The Application of Cryptographic Techniques to an Explicit Area of Computer Networks (Cloud Computing)

K.G.M.Sisira Kumara
Department of Computer Science and Data Science
National School of Business Management
gihan.sisirakumara2000@gmail.com

Abstract: **Cloud computing provides internet data storage, infrastructure, and applications, as well as remote control over devices and programming assets. But because administrators handle client information outside of their purview, security issues arise. Reliable security and protection are essential. The art of cryptography involves using various encryption techniques to safeguard and secure cloud data. Cloud computing uses a variety of cryptography-based encryption approaches to safeguard data that is utilized or stored there. Cryptography is used in various patterns to protect user data during these data communication via in the cloud. In this paper, specific security issues arising from the use of cryptography in cloud computing systems are surveyed, along with methods for implementing data security solutions that offer trustworthy security and safeguard sensitive data. These solutions include cloud data protection via encryption and cryptographic key management.**

Index Terms: Cloud Computing, Encryption, Cryptography

I. Introduction

The process of hiding information to maintain confidentiality during sensitive data transmission and communication is known as cryptography[1] Cryptography is derived from geek word krypton meaning hidden, secret and graphene, meaning writing or study. It is the study of the science and art behind securing communication of any third parties or public. Nowadays cryptography is highly based on mathematical theory, algorithms, and computer science practice.[2] Now we must understand how Cryptography is protected data & information. In here the important information is protected by cryptography, which transforms it into unintelligible data that is only accessible to authorized recipients. These recipients then transform the unintelligible data back into the original text. Encryption is the process of using a specific key to transform original text into unclear text (ciphertext); decryption is the process of doing the opposite of encryption.[3]

Cryptography Terminologies:

- Plain Text: It is same as human language. It is understood by the sender who generates the message, the recipient anyone who gets accessing that message.
- Cipher Text: The Cipher meaning is secret message. A message that results from codifying a plain text with any appropriate scheme is referred to as cipher text.
- Encryption: Encryption is the process of converting plain text transmissions into cipher text messages.
- Decryption: the process of translating messages from encryption text back to plain text.
- Key: This is the most important feature in cryptography and that is needed for both encryption and decryption is what gives cryptography its security.[2]

Purpose of Cryptography:

- Confidentiality: It is configured that the message which is secure by the cryptography, can be accessed only sender and receiver.
- Authentication: Mechanisms for authentication aid in establishing identity proof.
- Integrity: The integrity mechanism makes sure that the message's contents are exactly as they were delivered by the sender and arrive to the intended destination.
- Non-repudiation: A message's sender cannot dispute the assertion that they did not send it if they choose not to repudiate their message.
- Access Control: Who can access what is specified and controlled by access control.
- Availability: According to the availability principle, resources should always be accessible to those who are authorized.[2]

Nowadays the cloud system is the most popular platform for communication, sharing and stored data. For example, we can study about the bank system in our world. Nowadays, the internet is used for all tasks pertaining to banking, credit cards, ATMs, marketing, e-commerce, etc. Therefore, network protection must be offered. As a result, we employ a number of cryptography approaches for safe communication. We utilize various encryption methods to safeguard confidential data from unwanted access. In a cryptosystem, confidential communication is maintained by using encryption to secure data. Everyone encrypts their private messages before sending them, and the intended recipient uses their key to decrypt them. Perhaps the most crucial component of communication security is cryptography, which is also playing a bigger role as a fundamental component of computer security.[4]

II. Literature Review

The concept of cloud computing dates back to the 1960s, when John McCarthy used network diagrams that represented mutual master groups to forecast that computers will eventually be found in public utility areas**.**[5]A new secured cloud computing architecture known as "crypto cloud computing" is made up of a number of abstract, virtualized, dynamically-scalable, and managed resources, including platforms, services, processing power, and storage. In the here have 3 different type of cloud system,

- Public clouds: They include publicly accessible web applications.
- Community clouds: A collection of individuals with shared objectives and worries would use this cloud.
- Hybrid clouds: By combining many clouds, this would provide a greater range of developing apps and combining them in different ways.[5]

Ensuring privacy while developing a "SaaS" is one of the most important privacies concerns we are now dealing with. Hacking becomes a simple game while working on open files that have been encrypted. A thorough understanding of the various phases of data transmission is necessary to guarantee security in clouds. One fundamental technique that has been a significant component of cryptography is public key encryption. Understanding how it operates is still vital even when it is becoming older. Use sending an email as a general illustration. For example, your email address would be the public key. The public can send you emails, but they are unable to read your correspondence. They draft an email, encrypt it using your public key, and then send it to you. They only know how to encrypt the message using your public key after this has occurred, so they are unable to reverse the message since they are unable to open your lock. You must sign into your email account in order to view the message.[5]

It can provide system-level information security and provide accurate and convenient user access to shared services. Here, the sender's plain text message is encrypted using a cryptographic method to create a unique format known as "Cipher Text." After that this cipher text message is communicated via the network. By using a decryption technique, the recipient decrypts the encrypted text communication back into the original plain text. So that this special message which is secured by cryptography, can read only to sender and receiver.[6] A person's network with the outside world is protected with crypto cloud computing. It can guarantee personal safety without any information lag. Cloud architectures are created on-demand, allocating resources to users in response to their requests and then releasing those resources once the task is finished.[7] As Crypto cloud computing is based on the Quantum Direct Key system and QDK is a set of sophisticated asymmetric offline key mechanism. So Crypto cloud computing can avoid network traffic congestion, and other drawbacks of cloud data using current encryption system. This encryption technology enables entities to produce public keys offline without third-party assistance.[8] We called as a cipher text message which is obtained by applying cryptographic techniques to the encrypted message. Three different kinds of cryptography methods exist. Those are Symmetric Key Cryptography, Asymmetric key cryptography and Hash Function Cryptography.[6] Below figure1 show how cryptography is communication. Now we are looking for the various cryptography Technik for cloud computing area.

A. *Symmetric Encryption Algorithm (Secret Key Cryptography)*

One key is used by the symmetric encryption algorithm for both encryption and decryption.

- Data Encryption Standard (DES):
  The data encryption standard known as DES employs a secret key for both encryption and decryption. It uses a 64-bit secret key, of which 8 bits are needed for error detection and 56 bits are created at random. It uses the Data Encryption Algorithm (DEA), a secret block cipher that operates on 64-bit blocks with a 56-bit key. An algorithm that converts a fixed-length string of plaintext bits into a ciphertext bit string of the same length is the classic block cipher. The DES design enables single-user encryption, such as files saved in encrypted form on a hard drive, to be implemented in hardware.
- Advanced Encryption Standard (AES):
  The AES technique uses a symmetric key algorithm, meaning that the same key is used for both encryption and decryption. It is based on a National Institute of Standards and Technology (NIST) specification for encrypting electronic data. It is an iterated block cipher that operates by repeatedly carrying out the specified actions. Its block size is 128 bits, and its key sizes are 128 bits for AES-128, 192 bits for AES-192, and 256 bits for AES-256. AES's design facilitates efficient use across various network tiers and in both software and hardware.

B. *Asymmetric Encryption Algorithm (Public-Key Cryptography)*

The purpose of this encryption technique was to address issues with key management. A public key and a private key are both involved. While the sender maintains the private key confidential, the public key is made available to the public. Asymmetric encryption helps to guarantee confidentiality, integrity, authentication, and nonrepudiation in data management by using a key pair consisting of a public key that is accessible to everyone and a private key that is held exclusively by the key owner.

- Rivest Shamir Adleman (RSA) Algorithm
  A public-key cryptosystem called RSA is used for Internet authentication and encryption. RSA computes utilizing two huge prime numbers by applying elementary number theory and modular arithmetic . There are many different products, platforms, and sectors that employ the RSA system. One of the accepted encryption standards is this one. Operating systems from companies like Novell, Apple, and Microsoft incorporate RSA algorithms. The most widely used asymmetric algorithm is RSA. The security of the RSA algorithm is based on the computational difficulty of factoring huge integers that are the product of two large prime numbers. It's simple to multiply two prime numbers, but the complexity of determining the original numbers from the product is the foundation of RSA.

- Elliptic Curve Cryptography (ECC)
  Modern public-key cryptography called ECC was created to prevent the use of more cryptographic keys. The asymmetric cryptosystem creates a short, fast, and reliable cryptographic key using number theory and mathematical elliptic curves (algebraic structure). The tiny key size of the Elliptic Curve Cryptography (ECC) technique has led to proposals to replace the RSA algorithm with it.[9]

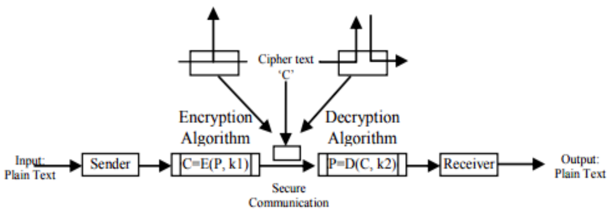

Figure 1: Cryptography Communication

III. FUTURE DIRECTION

Nowadays cloud computing is a very famous platform for a lot of services. for example, it is a software as a service, platform as a services and infrastructure as a service. So many users use cloud computing for stored data and to communication.[10]. Figure 2 show layers of cloud model.

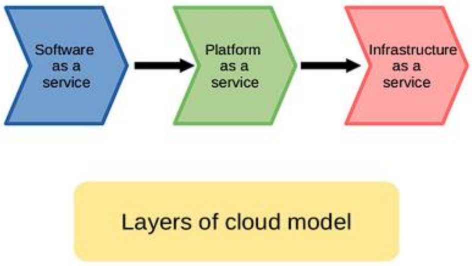

Figure 2: Layers of Cloud Computing Model

So, Cloud computing poses security challenges that have already been discussed by a number of researchers. It is stated unequivocally that the biggest obstacle to cloud computing adoption has been security related.[8] Numerous cloud companies, including Google, Amazon, and Microsoft, have implemented cryptography security safeguards to safeguard customer data housed on their cloud systems.[9].Figure3 show security problem of cloud platform.

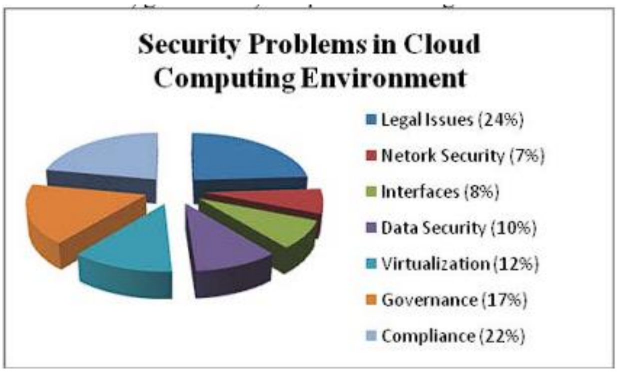

Figure 3: Security Problem in Cloud Computing Environment

In cryptography technology, currently use symmetric techniques, asymmetric techniques and algorithms to protect communication data.[11] Future advancements in cloud computing security and privacy can be made in a number of ways by integrating cryptography.

- Homomorphic Encryption for Secure Data Processing:
  Computations on encrypted data can be done without having to first decrypt it thanks to isomorphic encryption. Data secrecy can be preserved while processing data securely in the cloud with the integration of homomorphic encryption. Subsequent investigations may concentrate on enhancing the efficiency of homomorphic encryption algorithms to render them more applicable for practical cloud applications.

- Post-Quantum Cryptography:
  Traditional cryptography techniques may become more susceptible to assaults as quantum computing advances. The goal of post-quantum cryptography is to create encryption protocols that can withstand quantum attacks. One key line of inquiry for ensuring the long-term security of cloud-based systems is whether or not post-quantum cryptography techniques can be implemented in cloud contexts.

- Multi-Party Computation for Secure Collaboration:
  Several parties can collaboratively calculate a function over their private inputs while maintaining the confidentiality of those inputs thanks to multi-party computation (MPC). Cloud computing can benefit

from the secure collaboration of multiple users without sacrificing data privacy with the integration of MPC techniques. Future work may concentrate on creating effective and scalable MPC protocols for cloud-based applications, particularly in situations where sharing and analysis of sensitive data is involved.

- Blockchain-Based Security and Auditing:
  A decentralized, unchangeable ledger for safely documenting transactions is provided by blockchain technology. Data integrity, accountability, and transparency can all be improved by integrating blockchain technology with cloud computing. Subsequent investigations may examine innovative methods of utilizing blockchain technology to fortify security and auditing protocols in cloud-based systems. For example, smart contracts may be employed to enforce access control regulations and document audit trails.[12], [13], [14]

- IaaS Cloud Model:

  Public clouds struggle to meet the requirement for storage owners to not access or alter the data, as computations cannot be performed on encrypted data. In order to prevent keys from being disclosed to other tenants or administrators, cloud providers offer Cryptography as a Service (CaaS), giving users control over encryption and decryption activities.[15]

IV. CONCLUSION

Algorithms, computer science practice, and mathematical theory form the foundation of cryptography. It turns crucial information into incomprehensible data that is only available to those who are permitted to access it. Decryption is the reverse of encryption, which is the process of converting original text into ambiguous text (ciphertext) using a unique key. Terms used in cryptography include encryption, decryption, plain text, and cipher text. Its goal is to guarantee availability, non-repudiation, integrity, confidentiality, and authentication. Network security has become essential with the growth of cloud computing and the internet. Secret information is protected via cryptography, which encrypts private messages before sending them and uses a key to decipher them. Asymmetric encryption, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rist Shamir Adleman (RSA), symmetric encryption, and elliptic curve cryptography (ECC) are among the cryptography techniques used in cloud computing. DES employs a 64-bit secret key along with DEA, a secret block cipher, whereas symmetric encryption uses a single key for both encryption and decryption. With 128-bit block and key sizes, AES is an iterated block cipher. Using a public key and private key, asymmetric encryption ensures data management's secrecy, integrity, authentication, and nonrepudiation while addressing key management concerns. RSA is a popular public-key cryptosystem that leverages the difficulty of factoring large integers to provide encryption and authentication over the internet. Using number theory and mathematical elliptic curves, ECC is a contemporary public-key cryptography that generates a short, quick, and trustworthy cryptographic key. There have been suggestions to replace the RSA algorithm due to the small key size of ECC. Software as a service, platform as a service, and infrastructure as a service are just a few of the services that are offered on the well-known cloud computing platform. Security is still a major obstacle to its adoption, though. Businesses including Microsoft, Amazon, and Google have used cryptography to safeguard consumer. The approaches used now include algorithmic, symmetric, and asymmetric strategies. Cryptography can be integrated to accomplish future security and privacy breakthroughs in cloud computing. Post-quantum cryptography seeks to develop encryption algorithms that are resistant to quantum assaults, whereas homomorphic encryption permits secure data processing without the need for decryption. Secure collaboration is made possible by multi-party computation (MPC), which protects data privacy. Transparency, accountability, and data integrity can all be enhanced by blockchain-based security and auditing. By giving users authority over encryption and decryption processes, the IaaS cloud model satisfies the demand for safe communication and storage.

REFERENCES

[1] R. Denuwan and R. Denuwan Godage, “Cryptographic Techniques Cryptographic Techniques Cryptographic Techniques”, doi: 10.13140/RG.2.2.17003.21282.

[2] S. Mal, U. Banerjee, and B. Tech, “Cryptographic Techniques,” 2017. [Online]. Available: www.ijedr.org

[3] Y. Alemami, M. A. Mohamed, and S. Atiewi, “Research on various cryptography techniques,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 2 Special Issue 3, pp. 395–405, Jul. 2019, doi: 10.35940/ijrte.B1069.0782S319.

[4] A. Krishna A and L. C. Manikandan, “A Study on Cryptographic Techniques,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 321–327, Jul. 2020, doi: 10.32628/cseit206453.

[5] K. Rauber, “Cloud cryptography,” *International Journal of Pure and Applied Mathematics*, vol. 85, no. 1, pp. 1–11, 2013, doi: 10.12732/ijpam.v85i1.1.

[6] S. R. Pardeshi, V. J. Pawar, and K. D. Kharat, “Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques.”

[7] W. J. Akram Gdc Mendhar, “A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography).” [Online]. Available: https://www.researchgate.net/publication/348674997

[8] W. J. Akram Gdc Mendhar, “A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud

Cryptography).” [Online]. Available: https://www.researchgate.net/publication/348674997

[9] I. Lartey and F. Bentil, “Cloud Cryptography-A Security Aspect.” [Online]. Available: https://www.researchgate.net/publication/351991473

[10] M. U. Sana, Z. Li, F. Javaid, H. Bin Liaqat, and M. U. Ali, “Enhanced Security in Cloud Computing Using Neural Network and Encryption,” *IEEE Access*, vol. 9, pp. 145785–145799, 2021, doi: 10.1109/ACCESS.2021.3122938.

[11] G. H. Ching and M. F. Zolkipli, “Review on Cryptography Techniques in Network Security,” *Journal of ICT in Education*, vol. 8, no. 2, pp. 125–135, 2021, doi: 10.37134/jictie.vol8.1.10.2021.

[12] W. J. Akram Gdc Mendhar, “A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography).” [Online]. Available: https://www.researchgate.net/publication/348674997

[13] G. H. Ching and M. F. Zolkipli, “Review on Cryptography Techniques in Network Security,” *Journal of ICT in Education*, vol. 8, no. 2, pp. 125–135, 2021, doi: 10.37134/jictie.vol8.1.10.2021.

[14] S. Goyal and S. Jain, “A secure cryptographic cloud communication using DNA cryptographic technique.”

[15] B. Albelooshi, K. Salah, T. Martin, and E. Damiani, “Securing Cryptographic Keys in the IaaS Cloud Model,” in *Proceedings - 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing, UCC 2015*, Institute of Electrical and Electronics Engineers Inc., 2015, pp. 397–401. doi: 10.1109/UCC.2015.64.