International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cryptographic Mechanism for Security of Cloud Computing

Geeta Rani

Scholar M.Tech. Student, Bhagat phool Singh Mahila vishwavidyalya

Abstract:
By changing current data encryption standards to enable unique hybrid cryptography mechanisms, researchers hope to improve the security of polynomial encryption-based cloud servers. Because the cloud computing movement is quickly gaining traction, the first step for every business is to pinpoint the particular region where cloud-related hazards exist. Cloud computing has accelerated the transformation of industry and government. As a result, new security issues arose. The evolution of the cloud service model as a business-supporting technology has resulted in a significant shift in computer technology. These improvements, however, have resulted in new security vulnerabilities, including security concerns whose full scope is yet unknown. This paper provides an overview and analysis of cloud computing, as well as many security issues.

Keywords: Cloud environment, Encryption, Polynomial encryption, security

[1] Introduction

Although digital content is continuously developing, there are many ways for learners in distant regions to access it online. Data transfer to and from the cloud is still fraught with danger to digital assets. But the need for better digital information security was emphasized. At the moment, the emphasis of research is on enhancing cloud-based remote learning systems in terms of security and efficiency. Many sorts of cloud computing research have been done in order to give remote learning. Previous research has shown performance and data security to be problematic. Digital files must be sent safely and quickly from one place to another. During data transport, digital content assets must be protected and compressed. Researchers employed a content replacement approach to lower the packet's size. The proposed work has been made more secure by the use of the replacement approach. Polynomial encryption is employed instead of more time-consuming encryption techniques like the AES or DES. The method is both safe & speedy since the sender compresses and encrypts the data before sending it. Many hazards can be dealt with during packet transmission using the proposed technique. This includes errors and snafus. Decompression occurs after encryption at the receiver end. The suggested approach is compared to the Rivest–Shamir–Adleman (RSA) and DNA cryptography methods. The proposed work, RSA, and DNA cryptography have all been subjected to simulated packet-level attacks. The simulation results demonstrate that the proposed technology is more secure than RSA and DNA cryptography.

1.1 Cloud Environment

To utilise cloud computing, data is stored on remote servers and accessible through the internet by any computer with an Internet connection. A excellent example of a public cloud service is Google cloud, which is open to anybody. All application development is done on Google hardware.

On-demand access to computer system resources such as processing power is provided by a cloud computing service, which does not need the user to actively manage them. The functions of large clouds are generally spread over numerous data centres. For coherence, cloud computing uses a "pay as you go" paradigm, which reduces capital costs but may potentially lead to unanticipated running charges for users who aren't aware of them.

Although service-oriented architecture advocates "everything as a service," there are three main cloud computing service models: IaaS, PaaS, and SaaS, according to NIST (SaaS). Infrastructure, platform and SaaS are often thought to be connected, although this is not necessarily the case. IaaS may be used to run applications without enclosing them in SaaS, and it can also be used to run applications and have direct access to them without having to go via SaaS first.

1. IaaS

Data partitioning, scalability, security, and backup are just some of the low-level elements of network infrastructure that may be abstracted using high level APIs. A high-level API is offered by IaaS, which is a kind of internet service. A hypervisor oversees the running of the virtual machines used by the guests. High virtual machine count and ability to expand services to meet user demand are two advantages of cloud operating systems. On a single piece of hardware, a single Linux kernel is utilised to run all the containers. To provide the isolation, security and administration of containers, the Linux kernel's cgroups and namespaces are used. Containerization is more efficient than virtualization since there is no need for a hypervisor. When it comes to infrastructure as a service (IaaS), resources like as software packages are commonly included with virtual machine disc images, raw block storage, file or object storage, firewalls, load balancers, IP addresses, and VLANs.

2. PaaS

The provider's cloud infrastructure may be used to host customer-created or purchased applications developed using the supported programming languages, libraries, services, and tools. Cloud users have limited control over the underlying infrastructure, such as the network and servers, storage, operating systems, and other software that makes up the cloud platform.

3. SaaS

The client has access to the provider's cloud-based apps and services. Web browsers and programme interfaces may be used to access applications on various client devices. The client has no control over the underlying cloud infrastructure; the cloud service provider only has access to user-specific application configuration settings.

4. Function-as-a-Service (FaaS)

With serverless computing, you don't pay per virtual machine, per hour, but rather pay a flat rate for the code execution in the cloud that the cloud provider manages entirely. Code execution without servers is

not what it sounds like, contrary to the name. There are no servers or virtual machines necessary to run back-end code when using so-called "serverless computing."

Serverless computing approach called "function as a service" (FaaS) enables the cloud-deployment of discrete functions that may be invoked on-demand in response to external triggers. FaaS is often referred to as serverless computing, while some refer to it as FaaS and serverless computing.

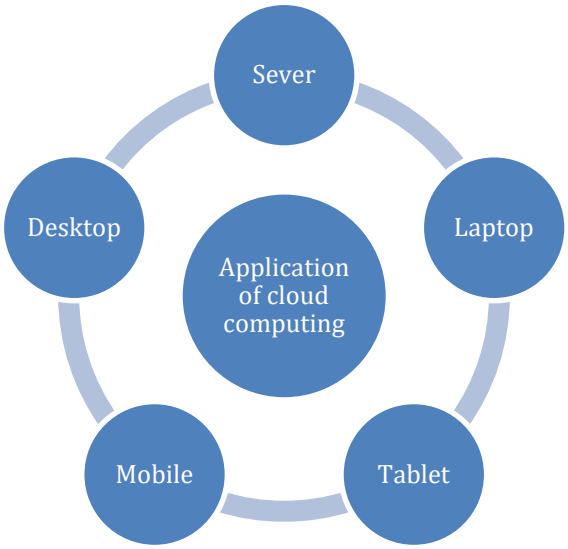

Fig 1 Cloud computing

1.2 Encryption mechanisms

Encryption algorithms are used to transform data from plaintext to ciphertext. The decryption key may be used to return the encrypted data to its original plaintext form, despite the fact that the encrypted data may seem random. The encryption key and an algorithm are used to achieve this.

Encoding data is the goal of the cryptographic procedure known as encryption. Plaintext is transformed into another kind of information known as ciphertext throughout this procedure. In an ideal world, a ciphertext can only be deciphered back to plaintext by authorised parties, preventing unauthorised individuals from seeing the original data. Encryption does not preclude interception, but it prevents a would-be interceptor from being able to decipher the message.

A pseudo-random encryption key produced by an algorithm is often used in encryption schemes for technical reasons. The message can be decrypted even if the key isn't there, but doing so would need a significant investment of processing power and expertise. The communication may be decrypted by an authorised receiver using the key supplied by the sender, but not by an unauthorised user.

Encryption is a tool used in the field of cryptography to maintain privacy. As data is accessible online, sensitive information such as passwords and personal communications may be at risk of being intercepted by hackers. Keys are used in the encryption and decryption of communications. Symmetric and public keys are the two most common forms of keys in cryptographic systems.

Even in the most complicated algorithms, basic modular arithmetic is often used in their implementation.

Symmetric key

Symmetric-key approaches use the same encryption and decryption keys to ensure security. All parties must use the same key in order to maintain the security of their communications. Messages were encoded and decoded using a new symmetric-key every day in the Enigma Machine.

Public key

Encryption keys in public-key encryption techniques are made public so that anybody may decrypt communications. The decryption key, on the other hand, can only be accessed by the person on the receiving end. A confidential paper from 1973 first outlined the concept of public-key encryption, which was previously known as symmetric-key encryption (also called private-key). 478 However, Diffie and Hellman's work was published in a well read publication after the fact, and the methodology's worth was clearly stated. The Diffie-Hellman key exchange was coined after the approach.

Another noteworthy public-key cryptosystem is RSA (Rivest–Shamir–Adleman). Although it was first developed in 1978, it is still widely used today for digital signature applications.. The RSA algorithm generates both the encryption and decryption keys by selecting two prime integers.

Pretty Good Privacy (PGP) was developed by Phil Zimmermann in 1991 and given free of charge with the source code, making it accessible to the general public. Symantec bought PGP in 2010 and periodically updates the software, making it more secure.

1.3 AES Encryption

NIST accepted Joan Daemen and Vincent Rijjen's proposal for an AES version during the selection process for the block cipher's successor. With various keys and blocks, the Rijndael family is diverse. One block size of 128 bits was chosen for each of the three Rijndael members.

U.S. government has embraced AES. Data Encryption Standard (DES), which was released in 1977, has been superseded by this new standard. AES uses a symmetric-key technique, means that same key is used to encrypt and decode the data in both directions.

1.4 DES Encryption

Digital data may be encrypted using the Data Encryption Standard (DES), a technique that uses a symmetric key. Despite the fact that its 56-bit key length is insufficient for most applications, it has had a significant impact on cryptography.

The DES may be credited with launching the non-military research and development of encryption algorithms. Academic research of cryptography was almost non-existent in the 1970s; cryptographers were mostly employed by military or intelligence agencies. There are currently a large number of active university cryptologists, mathematics departments with excellent programmes in cryptography, and commercial information security firms and consultants to draw from. A new generation of cryptanalysts has learned to break the DES algorithm by studying it. To put it another way: Bruce Schneier is a cryptography expert who has written extensively on this topic "Cryptanalysis was never the same after the invention of DES. There was an algorithm to learn about now." The DES is the gold standard against which all subsequent symmetric key algorithms have been measured in the 1970s and 1980s, when a staggering amount of free literature on cryptography dealt with it.

1.5 Limitation of existing encryption mechanism

It has been discovered that the current encryption technique consumes more time, implying that performance must be improved. DES, AES, and RSA are examples of encryption mechanisms that take more time to encode & decode data. At time of algorithm processing, there is a requirement to decrease CPU overhead. Furthermore, these security solutions are incapable of dealing with a variety of threats.

1.6 Need and motivation of research

Every day, the need for cloud-based services grows. There has been a lot of research done on the issue of cloud computing and digital content processing. However, there are certain limitations to these investigations. A number of the cloud-based methods previously exhibited for dealing with digital content lack adequate security. There is still a performance issue since protecting data takes time, but some researchers have opted to increase security. Concerns about cloud-based system performance and security are the focus of this research. There is a pressing need for a system that can both protect and speed up digital content. As a part of this research, previous studies on cloud-based online digital systems, as well as their techniques and limits, will be reviewed. To maintain the security and performance of such a system and its scope, it is necessary to enhance current research.

[2] Literature Review

There has been a lot of study done on encryption in the cloud. This section contains a summary of existing research. Polynomial encryption technique has been the subject of several studies.

In 2021, El-Attar [1] presented hybrid cryptography solutions for cloud data storage, with the purpose of enhancing data security and secrecy without depending on the CTP. ASC, ARC, and IARC are used to encrypt data chunks. We've come up with a new way to encrypt data by making the static S-box in the AES algorithm dynamic. The produced keys are protected by RSA and Twofish methods. Comparing our methods to current symmetrical key algorithms, such as DES, 3DES, and RC2, has been done.

Hermite polynomials, which may be represented as square matrices, can be added to the RSA algorithm to provide an extra layer of security, according to Raghad [2]. The RSA technique necessitates the use of very large numbers, which takes a long time to calculate; however, Hermite key encryption eliminates the need for such large numbers since the ciphertext is protected from hackers by two levels of encryption that are extremely difficult to crack.

Chong [3] studied the use of DL models in 2021 using a known plaintext circumstance. Models' goal is to predict a cipher's secret key. S-DES, Speck, Simeck, and Katan are among of the cyphers that the DL techniques are tested against, as well. A random guess is preferable than categorising the complete S-DES key set.

Thiers [4] plans to add codes for Eisenstein integers to this coding scheme in 2021. The usage of these codes helps the Niederreiter system. We advocate the use of generalised concatenated codes to further improve the code. With these codes, the work factor is more favourable than MDS in the rate area. Additionally, generalised concatenated codes are more resistant to structural assaults than traditional concatenated codes.

In 2021, LImniotis [5] plans to conduct a comprehensive assessment of all feasible cryptographic applications for the purpose of addressing privacy issues. For us, it's a chance to participate in a public debate about how law enforcement agencies might defeat encryption of communications in real time.

After Mingyang Song suggested a generic blockchain-based computing architecture in 2021, a method for secure polynomial multiplication on blockchain was developed. For polynomial multiplication and modular exponentiation, we combine the two safe outsourcing procedures using the hidden ideal lattice, resulting in an outsourcing scheme that employs homomorphic encryption and absolutely secure. [6]
Plabted [7] originally came up with the idea of completely homomorphic encryption in 2013. As a result of incorporating components of both issues, the performance of our system lies midway between that of the ideal lattice-based and integer-based techniques. Our method is based on an illustration of a problem with lower and upper limits. If we assume this security premise is valid, our system will be more efficient than both lattice-based and integer-based methods.
A. Fu [8] came up with two new and effective methods in 2018 for outsourcing exponentiation security. They outsource the modular exponentiation procedure to a single server, eliminating risk of collusion between 2 servers.
In 2012, Z. Brakerski proposed an unique tensoring method for LWE-based totally homomorphic encryption. The noise in the ciphertext has previously grown exponentially in previous research, whereas ours grows linearly (B B • poly(n)). When utilizing this method, scale-invariant totally homomorphic encryption schemes may be built, which only rely on the ratio of modulus q and beginning noise level B, and not on their absolute values.
According to D. Harvey [10], in his article released in 2019, polynomials of degree n in Fp[X] may be multiplied the bit operations. When it was first discovered, it was the best-known limit.

[3] Problem Statement

A number of researches have been conducted in the topic of cloud security, but those studies relied on the usage of standard encryption technology. Many researches have been done on cloud computing, though. However, no practical solution came out of these investigations. A new system that combines cloud computing must be created in order to boost cloud security. There have been many authors that have worked on cloud security, yet some limits have been recognized. A number of encryption approaches have been used to secure cloud environments. Confidence in and performance of encryption methods are limited. According to the above considerations, the proposed work includes.

[4] Need of Research

Current cloud computing security research and existing encryption technologies must be taken into account. Focusing on issues that affect cloud computing security is necessary because of these systems' workings and limitations. Encryption is an important part of cloud computing security. To keep the cloud safe from intrusions from the outside world, new approaches based on encryption are required. On the other hand, it is necessary to compare the security and dependability aspects of classic and modern research.

[5] Conclusion

A new hybrid automated security architecture for Cloud storage systems is being shown to these companies. By exploiting Hermite polynomials, researchers are working to improve the RSA cryptosystem. We'll be looking at how deep learning can be used to improve security analysis for cryptography algorithms. Generalized concatenated codes over Gaussian and Eisenstein ints for

generalised code-based cryptography is the name given to this effort in the cryptography field. A research shows that cryptography may be used to defend fundamental human rights. Researchers call their work "Blockchain-Based Secure Outsourcing of Polynomial Multiplication and Its Use in Fully Homomorphic Encryption." It is explained how the project will work. "Fully homomorphic" encryption with an ideal lattice that is hidden and doesn't change its modulus from classical gapsvp. Privacy work is ensuring that composite modular exponentiation outsourcing with the best checkability can be done in a single untrusted cloud server. research is shown. Using cyclotomic coefficient rings, you can do polynomial multiplication faster over finite fields. Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on fpga, and a new Jochemsz–May cryptanalytic bound for RSA systems with a common modulus N= p2q are some of the things being worked on. ZigBee security is getting better thanks to the RSA public algorithm used in WSN.

[6] Scope of Research

In the future, it's possible that even better compression techniques may be created. Future research may uncover new methods to enhance safety. Future research may leverage advanced cloud services and optimization methods to increase performance while decreasing error rates. The quality and reliability of service may be improved using soft computing technologies. It's possible that researchers may examine the cloud's high availability and zero downtime to determine if they can boost its reliability in real-life applications.

References

1. El-Attar, N.E.; El-Morshedy, D.S.; Awad, W.A. A New Hybrid Automated Security Framework to Cloud Storage System. *Cryptography* **2021**, *5*, 37. https://doi.org/10.3390/cryptography5040037
2. Raghad K. Saliha. Optimizing RSA cryptosystem using Hermite polynomials. Int. J. Nonlinear Anal. Appl. 13 (2022) 1, 955-961 ISSN: 2008-6822 (electronic) http://dx.doi.org/10.22075/ijnaa.2022.5614
3. Chong, B.; Salam, I. Investigating Deep Learning Approaches on the Security Analysis of Cryptographic Algorithms. Cryptography 2021, 5(4), 30; https://doi.org/10.3390/cryptography5040030.
4. Thiers, J.; Freudenberger, J. Generalized Concatenated Codes over Gaussian and sEisenstein Integers for Code-Based Cryptography. Cryptography 2021, 5(4), 33; https://doi.org/10.3390/cryptography5040033.
5. Limniotis, K. Cryptography as the Means to Protect Fundamental Human Rights. Cryptography 2021, 5(4), 34; https://doi.org/10.3390/cryptography5040034.
6. Mingyang Song , Yingpeng Sang , Yuying Zeng , and Shunchao Luo. Blockchain-Based Secure Outsourcing of Polynomial Multiplication and Its Application in Fully Homomorphic Encryption. Volume 2021 |Article ID 9962575 | https://doi.org/10.1155/2021/9962575
7. T. Plantard, W. Susilo, and Z. Zhang, "Fully homomorphic encryption using hidden ideal lattice," *IEEE transactions on information forensics and security*, vol. 8, no. 12, pp. 2127–2137, 2013.
8. A. Fu, S. Li, S. Yu, Y. Zhang, and Y. Sun, "Privacy-preserving composite modular sexponentiation outsourcing with optimal checkability in single untrusted cloud server," *Journal of Network and Computer Applications*, vol. 118, pp. 102–112, 2018.

9. Z. Brakerski, “Fully homomorphic encryption without modulus switching from classical gapsvp,” in *Proceedings of the Annual Cryptology Conference*, pp. 868–886, Santa Barbara, CA, USA, August 2012.
10. D. Harvey and J. van der Hoeven, “Faster polynomial multiplication over finite fields using cyclotomic coefficient rings,” *Journal of Complexity*, vol. 54, Article ID 101404, 2019.
11. W. Liu, S. Fan, A. Khalid, C. Rafferty, and M. O’Neill, “Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on fpga,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 10, pp. 2459–2463, 2019.
12. N.N.H. Adenan, M.R. Kamel Ariffin, S.H. Sapar, A.H. Abd Ghafar and M.A. Asbullah, New Jochemsz–May cryptanalytic bound for RSA system utilizing common modulus N= p2q, Mathematics, 9 (4) 2021 340.
13. N.A. Hassan and A.K. Farhan, Security improves in ZigBee protocol based on RSA public algorithm in WSN, Engin. Tech. J. 37(3B) (2019) 67–73.
14. R.K. Salih and M. S. Yousif, Hybrid encryption using playfair and RSA cryptosystems, Int. J. Nonlinear Anal. Appl. 12(2) (2021) 2345–2350.