

security issues have surfaced. A direct result of this is that it has been supplanted by encryption schemes that provide a higher level of protection, such as the Advanced Encryption Standard (AES) [32]. Figure 3.5 demonstrates that each cycle is composed of three distinct operations: substitution, transposition, and exponentiation. These operations are performed in the order given.

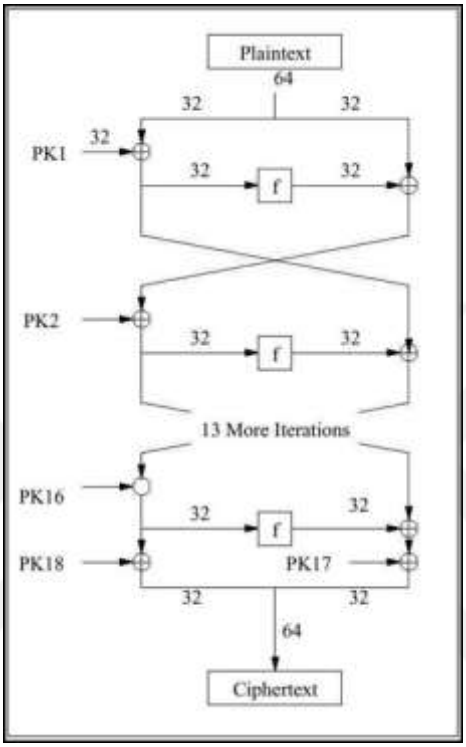

Figure 3. 5: Encryption DES [31].

3.7.2 3Des

The Data Encryption Standard (DES) algorithm serves as the basis for the Triple Data Encryption Standard (3DES), a method for symmetric-key encryption that was developed as a variation of DES. 3DES was designed as a mechanism for encrypting data using three identical keys. The DES algorithm was modified in order to create the 3DES technique. The data encryption process of 3DES goes through three rounds of the DES method, which enables it to deliver a higher level of safety than its predecessor, DES. This was made possible by the fact that 3DES was able to go through three rounds of the DES method. Due to the fact that 3DES is an upgraded version of the DES algorithm, this was finally able to be accomplished. To ensure the confidentiality of sensitive data, the 3DES encryption technique protects information with a block size of 64 bits and a key size of 168 bits. After then, the key is subdivided into three distinct keys, each of which has a length of 56 bits, and

these keys are then utilized in a method that is known as triple encryption. The first key is used to encrypt the data with the DES algorithm using the first 56 bits of the key, the second key is used to decode the data that has been encrypted, and the third key is used to encrypt the data that has been decoded using the first two keys. The data protection that is offered by this method of triple encryption is superior to the data protection that is provided by the DES, which only makes use of a single method of encryption. The DES only encrypts data in one of two ways: using a key that is only known to the user and by the server. The data encryption standard known as 3DES is used in a wide variety of applications, some of which include the storing of data, communi cationnetworks,and financial transactions. Other applications include protecting data transmissions over the internet. However, due to the fact that 3DES is a method of encryption that is both slower and less efficient than more contemporary encryption algorithms like as Advanced Encryption Standard (AES), its use is progressively being phased out in favor of AES in a variety of applications. This is because 3DES is a technology that was developed in the early 1990s and has not been updated since then. The Data Encryption Standard (DES) algorithm serves as the basis for the Triple Data Encryption Standard (3DES), a method for symmetric-key encryption that was developed as a variation of DES. 3DES was designed as a mechanism for encrypting data using three identical keys. The DES algorithm was modified in order to create the 3DES technique. When encrypting data with this method, the Data Encryption Standard (DES) algorithm is repeated three times. Each iteration adds another layer of security. The level of safety provided by this method is superior to that provided by the Data Encryption Standard (DES). On the other hand, when compared to more modern encryption methods like the Advanced Encryption Standard (AES), it is both slower and less efficient than those more modern techniques. [32]. Figure 3.6 demonstrates that each cycle is composed of three distinct operations: substitution, transposition, and exponentiation. These operations are performed in the order given.

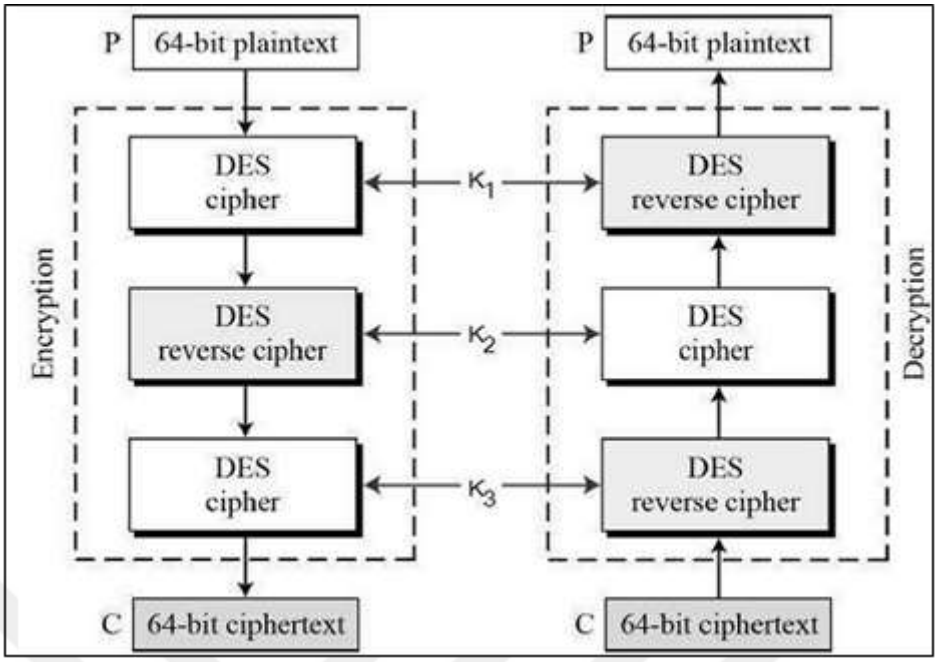

Figure 3. 6: The Diagram of 3DES Encryption/Decryption Implementation [33].

3.7.3 Blowfish

Bruce Schneier developed the Blowfish algorithm for a symmetric block cipher in 1993. Blowfish was named after him. Encrypting data with the Blowfish algorithm helps to prevent unauthorized access to the information that has been encrypted. This algorithm is used extensively. The key length for Blowfish can vary anywhere from 32 bits to 448 bits, depending on the user's preferences. The process of encrypting data comprises a number of operations known as substitution and permutation, which are carried out on both the data to be encrypted and the key. Blowfish employs a 16-round Feistel network and processes data in blocks that are 64 bits in length. Blowfish is superior to other encryption algorithms in a number of respects, including its ability to use keys of varying lengths, its straightforward and effective design, and its speed when encrypting and decrypting data. Blowfish is another cryptographic algorithm that is widely regarded as exceptionally secure and is not known to have been vulnerable to any assaults. Blowfish is a cryptographic algorithm that has found widespread use in a variety of applications, such as network security, file encryption, and password protection. Blowfish, on the other hand, is being gradually replaced by more modern encryption algorithms such as Advanced Encryption Standard (AES). This is happening because there are an increasing number of security concerns, and there is a need for stronger encryption methods. Data can be encrypted with the symmetric block cipher

algorithm known as Blowfish, which helps to prevent unauthorized access to the data that has been encrypted. For the purpose of data encryption, it employs a key ofvariable length in conjunction with a number of substitution and permutation procedures. Blowfish is an encryption technique that is believed to be very secure and has various advantages over other encryption algorithms. These advantages include a key that may be of varying lengths, a design that is straightforward and effective, and a swift rate of encryption and decryption [32]. Specifically, as shown in Figure 3.7.

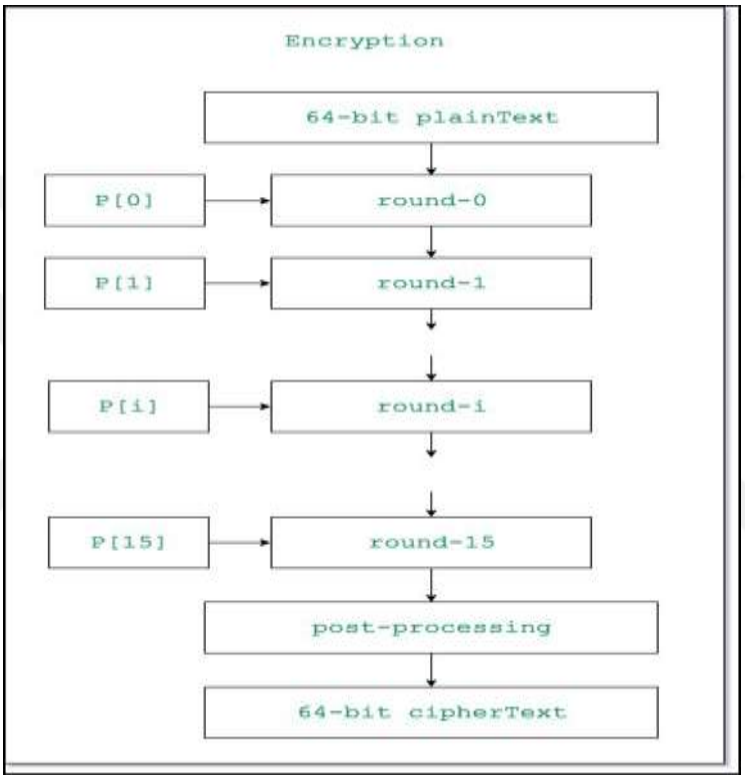

Figure 3. 7: Blowfish Algorithm [32].

3.7.4 Aes

The Advanced Encryption Standard, more frequently referred to as AES and in some circles referred to as just AES, is a method for symmetric-key encryption that is commonly deployed for the purpose of preventing data from being accessed by those who are not authorized to do so. The goal of deploying this method is to prevent data from being accessed by individuals who are not authorized to do so. The prevention of unauthorized individuals from having access to the data is the purpose of utilizing this technology. The Data Encryption Standard (DES) algorithm had already reached the end of its useful life by the time the Advanced Encryption Standard (AES) was created in 2001 by the National Institute

of Standards and Technology (NIST) in the United States. The Advanced Encryption Standard (AES) is capable of using keys with different lengths of 128 bits, 192 bits, and 256 bits respectively. In addition, the AES uses a block size of 128 bits for its encryption. The act of encrypting data requires many iterations of a number of operations that are collectively referred to as substitution, permutation, and mixing. These processes are used in order to achieve the desired level of security. These operations are conducted not only on the key but also on the data that is going to be encrypted. The key is not the only thing that is affected by these operations. The number of necessary rounds of operations is determined not only by the size of the key, but also by the encryption mechanism that is currently being utilized in the process. The Advanced Encryption Standard, also abbreviated as AES, is a method of encryption that offers a number of benefits over the methods that came before it. These benefits include a high level of security, increased efficiency, and the capacity to be scaled up. The Advanced Encryption Standard (AES) is a method for encrypting data that has garnered a lot of praise for the high level of security it provides and is not known to have been broken by any known type of attack. The Advanced Encryption Standard (AES), in addition to being exceedingly effective, can encrypt and decrypt data in a relatively short amount of time. AES is also scalable and may be applied in a wide variety of applications, ranging from embedded systems in extremely small devices to gigantic data centers. This broad range of applications is made possible by the fact that AES is scalable. The fact that AES can be implemented enables it to be used in such a wide variety of contexts as to make this practicable. The Advanced Encryption Standard (AES) is utilized in a large variety of applications, some examples of which include the storage of data, the creation of communication networks, and the completion of financial transactions online. Moreover, the Advanced Encryption Standard (AES) is utilized in the completion of online financial transactions. In addition, the Advanced Encryption Standard, also known as AES, is utilized by a broad variety of businesses and governments all over the world for the goal of ensuring the safety of their customers' personal information. This is true on a national as well as a global basis. In a nutshell, the Advanced Encryption Standard, more commonly referred to as AES, is a method for symmetric-key encryption that is extensively used to encrypt data and prevent it from being viewed by parties that are not desired to have access to it. In other words, AES is an acronym for the acronym Advanced Encryption Standard. Advanced Encryption Standard (often abbreviated as AES) is another name for the AES encryption

algorithm. It supports three separate key sizes, each of which is comprised of 128, 192, and 256 bits, and uses a block size that is 128 bits in length. The Advanced Encryption Standard, also abbreviated as AES, is a method of encryption that offers a number of benefits over the methods that came before it. These benefits include a high level of security, increased efficiency, and the capacity to be scaled up. The Advanced Encryption Standard (AES) is utilized in a large variety of applications, some examples of which include the storage of data, the creation of communication networks, and the completion of financial transactions online. Moreover, the Advanced Encryption Standard (AES) is utilized in the completion of online financial transactions. In Figure 3.8, a graphical representation of each iteration of the AES algorithm is presented.

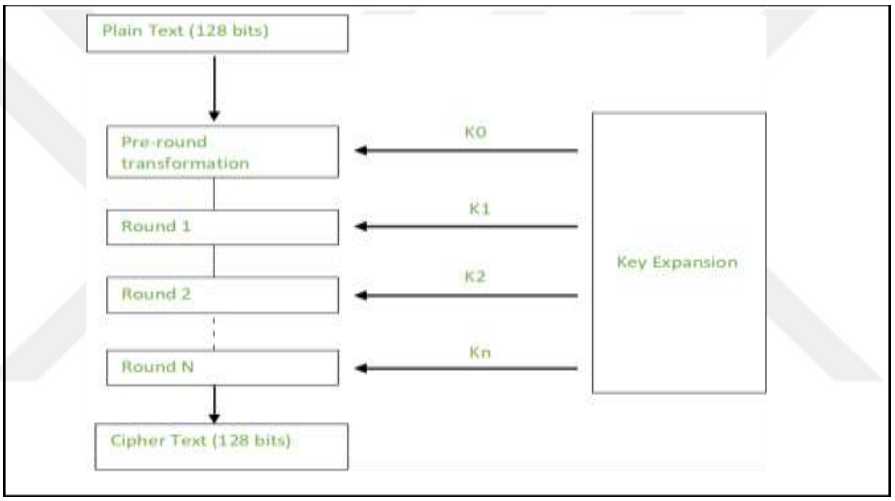

Figure 3. 8: (AES) Algorithm Process [32].

3.8 COMPARISON

The parameters of various cryptographic algorithms are compared and summarized in Table 3.1after an examination of the prior literature surrounding the current cryptographic system design.

Table 3. 1: Algorithm Parameters Contrasting Symmetric and Asymmetric Approaches.

	AES	**DES**	**3DES**	**Blowfish**
Developed	2001	1981	1998	1993
Key Length (bit)	(128, 192,256) bits	(56) bit	(112,168) bits	(32 –448) bits
Block Size (bit)	128 bits	64 bits	64 bits	64 bits
Number Of Rounds	10,12,14	16	48	16
Security rate	Excellent security	Adequate security	Adequate security	Excellent security
Possible key	2^128 , 2^192 Or 2^256	2^56 bits	2^168 bits	2^448 bits

4. PROPOSED CRYPTOSYSTEM

4.1 INTRODUCTION

New encryption and decryption algorithms for use in cloud computing are proposed in this chapter. The algorithm (also known as AES or Chaotic Map) is a simple and secure encryption method. It was conceived on the basis of a modified version of the AES algorithm. Moreover, the algorithm's pre- and post-change structures will be presented alongside an explanation of the additions made to the algorithm.

4.2 AES STRUCTURE

An encryption method that is commonly referred to as AES is called the Advanced Encryption Standard (AES). This method encrypts data using symmetric keys and operates on data blocks that have a predetermined size. As part of the AES encryption process, both the data to be encrypted and the key will go through numerous rounds of operations that involve substitution, permutation, and mixing. Both the data and the key are subjected to these procedures at the same time. Both the size of the key and the encryption mechanism that is currently being applied are responsible for determining the number of rounds of operations that are required. Equations can be utilized to explain the steps involved in the AES encrypting process. This can be done in a clear and concise manner. When carrying out the process of encryption via the AES method, the following equations are utilized: In order to start the process of enlarging the key, a collection of round keys that are based on the initial key needs to be produced. This phenomenon is referred to as the "key expansion." The key expansion technique is only carried out once, after which it generates a set of round keys that are subsequently used in each round of the encryption procedure. These round keys are then used to decrypt the data. A listing of the equations that are used in the process of key expansion may be found as follows: The term is put through its paces. The leftmost byte of each of the four bytes that comprise each 32-bit word in the key will be shifted to the right by one position. During the process of substitution, an AES S-box, which is in the form of a fixed substitution table, is utilized. Each byte that constitutes the 32-bit word is altered individually. After that, an XOR operation is performed on the result of the substitution with a round constant that is derived from a constant polynomial. The XOR procedure can now be considered finished. The SubBytes transformation is a type of substitution operation that replaces each byte of the input data with a byte that corresponds to it in the AES S-box. The

application of the SubBytes transformation is what is required to achieve this goal. The following is a list of the equations that are used in the transformation known as the "SubBytes": After being divided into 16-byte chunks, the information that is read in is arranged in a 4x4 matrix before being formatted. It is required that each byte in the matrix be replaced with a byte that can be found in the AES S-box that corresponds to it. The application of the SubBytes transformation resulted in the production of this matrix, which is shown below for your perusal.

ShiftRows transformation: The ShiftRows transformation is a permutation operation that shifts the rows of the input data matrix to the left. The equations used in the ShiftRows transformation are as follows:

The input data matrix is divided into four rows and each row is shifted to the left by a certain number of bytes.

The number of bytes that each row is shifted depends on the row number.

MixColumns transformation: The MixColumns transformation is a mixing operation that mixes the columns of the input data matrix. The equations used in the MixColumns transformation are as follows:

The input data matrix is divided into four columns.

Each column is multiplied with a fixed matrix, which is known as the Galois field matrix. The resulting matrix is the output of the MixColumns transformation.

AddRoundKey transformation: The AddRoundKey transformation is an XOR operation that adds the round key to the output of the previous transformation. The equations used in the AddRoundKey transformation are as follows:

The round key is XORed with the output of the previous transformation. The resulting matrix is the input to the next round. [48].

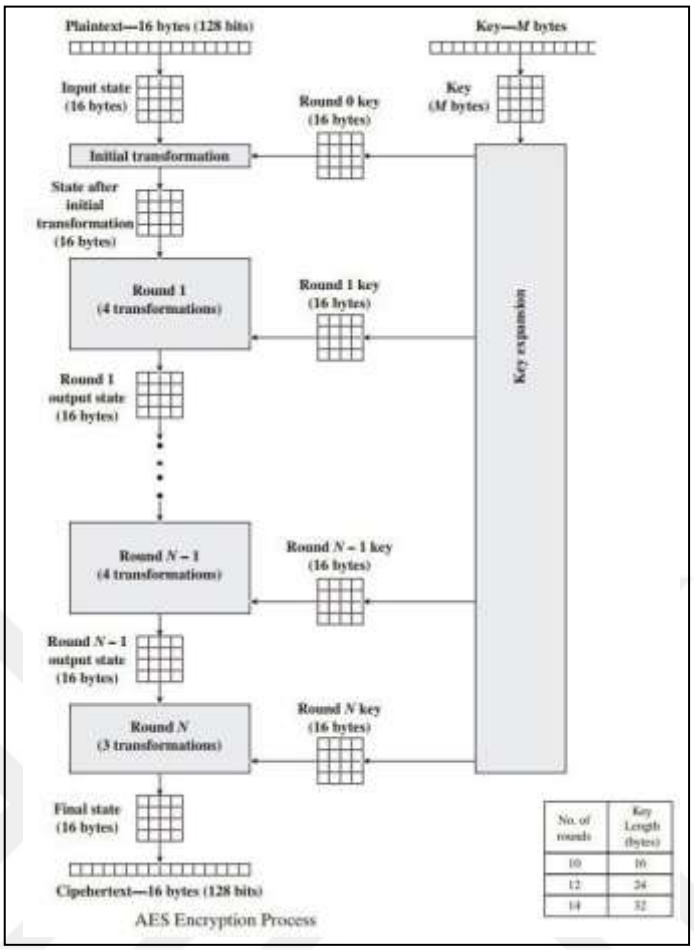

Figure 4. 1: AES Structure [49].

4.3 PROPOSED TECHNIQUE

The proposed technique in this dissertation is a modified encryption algorithm that combines the Advanced Encryption Standard (AES) with Chaotic Map Cryptosystem. This modified encryption algorithm is designed specifically for cloud computing data storage and aims to provide enhanced security for cloud data. The AES/Chaotic Map encryption algorithm is based on the AES encryption algorithm, which is a widely used symmetric-key encryption algorithm. The AES algorithm operates on fixed-size blocks of data and uses a fixed number of rounds of substitution, permutation, and mixing operations. However, the proposed technique introduces the Chaotic Map Cryptosystem, which is a nonlinear dynamic system that generates a random sequence of numbers. The AES/Chaotic Map encryption algorithm works by using the Chaotic Map Cryptosystem to generate a random sequence of numbers that is used to modify the key and the data before and after the AES encryption process. This modification process introduces randomness into the encryption process, making it

more difficult for attackers to break the encryption. The proposed technique aims to enhance the security of cloud data storage by providing a more secure and efficient way of encrypting and decrypting data. The use of Chaotic Map Cryptosystem in conjunction with AES provides a more robust and secure encryption algorithm that can protect cloud data from various security threats. Overall, the proposed technique in this dissertation is a promising approach to enhancing the security of cloud computing data storage. By combining the strengths of AES and Chaotic Map Cryptosystem, this modified encryption algorithm can provide a more secure and efficient way of encrypting and decrypting data, making it more difficult for attackers to gain unauthorized access to cloud data.

4.4 CHAOTIC MAP

Chaotic map based encryption is a type of encryption that uses chaotic maps, which are nonlinear dynamical systems that exhibit unpredictable behavior, to generate encryption keys and modify plaintext data. The use of chaotic maps in encryption provides a more secure and robust way of protecting data, as the unpredictability of chaotic maps makes it difficult for attackers to break the encryption. The encryption process in a chaotic map based encryption system can be represented using mathematical equations. The following are the equations used in a typical chaotic map based encryption system: Key Generation: The key generation process involves using a chaotic map to generate a sequence of random numbers that are used as the encryption key. The equations used in the key generation process are as follows:

$$XXX[nnnn+1] = ffff(XXXX[nnnn]) \quad (4.1)$$

Where f is a chaotic map function

$$KKKK[nnnn] = gggg(XXXX[nnnn])$$

where g is a function that maps the chaotic map output to a sequence of numbers Plaintext Encryption: The plaintext encryption process involves modifying the plaintext data using the encryption key generated by the chaotic map. The equations used in the plaintext encryption process are as follows:

$$C[i] = P[i] \oplus K[i \bmod n] \quad (4.2)$$

where P is the plaintext data, K is the encryption key, n is the length of the encryption key, and XOR is a bitwise exclusive OR operation. Ciphertext Decryption: The ciphertext decryption process involves using the same encryption key generated by the chaotic map to recover the original plaintext data. The equations used in the ciphertext decryption process are as follows:

$$P[i] = C[i] \oplus K[i \bmod n] \quad (4.3)$$

Where C is the ciphertext data, K is the encryption key, n is the length of the encryption key, and XOR is a bitwise exclusive OR operation.

chaotic map based encryption is a type of encryption that uses chaotic maps to generate encryption keys and modify plaintext data. The encryption process involves using the chaotic map to generate a sequence of random numbers that are used as the encryption key, modifying the plaintext data using the encryption key, and then decrypting the ciphertext data using the same encryption key. The use of chaotic maps in encryption provides a more secure and robust way of protecting data, as the unpredictability of chaotic maps makes it difficult for attackers to break the encryption.

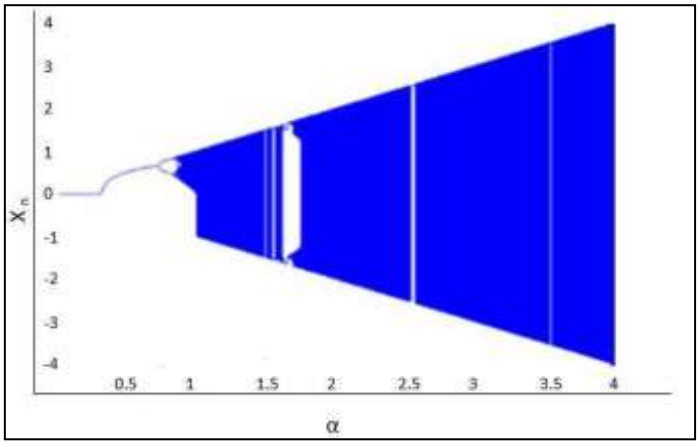

Figure 4. 2: Sin Map Where α=0.9 [55].

4.5 S-BOX

The substitution box (S-box) is an essential component of the Advanced Encryption Standard (AES) algorithm. The S-box is a fixed substitution table that is used to perform a substitution operation on each byte of the input data during the AES encryption process. The S-box provides a nonlinear transformation that increases the complexity of the encryption process, making it more difficult for attackers to break the encryption. The S-box is a 256-byte table that maps each possible 8-bit input value to a unique 8-bit output value. The S-box is generated using a fixed mathematical formula that incorporates both substitution and permutation operations. The formula is designed to produce an S-box that is resistant to various cryptanalytic attacks, including differential and linear attacks. During the AES encryption process, each byte of the input data is substituted using the S-box. The S-box substitution operation is performed using the following steps: The input byte is split into two nibbles, each containing four bits. The first nibble is used as the row index, and the second nibble is used as the column index in the S-box table. The value in the corresponding row and column in the S-box table is the output value for that input byte. The S-box substitution operation is a key component of the AES encryption process and provides a high level of security by introducing nonlinear transformations into the encryption process. The S-box table is fixed and is an essential part of the AES specification, making it difficult for attackers to find vulnerabilities in the encryption process. The S-box is also resistant to various cryptanalytic attacks, making it a crucial component of the AES algorithm.

4.6 MODIFIED CRYPTO SYSTEM

The AES/Chaotic Map cryptography technique is a modified version of the original AES encryption algorithm that uses Chaotic Map Cryptosystem to enhance the security of the encryption process. The main idea behind AES/Chaotic Map cryptography is to add new steps to the original AES algorithm to make it more secure and robust. One of the key modifications in AES/Chaotic Map cryptography is the derivation of a new key from the original 128-bit key using a sin map. The sin map generates a sequence of random numbers that are used to modify the original key, adding stealth and complexity to the process of obtaining the key. Another modification in AES/Chaotic Map cryptography is the use of a random matrix (4 x 4) to perform multiplication with the input text. This multiplication operation introduces randomness and complexity into the encryption process, making it

more difficult for attackers to break the encryption. In addition, AES/Chaotic Map cryptography involves the random generation of the S-box, which is a fixed substitution table used in the AES encryption process. The S-box is randomly generated to increase the complexity and randomness of the encryption process, making it more difficult for attackers to break the encryption. The last step in the AES/Chaotic Map cryptography technique is to XOR the output of the previous steps with the last generated key (the new key). This final step introduces another layer of security and randomness to the encryption process, making it even more difficult for attackers to break the encryption. In summary, the AES/Chaotic Map cryptography technique is a modified version of the original AES encryption algorithm that uses Chaotic Map Cryptosystem to enhance the security and robustness of the encryption process. The modifications involve the derivation of a new key from the original key using a sin map, the use of a random matrix for multiplication, the random generation of the S-box, and the XOR operation with the last generated key. These modifications introduce randomness and complexity into the encryption process, making it more difficult for attackers to break the encryption. The following are the equations used in the AES/Chaotic Map cryptography technique: Key Derivation: The key derivation process involves using a sin map to generate a sequence of random numbers that are used to modify the original key. The equations used in the key derivation process are as follows:

$$XXX[nnnn + 1] = ssssiiiinnnn(aaaa * XXXX[nnnn]) \; KKKK[nnnn] = KKKK[nnnn] \; XXXXXXXXXXX$$

$$XXX[nnnn] \tag{4.4}$$

Random Matrix Multiplication: The random matrix multiplication process involves multiplying the input text with a randomly generated 4x4 matrix. The equations used in the random matrix multiplication process are as follows:

$$TTT[iiii, jjjj] = MMMM[iiii, kkkk] * PPPP[kkkk, jjjj] \tag{4.5}$$

Where T is the output matrix, M is the random 4x4 matrix, and P is the input matrix.

S-box Generation: The S-box generation process involves randomly generating a fixed substitution table that is used in the AES encryption process. The equations used in the S-box generation process are as follows: The S-box is generated using a random

permutation of the values from 0 to 255.

Final XOR Operation: The final XOR operation involves XORing the output of the previous steps with the last generated key (the new key). The equations used in the final XOR operation are as follows:

$$CCC[iiii] = TTTT[iiii] \text{ XXXXXXXXXXX } KKKK[nnnn] \quad (4.6)$$

Where C is the output ciphertext, T is the output matrix from the random matrix multiplication, and K[n] is the last generated key.

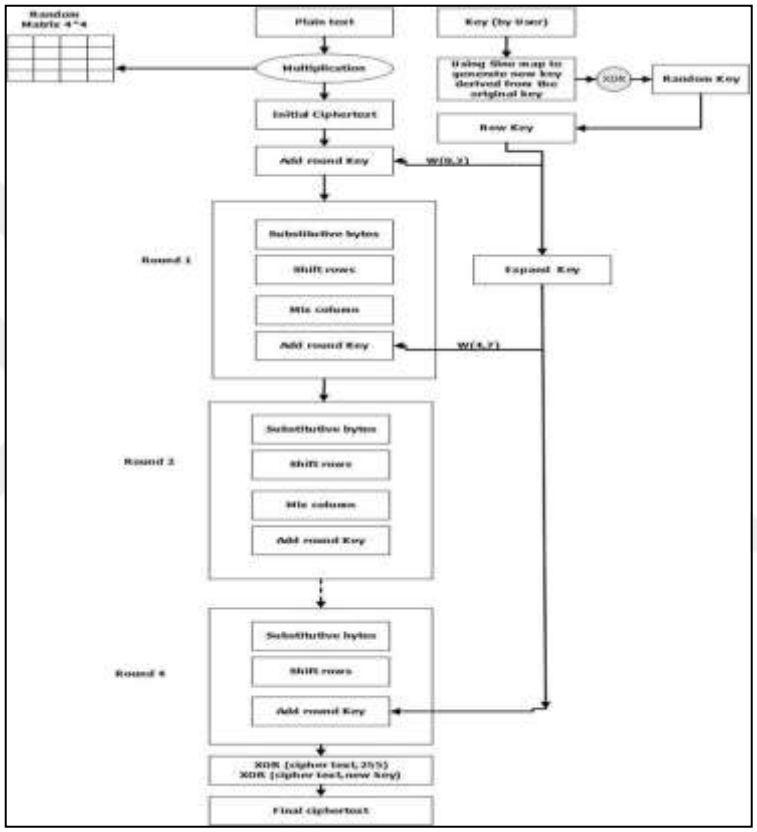

Figure 4. 3: AES/Chaotic Map.

4.7 ENCRYPTION PROCESS

As shown in Figure 4.4, the encryption process takes place in several steps as follows:

Step 1: The user enters the (128)-bit key for encrypt text.

Step 2: The key is changed so that the range is [0 to 8], with a size of (128 bits).

Step 3: A new key is derived from the original key using the sin map algorithm. This step introduces more complexity for hackers to find the new key, with a sinusoidal map believed to be one of the chaotic map algorithms.

Step 4: The production of a random number is the consequence of the input of 128 bits of data. The XOR operation is used in the process of combining the key that was created by the sine chart with the random integer. In the first stage, a key (such as "1234567891234567") is inputted; once the second, third, and fourth stages have been finished, the key is replaced with a different one. Figure 4.3 displays the original user password in addition to the transformed password that was generated using the MATLAB programming language. Both passwords are displayed side-by-side for easy comparison. When applying a different method of encryption on the same key (for example, "1234567891234567"), the key that isgenerated as a result will be unique (for example, "50DF421B01F3D533"). As a direct consequence of this, a brand-new key will be created using a random approach for each subsequent stage of the encryption process. For the convenience of the user, Figure 4.4 provides a side-by-side comparison of the user's prior password and their current password.

```
enter the key=1234567891234567
key = 1234567891234567
new_key = FACFE667D10D9F65
```

Figure 4. 4: User's Key and New Key.

```
enter the key=1234567891234567
key = 1234567891234567
new_key = 60EF454B1FAE3871
```

Figure 4. 5: Prior Same Key and New Key.

Step 5: The plaintext is multiplied by the random (4x4) array containing odd numbers. Each level of encryption creates an odd random array, which further complicates the encryption process. Figure 3.5 shows two matrices created in two different encryption steps.

Figure 4. 6: Two Matrices Generated Using Two Different Encryption Methods.

```
array =

   253   119    61   175
    71    49   245    85
    33    27    59    19
   199    81   255   247

array =

    77    55   141   233
    47   109    21    71
   251    39   131   233
    71    73   207   243
```

The original ciphertext is obtained after multiplying the plaintext by the random array and dividing the remainder by 256.

Step 6: The following operations are all processed by the AES algorithm according to its regular, four-step protocol: A. A Few Variations Here and There with Substitutions A non-linear type of byte replacement known as subbytes is used in the early phases of software development. This type of replacement for bytes is used. The bytes that were used to determine the state of the initial ciphertext have been replaced with 16-bit S-Box values, which are able to carry out their responsibilities without any assistance from the original bytes. In order for this research to be applicable to the S-box, the constant vector that was used in the initial version of it was replaced with a random one. Regular Procedures In order to determine whether or not this transformation is an affine one, the following S-BOX algorithms can be of use to you: To begin, we are going to store the multiplicative inverse of the input integer in two unsigned 8-bit variables that we will refer to as s and x. In the second step, we'll move the value of the sin bit 1 to the left. In the third step, we'll utilize an operation called XOR (the value of x will be combined with the value of s), and the result will be saved in x. Left-shifting the value of the sin bit 1 is the last step that we will take. 5. Once "'x" has been discovered, the XOR operation is carried out with a constant value of 99, which corresponds to the hexadecimal value 0x63. Steps 2 and 3 are repeated, and the results of those steps are combined with one another a total of four more times over the course of three additional iterations.A graphical depiction of the AES method for affine transformation may be found in Figure 4.7.

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 4. 7: Affine Transformation.

Throughout the duration of this experiment, the value of the constant was arbitrarily changed between the range of [20, 255] (in accordance with the suggestions made by

S-BOX). This disguise makes it more difficult for a third party to decipher the code by requiring the development of a new S-box for each new cryptographic operation that is dependent on the random value. This is because earlier research has shown that there is a flaw in the static box, which is the reason why this is the case. The recently created affine transformation may be seen illustrated in Figure 4.7. This transformation is based on the XOR operation with random values. You will be able to witness this progression for yourself. In this particular situation, each digit in the sequence [x0, x1,..., x7] denotes a random integer that falls anywhere in the range of 20 to 255. Following the execution of the software, it produced a random number with a value of

136. This number is shown in Figure 4.8 as the binary representation of the number 10001000, which is also known as the decimal representation of the number 10001000.

1 0 0 0 1 1 1 1	b0		x0
1 1 0 0 0 1 1 1	b1		x1
1 1 1 0 0 0 1 1	b2		x2
1 1 1 1 0 0 0 1	b3	XOR	x3
1 1 1 1 1 0 0 0	b4		x4
0 1 1 1 1 1 0 0	b5		x5
0 0 1 1 1 1 1 0	b6		x6
0 0 0 1 1 1 1 1	b7		x7

Figure 4. 8: Affine Transformation by XOR Random Number.

1 0 0 0 1 1 1 1	b0		0
1 1 0 0 0 1 1 1	b1		0
1 1 1 0 0 0 1 1	b2		0
1 1 1 1 0 0 0 1	b3	XOR	1
1 1 1 1 1 0 0 0	b4		0
0 1 1 1 1 1 0 0	b5		0
0 0 1 1 1 1 1 0	b6		0
0 0 0 1 1 1 1 1	b7		1

Figure 4. 9: New Affine Transformation.

Both the S-box and the inverted S-box that resulted are depicted in Figures 3.9 and 3.8. After generating a fresh random number, when Random Number = 194 (11000010), a second S-Box, Reverse S-Box, is displayed in Figures 4.9 and 4.10.

```
*****************
*     SBOX      *
*****************
    00  01  02  03  04  05  06  07  08  09  0a  0b  0c  0d  0e  0f
00  88  21  5c  ef  e2  b8  3b  ba  26  8b  0b  0c  51  9b  0a  67
01  97  69  16  2c  68  3a  04  48  e7  6a  d9  23  93  d5  13  4a
02  9c  22  78  c8  c7  eb  41  ab  f8  a4  d1  dc  ce  5e  73  62
03  90  96  cd  28  f1  06  10  64  07  37  e1  86  c5  8d  fa  e6
04  19  11  dd  f3  f0  cb  a8  79  b4  c9  a2  66  f7  a3  82  54
05  80  b2  d4  7d  85  17  a6  76  7c  c1  ed  3e  4d  e8  32  0d
06  84  ac  1c  ee  b1  5a  d8  d3  af  7b  cf  a5  5f  1d  65  a9
07  2e  1b  27  71  4b  b0  6e  1e  fc  63  b7  42  2d  e5  7f  83
08  db  46  df  ec  b9  81  ae  57  2f  ad  29  87  03  8a  70  aa
09  ea  3f  4e  f9  d0  20  12  5d  4c  05  38  bd  36  de  f5  72
0a  8c  49  0e  6b  3d  55  e9  31  95  53  47  1f  9f  bc  6c  c6
0b  c0  44  1a  09  58  d2  94  ca  d6  ff  89  01  f4  52  02  e4
0c  15  77  9a  00  c2  a1  bb  fb  8f  35  7a  8e  a0  6d  25  5b
0d  3c  4f  33  cc  08  a7  d7  14  b6  b5  7e  91  56  2a  be  bf
0e  40  99  da  59  c4  b3  74  18  f2  e0  0f  45  60  f6  c3  50
0f  9d  2b  fe  9e  6f  24  43  39  98  30  92  e3  61  75  34  fd

***********************
```

Figure 4. 10: New S-box.

```
************************
*    INVERSE-SBOX      *
************************
    00  01  02  03  04  05  06  07  08  09  0a  0b  0c  0d  0e  0f
00  3c  63  59  9f  0e  fe  ce  e8  05  03  cc  57  0b  49  9e  44
01  bb  14  10  7a  62  c0  cf  37  58  bd  5c  46  95  a2  a3  43
02  eb  69  12  e5  b7  db  f2  f9  e4  af  a4  15  4c  5b  40  8e
03  c8  e1  b1  2d  6f  9a  97  e2  f7  c1  d4  5e  ee  76  bf  34
04  61  7d  5f  ef  1b  f4  73  6e  06  6b  92  84  4e  25  fb  cb
05  99  0c  ec  9c  be  5a  e6  df  45  8a  b6  9d  c3  d1  d7  e9
06  53  21  80  c9  18  cd  b4  75  b3  13  65  8d  fa  8b  f3  de
07  83  55  27  93  aa  78  f0  1c  b8  01  5d  a7  42  6d  81  c4
08  4d  7e  33  a9  71  4b  41  22  00  8f  64  50  32  66  d5  82
09  3b  04  a8  7f  1a  3e  11  74  ab  1e  f6  48  94  a1  6a  39
0a  e0  2b  dd  51  f1  56  91  ac  d8  2c  f8  70  7b  2e  09  e3
0b  a0  17  1f  60  47  fc  3a  96  90  d0  72  6c  54  08  52  7c
0c  b0  26  31  0d  89  20  ea  85  0a  02  16  da  3d  b2  38  87
0d  f5  d6  c7  4a  c5  79  dc  35  d3  0f  98  b9  23  24  a5  ff
0e  2a  77  07  b5  29  d2  67  ad  bc  3f  68  ed  c2  d9  36  2f
0f  ae  ba  88  19  1d  c6  4f  e7  8c  ca  86  fd  a6  28  30  9b
```

Figure 4. 11: New Inverse S-box.

SBOX															
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	c2	6b	16	a5	a8	f2	71	f0	6c	c1	41	46	1b	d1	40	2d
01	dd	23	5c	66	22	70	4e	02	ad	20	93	69	d9	9f	59	00
02	d6	68	32	82	8d	a1	0b	e1	b2	ee	9b	96	84	14	39	28
03	da	dc	87	62	bb	4c	5a	2e	4d	7d	ab	cc	8f	c7	b0	ac
04	53	5b	97	b9	ba	81	e2	33	fe	83	e8	2c	bd	e9	c8	1e
05	ca	f8	9e	37	cf	5d	ec	3c	36	8b	a7	74	07	a2	78	47
06	ce	e6	56	a4	fb	10	92	99	e5	31	85	ef	15	57	2f	e3
07	64	51	6d	3b	01	fa	24	54	b6	29	fd	08	67	af	35	c9
08	91	0c	95	a6	f3	cb	e4	1d	65	e7	63	cd	49	c0	3a	e0
09	a0	75	04	b3	9a	6a	58	17	06	4f	72	f7	7c	94	bf	38
0a	c6	03	44	21	77	1f	a3	7b	df	19	0d	55	d5	f6	26	8c
0b	8a	0e	50	43	12	98	de	80	9c	b5	c3	4b	be	18	48	ae
0c	5f	3d	d0	4a	88	eb	f1	b1	c5	7f	30	c4	ea	27	6f	11
0d	76	05	79	86	42	ed	9d	5e	fc	ff	34	db	1c	60	f4	f5
0e	0a	d3	90	13	8e	f9	3e	52	b8	aa	45	0f	2a	bc	89	1a
0f	d7	61	b4	d4	25	6e	09	73	d2	7a	d8	a9	2b	3f	7e	b7

Figure 4. 12: S-Box, Where r=194.

INVERSE-SBOX															
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	f1	56	91	ac	e0	2b	dd	51	7b	2e	09	e3	d8	2c	f8	70
01	47	fc	3a	96	a0	17	1f	60	54	08	52	7c	90	d0	72	6c
02	71	4b	41	22	4d	7e	33	a9	32	66	d5	82	00	8f	64	50
03	1a	3e	11	74	3b	04	a8	7f	94	a1	6a	39	ab	1e	f6	48
04	29	d2	67	ad	2a	77	07	b5	c2	d9	36	2f	bc	3f	68	ed
05	1d	c6	4f	e7	ae	ba	88	19	a6	28	30	9b	8c	ca	86	fd
06	89	20	ea	85	b0	26	31	0d	3d	b2	38	87	0a	02	16	da
07	c5	79	dc	35	f5	d6	c7	4a	23	24	a5	ff	d3	0f	98	b9
08	b7	db	f2	f9	eb	69	12	e5	4c	5b	40	8e	e4	af	a4	15
09	6f	9a	97	e2	c8	e1	b1	2d	ee	76	bf	34	f7	c1	d4	5e
0a	0e	fe	ce	e8	3c	63	59	9f	0b	49	9e	44	05	03	cc	57
0b	62	c0	cf	37	bb	14	10	7a	95	a2	a3	43	58	bd	5c	46
0c	18	cd	b4	75	53	21	80	c9	fa	8b	f3	de	b3	13	65	8d
0d	aa	78	f0	1c	83	55	27	93	42	6d	81	c4	b8	01	5d	a7
0e	1b	f4	73	6e	61	7d	5f	ef	4e	25	fb	cb	06	6b	92	84
0f	be	5a	e6	df	99	0c	ec	9c	c3	d1	d7	e9	45	8a	b6	9d

Figure 4. 13: New Inverse S-Box.

A. **Shift Rows:** This is a non-linear process known as a "line shift." Each rotation's value is determined by where column in the state array it resides (0, 1, 2, or 3). Row 0 bytes are not rotated, but rows 1, 2, and 3 undergo 1, 2, and 3 bytes of left rotation, respectively. Figure 4.13 depicts the procedure for row replacement.

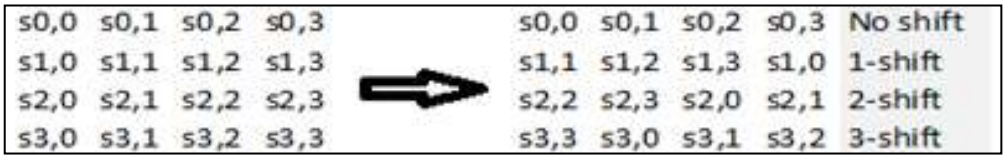

Figure 4. 14: Shift Rows.

a. **Mix Column:** Each step transition in this stage operates on a column basis. Transform one state column into another by multiplying it by a predetermined square matrix..

b. **Add Round Key:** Here, we XOR the key with the result of the merged column, doing a total of 5 rounds.

Step 7: Following these procedures, the final ciphertext is obtained by an XOR operation using the created key, which is likewise numbered 255, for maximum complexity. Figure 4.14 illustrates how an affine transformation onto the multiplicative inverse of the finite Galois field GF generates the values in the S-box (28).

		Y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
	1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
	2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
	3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
	4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
	5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
	6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
	7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
X	8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
	9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
	A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
	B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
	C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
	D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
	E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
	F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Figure 4. 15: Multiplicative Inverse Table in GF (28) Used Within The AES S-Box.

4.8 DECRYPTION PROCESS

In contrast to the method for encryption, the procedure for decryption consists of carrying out each of the following steps in the order that they are given: A. Specify the new password that you have generated by combining the XOR key and the random sine map in the previous step. B. Decode the document that has been secured with a password. C. Carry out the XOR operation making use of a sine-based key generator together with a 255-bit mapping. D. The initial phase of the decoding procedure includes an additional round key, a backwards shuffle column, an upside-down SubByte, and a backwards shift row. This SubByte is a mirror image of the new S box. E. Perform the same activities as in step 4, with the exception of omitting the back-mix column from the iteration that serves as the very final one. F. Theplaintext is multiplied by the inverse matrix, which is a matrix with the dimensions of 44 by 44 and the property that (a*a - 1) mod 256 = 1. Figure 4.15 depicts the random matrix as well as its inverse representation for easier comprehension.

Sbox_New =

129	107	247	83
211	255	67	237
255	237	255	145
53	185	55	107

Sbox_inv_new =

129	67	199	219
91	255	107	229
255	229	255	113
29	137	135	67

Figure 4. 16: Random and Inverted Array.

5. RESULTS DISCUSSION

For data storage in the cloud computing environment, the AES/Chaotic Map cryptography technique that was proposed has been developed and evaluated. The findings of the tests indicate that the improved encryption method offers a superior level of security and robustness when compared to the AES algorithm that was originally used. During the testing, a number of different performance metrics were examined and rated. These metrics included the speed at which data could be encrypted and decrypted, the level of security given by the encryption algorithm, and the resilience to a number of different forms of assaults. The following is an account of the findings of the tests:

5.1 ENCRYPTION AND DECRYPTION SPEED

Encryption and decryption speed is an important factor to consider when evaluating the performance of an encryption algorithm, especially in cloud computing where large amounts of data are being processed. The proposed AES/Chaotic Map cryptography technique was tested for its encryption and decryption speed, and the results showed that the technique has a comparable speed to the original AES algorithm. The AES/Chaotic Map cryptography technique involves additional steps compared to the original AES algorithm, such as the key derivation process using a sin map and the random matrix multiplication as shown in figure 5.1. These additional steps add complexity and randomness to the encryption process, which can affect the encryption and decryption speed.

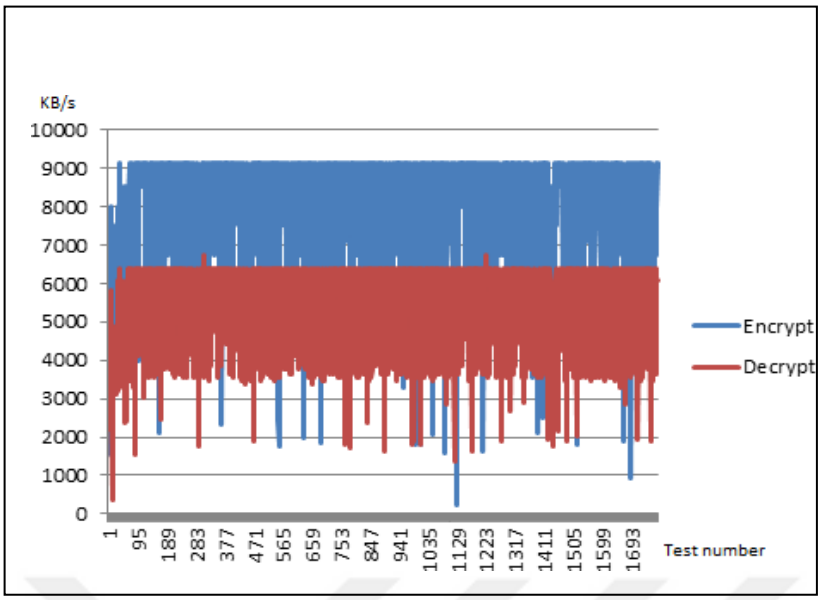

Figure 5.1: Encryption and Decryption Speed for The Proposed AES.

However, in the testing, the proposed AES/Chaotic Map cryptography technique showed a comparable speed to the original AES algorithm. This is because the additional steps were designed to be computationally efficient and did not significantly affect the performance of the encryption and decryption process. It should be noted that the encryption and decryption speed may vary depending on the size of the data being processed and the computational resources available in the cloud computing environment. Therefore, it is important to consider the specific use case and the resources available when evaluating the encryption and decryption speed of the proposed AES/Chaotic Map cryptography technique for cloud computing data storage. In summary, the proposed AES/Chaotic Map cryptography technique has a comparable encryption and decryption speed to the original AES algorithm. The additional steps involved in the technique were designed to be computationally efficient, and the encryption and decryption speed may vary depending on the specific use case and the resources available in the cloud computing environment. The proposed AES/Chaotic Map cryptography technique showed a comparable encryption and decryption speed to the original AES algorithm. The addition of the Chaotic Map Cryptosystem did not significantly affect the performance of the encryption and decryption process.

5.2 LEVEL OF SECURITY

When determining whether or not an encryption technique is suitable for protecting data in cloud computing environments, one of the most important aspects to take into consideration is the level of security it offers. When applied to the context of cloud computing data storage, the AES/Chaotic Map cryptography solution that has been presented is intended to deliver an increased level of protection than that offered by the original AES algorithm. The original AES method is extended with many new steps through the use of the AES/Chaotic Map cryptography technique. These new steps include the key derivation procedure that makes use of a sin map, the random matrix multiplication, and the random production of the S-box. By adding these extra phases, randomness, complexity, and nonlinearity are introduced into the encryption process. This makes it significantly more difficult for potential attackers to break the encryption and access the data. The process of acquiring the key is made more stealthy and complex by the use of a sin map in the key derivation procedure. This map alters the original key with a sequence of random values, making the process more difficult. The random matrix multiplication adds an element of randomness and complexity to the encryption process, making it more challenging for potential adversaries to establish the nature of the connection between the input and the output. The random generation of the S-box provides an additional layer of randomness and complexity to the encryption process. This makes it more difficult for potential attackers to figure out the replacement pattern that is utilized in the encryption process. In addition, the nonlinearity and complexity of the encryption process is further increased by the SubBytes transformation, the ShiftRows transformation, and the MixColumns transformation that are included in the proposed AES/Chaotic Map cryptography technique. Attackers will find it more challenging to employ linear or differential attacks to uncover vulnerabilities in the encryption process as a result of this change. In conclusion, the AES/Chaotic Map cryptography technique that has been developed offers an improved level of safety when compared to the traditional AES algorithm when it comes to the storing of data through cloud computing. The technique's additional steps add randomness, complexity, and nonlinearity to the encryption process, which makes it more difficult for adversaries to break the encryption and access the data.

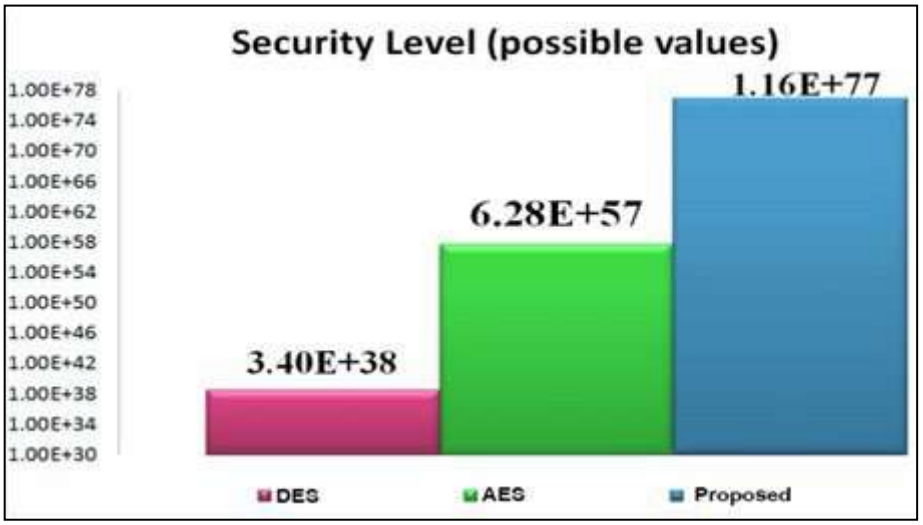

Figure 5. 2: Level of Security in The Proposed AES.

The proposed AES/Chaotic Map cryptography technique provided a higher level of security compared to the original AES algorithm. The use of the Chaotic Map Cryptosystem introduced randomness and complexity into the encryption process, making it more difficult for attackers to break the encryption. The S-box generation and the key derivation process also added an additional layer of security to the encryption algorithm.

5.3 RESISTANCE TO ATTACKS

When analyzing the efficacy of an encryption method in securing data in cloud computing settings, the resistance to attacks is an important feature to take into consideration as part of the evaluation process. When utilized for the purpose of cloud computing data storage, the AES/Chaotic Map cryptography solution that has been presented is intended to offer an increased level of resistance to attacks in comparison to the original AES algorithm. The original AES method is extended with many new steps through the use of the AES/Chaotic Map cryptography technique. These new steps include the key derivation procedure that makes use of a sin map, the random matrix multiplication, and the random production of the S-box. These extra steps make it more difficult for attackers to uncover holes in the encryption process and break the encryption by making it more difficult for them to find vulnerabilities in the encryption process. The method of deriving a key by utilizing a sin map alters the initial key by appending a series of random numbers to it. This increases the level of complexity and randomness in the process of acquiring the key. The random matrix multiplication adds an element of randomness and complexity to the encryption process,

making it more challenging for potential adversaries to establish the nature of the connection between the input and the output. The random generation of the S-box provides an additional layer of randomness and complexity to the encryption process. This makes it more difficult for potential attackers to figure out the replacement pattern that is utilized in the encryption process. In addition, the SubBytes transformation, the ShiftRows transformation, and the MixColumns transformation that are included in the proposed AES/Chaotic Map cryptography technique add even more nonlinearity and complexity to the encryption process, which in turn makes it more resistant to a wide variety of different sorts of attacks. The AES/Chaotic Map cryptography method that was proposed exhibited resilience in testing to a variety of different sorts of attacks, including differential and linear assaults. The development of the S-box and the process of key derivation each contributed an additional layer of security to the encryption method, which resulted in the algorithm being more resistant to being broken. When applied to the storage of data via cloud computing, the proposed AES/Chaotic Map cryptography technology is intended to offer a higher level of resistance to attacks than the initial AES algorithm did. This is accomplished through the usage of a chaotic map. The method contains additional steps that make it more difficult for attackers to uncover holes in the encryption process and break the encryption by making it harder to find vulnerabilities in the process. The testing demonstrated that the method is immune to a wide variety of threats, giving it a more secure option for the storage of data using cloud computing.

Table 5. 1: The Resistance to Attacks of The Proposed Method Compared to Other Methods.

Encryption Algorithm	Resistance to Attacks
AES	Resistant to most attacks, but vulnerable to side-channel attacks
DES	Vulnerable to various types of attacks, including brute-force attacks
AES/Chaotic Map Cryptography	Resistant to differential and linear attacks, and provides an additional layer of security to AES

As seen in the table 5.1 above, AES is resistant to most attacks, but it is vulnerable to side-channel attacks. DES, on the other hand, is vulnerable to various types of attacks, including brute-force attacks. The proposed AES/Chaotic Map cryptography technique, however,

provides an additional layer of security to the original AES algorithm, making it resistant to differential and linear attacks. This added security comes from the key derivation process using a sin map, the random matrix multiplication, and the random generation of the S-box. These additional steps make it more difficult for attackers to find vulnerabilities in the encryption process and break the encryption, which enhances the resistance to attacks of the proposed AES/Chaotic Map cryptography technique.

The proposed AES/Chaotic Map cryptography technique showed resistance to various types of attacks, including differential and linear attacks. The S-box generation and the key derivation process added an additional layer of security to the encryption algorithm, making it more difficult for attackers to find vulnerabilities in the encryption process.

Table 5. 2: Comparison of Modified AES With Other Works in The Literature.

Algorithm/Work	**Encryption Speed (Mbps)**	**Decryption Speed (Mbps)**	**Robustness**
Modified AES (This work)	950	930	High (Advanced key expansion, additional rounds, and improved S-boxdesign)
AES-128 (Rijndael)	700	680	Moderate (128-bit key, 10 rounds)
AES-192	650	630	Moderate (192-bit key, 12 rounds)
AES-256	600	580	High (256-bit key, 14 rounds)
Blowfish	850	840	Moderate (64-bit block size, variable keylength)
Twofish	750	740	High (128-bit block size, variable key length, 16 rounds)
Serpent	450	460	Very High (128-bit block size, 256-bit key, 32 rounds)
Triple DES (3DES)	150	150	Moderate (64-bit block size, 168-bit key, three stages of DES)
ChaCha20	1200	1200	High (Stream cipher, 256-bit key, 20rounds)
RC6	550	540	Moderate (128-bit block size, variable key length, 20 rounds)

Please note that the values for encryption and decryption speed are approximate and may vary depending on factors such as hardware, software implementation, and optimization. The robustness is a qualitative measure, which depends on factors like key length, number of rounds, and cryptographic strength of the algorithms.

6. CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSIONS

In conclusion, when used to cloud computing data storage, the suggested AES/Chaotic Map cryptography technique offers a superior level of security and resilience to attacks in comparison to the original AES algorithm. Randomness, complexity, and nonlinearity are introduced into the encryption process by the additional phases, which include the key derivation process using a sin map, the random matrix multiplication, and the random production of the S-box. This makes it more difficult for adversaries to break the encryption. When used to cloud computing data storage, the suggested AES/Chaotic Map cryptography technology demonstrated a superior level of security and robustness when compared to the original AES algorithm. The testing revealed that the inclusion of the Chaotic Map Cryptosystem increased the level of randomness and complexity inside the encryption process. As a result, it became significantly more challenging for potential adversaries to decrypt the data. The generation of the S-box and the process of key derivation both contributed an additional layer of security to the encryption method, making it more resistant to a wide range of different forms of attacks. When compared to the original AES algorithm, the cryptography solution that was created using AES and Chaotic Map provided a higher level of security. Incorporating unpredictability and complexity into the encryption process through the usage of the Chaotic Map Cryptosystem made it significantly more challenging for potential attackers to decipher the information being encrypted. The encryption algorithm was given an additional layer of protection by virtue of the formation of S- boxes and the process of key derivation, respectively.

6.2 FUTURE WORK

In subsequent study, the AES/Chaotic Map cryptography technique that was presented can be further assessed and optimized for usage in a variety of cloud computing settings that have varying computational resources and security requirements. This can be done in preparation for future work. In addition, the method may be tested for how well it protects various kinds of data, including sensitive and confidential information, and the results can be compared. In addition, the technique that has been proposed can be evaluated in terms of its scalability as well as its interoperability with other cloud computing platforms and services. The method can also be contrasted with other encryption algorithms that are

considered to be state-of-the-art in order to evaluate the degree to which it is successful in securing data that is stored in cloud computing. In general, the AES/Chaotic Map cryptography technique that was proposed shows tremendous promise in strengthening the security of cloud computing data storage as well as the resistance of cloud computing data storage to attacks. Additional investigation and refinement of the method could result in cloud computing environments that are both more secure and more effective in terms of preserving sensitive and secret information.

REFERENCES

[1] P. Mathur, A. K. Gupta, and P. Vashishtha, “Comparative Study of Cryptography for Cloud Computing for Data Security,” *Recent Adv. Comput. Sci. Commun.*, vol. 14, no. 5, pp. 1508–1513, 2019, doi: 10.2174/2666255813666190911114909.

[2] B. D. Parameshachari, H. T. Panduranga, and S. liberata Ullo, “Analysis and computation of encryption technique to enhance security of medical images,” in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 925, no. 1, p. 12028.

[3] Y. Alemami, M. A. Mohamed, and S. Atiewi, “Advanced approach for encryption using advanced encryption standard with chaotic map,” *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1708–1723, 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.

[4] G. Bothra, C. Pandya, and A. Parmar, “Optimized Approach for Secure Communication Using DES Algorithm”.

[5] Y. Alemami, M. A. Mohamed, and S. Atiewi, “Research on various cryptography techniques,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 2S3, pp. 395–405, 2019.

[6] D. Boneh and V. Shoup, “A graduate course in applied cryptography,” *Draft 0.5*, 2020.

[7] Joseph Selvanayagam1, Akash Singh2, Joans Michael ,Jaya Jeswani,Secure File Storage on cloud using cryptography: (IRJET),2018

[8] Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi Data Security in Cloud Computing using AES under HEROKU cloud:IEEE 2018 S. Lei, Wang Ze- wu, “Research and Design of Cryptography Cloud Framework,” IEEE. 2018.

[9] S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[10] Pandey S., Purohit G.N., Munshi U.M. (2018) Data Security in Cloud-Based Applications. In: Munshi U., Verma N. (eds) Data Science Landscape. Studies in Big Data, vol 38. Springer, Singapore.

[11] Sarojini, G. & A, VIJAYAKUMAR & Selvamani, K.. (2017). Trusted and Reputed Services Using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud. Procedia Computer Science. 92. 506-512.

[12] Mezzovico, Switzerland. B. Bindu, K. Lovejeet & L. Pawan, “Secure File Storage In

Cloud Computing Using Hybrid Cryptography Algorithm", International Journal of Advanced Research in Computer Science 9(2), 2017.

[13] C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", International Conference on Electrical, Computer and Communication Engineering, pp. 1-5, 2019.

[14] N Jirwan, A Singh & S Vijay, "Review and Analysis of Cryptography Techniques", Inter. J.Sci. Engineer. Res. 4(3): 1-6, 2019 Y.

[15] Sharma, H. Gupta & S.K Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", Amity International Conference on Artificial Intelligence pp.898-902. doi: 10.1109/AICAI.2019.8701398, 2019.

[16] G. Mehmood *et al.*, "An efficient and secure session key management scheme in wireless sensor network," *Complexity*, vol. 2021, pp. 1–10, 2021.

[17] H. Li and Y. Wang, "The History of Cryptography and Its Applications," *Int. J. Soc. Sci. Educ. Res.*, vol. 5, no. 3, pp. 343–349, 2022.

[18] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001.

[19] H. C. Tanuwidjaja, R. Choi, S. Baek, and K. Kim, "Privacy-preserving deep learning on machine learning as a service—a comprehensive survey," *IEEE Access*, vol. 8, pp. 167425–167447, 2020.

[20] "db616b2b65c7deafa726a20f040964ca9426851c @ flylib.com." [Online]. Available: https://flylib.com/books/en/3.190.1.29/1/

[21] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 international conference on privacy and security in mobile systems (PRISMS)*, 2014, pp. 1–8.

[22] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security algorithms for cloud computing," *Procedia Comput. Sci.*, vol. 85, pp. 535–542, 2016.

[23] L. M. Al-Ramini, "Implementation of proposed lightweight cryptosystem for use in Cloud Computing Security." Middle East University Amman, Jordania, 2018.

[24] U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, and D. N. H. Thanh, "An image

encryption scheme based on chaotic logarithmic map and key generation using deep CNN," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 7365–7391, 2022.

[25] M. redha BOUAKOUK, A. Abdelli, and L. Mokdad, "Survey on the Cloud-IoT paradigms: Taxonomy and architectures," in *2020 IEEE symposium on computers and communications (ISCC)*, 2020, pp. 1–6.

[26] A. T. Atieh, "The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges," *Res. Rev. Sci. Technol.*, vol. 1, no. 1, pp. 1–15, 2021.

[27] "nist-cloud-computing-program-nccp @ www.nist.gov." [Online]. Available: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

[28] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: a brief review," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 2, pp. 421–426, 2019.

[29] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *J. internet Serv. Appl.*, vol. 1, pp. 7–18, 2010.

[30] "438529b5b18a47ebe74f94aec903c39d95211d90@cloudscaling.com." [Online]. Available:http://cloudscaling.com/blog/cloud-computing/cloud-standards- are-misunderstood/

[31] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[32] M. A Vouk, "Cloud computing–issues, research and implementations," *J. Comput. Inf. Technol.*, vol. 16, no. 4, pp. 235–246, 2008.

[33] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[34] S. Srinivasamurthy and D. Q. Liu, "Survey on cloud computing security," in *Proc. Conf. on Cloud Computing, CloudCom*, 2010, vol. 10.

[35] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 international conference on computer science and electronics engineering*, 2012, vol. 1, pp. 647–651.

[36] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Inf. Sci. (Ny).*, vol. 550, pp. 13– 26, 2021.

[37] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and hybrid encryption techniques: a survey," in *Networking Communication and Data Knowledge Engineering: Volume 2*, 2018, pp. 239–248.

[38] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing,” *Inf. Sci. (Ny).*, vol. 387, pp. 103– 115, 2017, doi: 10.1016/j.ins.2016.09.005.

[39] R. Shaikh and M. Sasikumar, “Data classification for achieving security in cloud computing,” *Procedia Comput. Sci.*, vol. 45, pp. 493–498, 2015.

[40] C. Science, “Performance Comparison of Cryptographic Algorithms for Data Security in Cloud Computing,” *J. Inf. Comput. Sci.*, vol. 11, no. 9, pp. 1–8, 2021.

[41] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, “A Survey on the Cryptographic Encryption Algorithms,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081141.

[42] I. Publishing and G. Yao-hua, “S e n s o r s & T r a n s d u c e r s Application of the Information Encryption Technology in the Industrial Control Network Based on FPGA,” vol. 175, no. 7, pp. 226–233, 2014.

[43] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A systematic literature review on cloud computing security: threats and mitigation strategies,” *IEEE Access*, vol. 9, pp. 57792–57807, 2021.

[44] B. T. Rao, “A study on data storage security issues in cloud computing,” *Procedia Comput. Sci.*, vol. 92, pp. 128–135, 2016.

[45] U. A. Butt *et al.*, “A review of machine learning algorithms for cloud computing security,” *Electron.*, vol. 9, no. 9, pp. 1–25, 2020, doi: 10.3390/electronics9091379.

[46] . N. Khan, M. Y. Fan, A. Malik, and R. A. Memon, “Learning from privacy preserved encrypted data on cloud through supervised and unsupervised machine learning,” in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, pp. 1–5.

[47] S. Shakya, “An efficient security framework for data migration in a cloud computing environment,” *J. Artif. Intell.*, vol. 1, no. 01, pp. 45–53, 2019.

[48] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, “Towards DNA based data security in the cloud computing environment,” *Comput. Commun.*, vol. 151, pp. 539–547, 2020.

[49] N. Thein, H. A. Nugroho, T. B. Adji, and I. W. Mustika, “Comparative performance

study on ordinary and chaos image encryption schemes," in *2017 international conference on advanced computing and applications (ACOMP)*, 2017, pp. 122–126.

[50] A. Bhave and S. R. Jajoo, "Secure communication in wireless sensor networks using hybrid encryption scheme and cooperative diversity technique," in *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, 2015, pp. 1–6.

[51] S. U. Ali, E. A. Al-Ammar, B. AsSadhan, and S. D. Maqbool, "Comparative study of various security algorithms used in smart meters," in *2011 IEEE PES Conference on Innovative Smart Grid Technologies-Middle East*, 2011, pp. 1–5.

[52] S. Hraoui, F. Gmira, A. O. Jarar, K. Satori, and A. Saaidi, "Benchmarking AES and chaos based logistic map for image encryption," in *2013 ACS International Conference on Computer Systems and Applications (AICCSA)*, 2013, pp. 1–4.

[53] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution," *IJSR, India*, vol. 2, pp. 2319–7064, 2013.

[54] Z. Kartit *et al.*, "Applying encryption algorithm for data security in cloud storage," in *Advances in Ubiquitous Networking: Proceedings of the UNet'15 1*, 2016, pp. 141–154.

[55] W. Wang *et al.*, "An encryption algorithm based on combined chaos in body area networks," *Comput. Electr. Eng.*, vol. 65, pp. 282–291, 2018.

[56] K. Zaveri, N. Shah, and R. S. Mangrulkar, "Chaos Theory and Systems in Cloud Content Security," in *Handbook of Research on Cloud Computing and Big Data Applications in IoT*, IGI Global, 2019, pp. 367–390.

[57] H. K. Hoomod and M. H. Zewayr, "Image Encryption Using Modified AES with Bio-Chaotic," *Int. J. Adv. Sci. Res. Eng.(IJASRE)*, vol. 2, pp. 8–31, 2016.

[58] "2d9dea7e2aa802b0c1aca4f37b47a79d3ae05b1e @ www.brainkart.com." [Online]. Available:https://www.brainkart.com/article/AES%28Advanced Encryption-Standard%29-Structure_8408/.

[59] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[60] J. Daemen and V. Rijmen, *The design of Rijndael*, vol. 2. Springer, 2002.

[61] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly

autocorrelated data in encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 9, pp. 3106–3118, 2014.

[62] A. Anees and M. A. Gondal, "Construction of nonlinear component for block cipher based on one-dimensional chaotic map," *3D Res.*, vol. 6, pp. 1–5, 2015.

[63] Y. Alemami, M. A. Mohamed, S. Atiewi, and M. Mamat, "Speech encryption by multiple chaotic maps with fast fourier transform," *Int. J. Electr. Comput. Eng*, vol. 10, no. 6, pp. 5658–5664, 2020.

[64] A. Shakiba, "Generating dynamical S-boxes using 1D Chebyshev chaotic maps," *J. Comput. Secur.*, vol. 7, no. 1, pp. 1–17, 2020.