Cloud Security Aspects using Homomorphic Encryption: A Review

Dipti Gautam[1], Rakesh Shivhare[2]
[1]Department of CSE, Radharaman Engineering College, Bhopal (M.P.), India
[2]Department of CSE, Radharaman Engineering College, Bhopal (M.P.), India
[1]gautamdipti9644@gmail.com

* Corresponding Author: Dipti Gautam

Abstract: *A group of rules, controls, procedures, and technologies come together to form cloud security, often referred to as cloud computing security, in order to safeguard the infrastructure, data, and systems that are hosted in the cloud. These security procedures are set up to safeguard cloud data, assist with regulatory compliance, safeguard consumer privacy, and establish authentication policies for particular users and devices. The provider is always responsible for the security of the infrastructure, including adding security to, patching, and configuring the hardware hosts and physical networks that house the computing instances, storage, and other components. The different kinds of cloud settings and the value of cloud security are discussed in this study. In addition, we went over an overview of the symmetric encryption method utilized for cloud security.*

Keywords:. *cloud, cloud security, Iaas, Paas, Saas, homomorphic encryption,*

I. Introduction

The transmission of hosted services, such as software, hardware, and storage, through the Internet is known as cloud computing. The advantages of rapid adoption, flexibility, low initial costs, and scalability have practically forced enterprises of all sizes to use cloud computing, frequently as a component of a hybrid/multi-cloud infrastructure architecture. The technology, rules, procedures, and services that shield cloud data, application, and infrastructure against dangers are referred to as cloud security [1].

A group of rules, controls, procedures, and technologies come together to form cloud security, often referred to as cloud computing security, in order to safeguard the infrastructure, data, and systems that are hosted in the cloud. In addition to establishing authentication policies for certain users and devices, these protective measures are configured to safeguard cloud data, support regulatory compliance, secure customers' privacy, and protect cloud data [2,3]. Cloud security can be customized to precisely meet the requirements of the company, from verifying access to traffic filtering. Additionally, administrative costs are decreased and IT teams are freed up to concentrate on other aspects of the business because these rules can be created and handled in a single location.

Figure 1 Importance of cloud security

Both the cloud service provider and the client are accountable for cloud security. In the Shared Responsibility Model, responsibilities fall into three general categories: those that are always the provider's, those that are always the customer's, and those that change depending on the service model: Cloud email is an example of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) [4-6].

The provider is always responsible for the security of the infrastructures, including controlling access to, patching, and configuring the physical hosts and physical networks that house the computing instances, storage, and other resources.

The client is always accountable for supervising users and their access privileges (identification and access management), preventing unwanted access to cloud accounts, encrypting and securing cloud-based data assets, and regulating its security posture (compliance).

II. TYPES OF CLOUD ENVIOURONMENTS

1. Public clouds
Third-party cloud services host cloud service. Since the provider takes care of everything, a business doesn't need to set up anything to use the cloud. Clients typically use web browsers to access a provider's web services. Public clouds must have security features like access control, password protection, and authentication.

2. Private clouds
Since private clouds are often assigned to a single group or person and depend on that group's or user's firewall, they are frequently more secure than public clouds. Since only one institution can access these clouds, their isolation aids in keeping them safe from outside attacks. However, some risks, such as social engineering and breaches, continue to pose security concerns. As the needs of your business grow, scaling these clouds may prove challenging.

3. Hybrid clouds
In hybrid clouds, better resource control provided by private clouds is combined with the scalability of public clouds. These clouds link several settings that can scale more easily dependent on demand, such as a private cloud and a public cloud. Users can access all of their environments through an unified system content management portal in successful hybrid clouds.

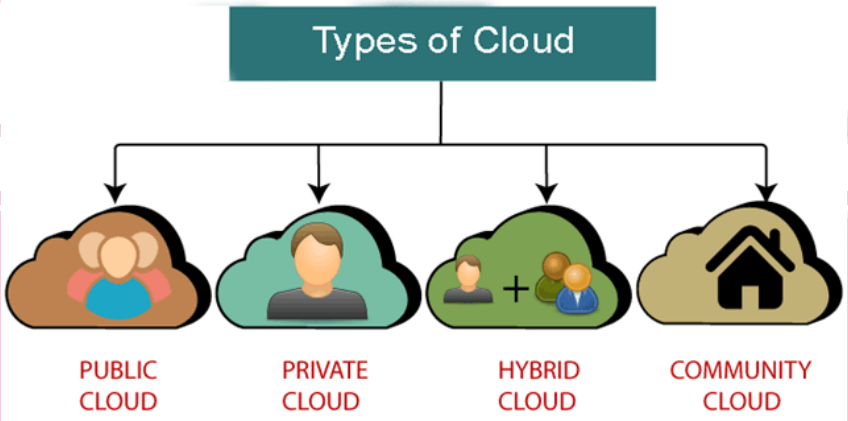

Figure 2 Different Types of Clouds

III. HOMOMORPHIC ENCRYPTION

In contrast to conventional encryption techniques, homomorphic encryption enables computing to be done directly on encrypted data without the need for a secret key. The outcome of such a calculation is preserved in encrypted form and may eventually be made public by the holder of the secret key [9]. How organizations and people use and manage their data has fundamentally changed thanks to affordable cloud computing and cloud storage. Traditional encryption techniques, such AES, are incredibly quick and make it possible to store data comfortably encrypted.However, the owner of the data must download, decode, and act on the encrypted data locally, which can be expensive and provide a logistical barrier [14,15], or the cloud server must have access to the secret key, raising security issues. Because the cloud may directly process the encrypted data and only provide the encryption output to the data owner, data encryption can greatly simplify this scenario. Buyer and seller having private data that a third party can access in more complicated application situations can be involved, and the result can be returned to one or more participants for decryption.

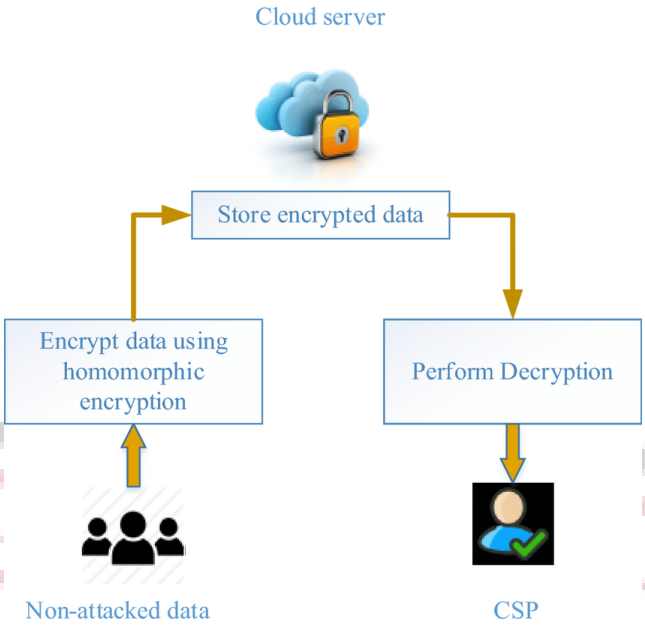

Figure 3 Cloud Security using Homomorphic Encryption

The Ring-Learning With Errors (RLWE) problem, a challenging mathematical problem associated with high-dimensional lattices, is the foundation for the security of the majority of effective rsa algorithm cryptographic techniques. In particular, the security premise underlying these encryption methods is that if the encryption method can be efficiently overcome, so can the RLWE problem. We are certain that these techniques are in fact at least as safe as any standardized cryptosystem because there is a substantial body of peer-reviewed research demonstrating the difficulty of the RLWE problem [12].

The RLWE problem is closely connected to well-known hard lattice problems, which are now thought to be secure against supercomputers, as was already described above. Similar to factorization and discrete logarithm-based systems, such as RSA and many types of elliptic curve cryptography, RLWE is thought to be secure against quantum computers. As a result, most homomorphic encryption algorithms are also thought to be secure against quantum computers. In fact, some submissions to the NIST-sponsored post-quantum cryptography standardisation project were based on hard lattice issues resembling those employed by contemporary encryption algorithm [13].

IV. Literature review

Arif Sari [1] One method for detecting intrusions is the anomaly detection system. The identification of odd activity in cloud networks is a branch of the cloud environment that has recently developed. Although there are many Access Control technologies developed in the cloud environment, this review paper highlights various IDS in cloud networks through various categorizations and conducts a comparative study on the security precautions of Dropbox, Google Drive, and iCloud to highlight their strengths and weaknesses in terms of security.

Yazan Al-Issa [2] Examine the problems associated with cloud security and confidentiality as well as how cloud computing is used in the healthcare sector. The centralized storage of data on the cloud gives rise to several security and privacy issues for patients and healthcare professionals. The loss of control over sensitive data occurs as a result of (1) the centralization of data and (2) the transfer of data ownership to cloud service providers. This gives hackers a one-stop honeypot from which to steal and intercept data in-motion. As a result, issues with security, privacy, effectiveness, and adaptability are preventing the widespread use of cloud computing. In our work, we discovered that the cutting-edge solutions only fully solve a portion of those issues. -us, there is an urgent need for a comprehensive solution that strikes a balance between all the conflicting demands.

RiddhiDoshi [3] addressed the challenges with cloud computing and some of the ensuing models that were put forth to address them.

DuyguSinanc [4] discusses security aspects, models, dangers, and precautions with regard to cloud computing. The most recent articles were categorized, and after that, they were examined for issues, solutions, and challenges. Conclusion: When evaluating dangers, standards, measurements, and metrics must first be thoroughly considered before being put into practice.

The method of contingency analysis is frequently used to foresee outcomes of outages, such as failures of apparatus, conductor, etc., and to demand necessary actions to maintain the facility system's security and dependability. Given the sheer number of components in a power system, conducting an offline analysis to determine the effects of each individual

contingency could be time-consuming. This review paper provides several contingency analysis techniques, and it also cites the use of artificial neural networks for contingency analysis.[5].

CLAUDIO A. ARDAGNA [5] focuses on the intersection of cloud security assurance and cloud security. First, we give a quick rundown of the most recent developments in cloud security. The idea of cloud security assurance is then discussed, and its expanding influence on cloud security methods is examined. We conclude by offering some suggestions for the creation of subsequent-generation cloud security and authentication solutions.

Mohamed Alloghani [6] use the PRISMA checklist in addition to a few elements of the Cochrane Quality Assessment to evaluate papers acquired from different sources. It was clear from the publications we evaluated that big data and cloud security had gotten the most attention. Although additional possible issues have been found by the qualitative data, homomorphic encryption was recommended in the majority of studies. The explicit declaration of research aims, acknowledgment of the technique, and sources of financing employed in the study were three criteria that 38% of the articles did not match.

Goiuri Peralta [7] review of the NC and HE advantages over the entire IoT cloud architecture industry. The infrastructure may provide a variety of benefits by combining the two technologies: The first benefit is that it offers complete data privacy, from end users to end devices. Second, without worrying about their privacy, sensitive data can be kept in public cloud systems.

Dabeeruddin Syed [8] recommends the use of encryption techniques, which makes it possible to train both traditional and deep learning machine learning models while maintaining the data's security and privacy. Applications of fault localization and identification, as well as load forecasting in smart grids, are tested using the suggested methodology. The classifications accuracy of the proposed privacy-preserving deep learning model when utilizing cryptographic algorithm is 97-98%, which is comparable to 98-99% classification accuracy of the model on plain data, according to the fault diagnosis results.

AbdulatifAlabdulatif [9] provide a decentralised analytics platform for huge data on the cloud that protects privacy. A new and potent cryptosystem that can perform analytical operations on encrypted data is called Fully Homomorphic Encryption (FHE). The scaleability of the developed distributed technique allows for the division of data and analytical calculations into smaller groups of cloud computing nodes that can act freely. This significantly improves the performance of interpreting encrypted data while maintaining a high level of assessment accuracy.

Weichao Gao [10]By utilizing the idea of hash - based cryptography and protected network protocol design, the problem of privacy protection for data auction in CPS is addressed. Our proposal is a general Privacy-Preserving Auction Scheme (PPAS), in which an unreliable third-party trade platform is made out of the two independent entities of the auctioneer and intermediate platform. A winner in the auction can be identified and all bidder information is hidden by using cryptographic algorithm and a one-time pad. We also suggest an Enhanced Privacy-Preserving Auction Scheme (EPPAS), which makes use of an extra signature verification technique, to further increase the security of the privacy-preserving auctions.Both schemes' viability is confirmed through in-depth theoretical analysis and thorough performance tests, which also include an examination of attack resilience. Additionally, we go over several unresolved problems and scheme extensions.

PAULO MARTINS [11] The more potent and modern Fully Searchable symmetric Encryption (FHE) schemes are thoroughly investigated, along with both the old and new Somewhat Homomorphic Encryption (SHE) schemes. These schemes' supporting principles are provided, and an engineering analysis of their security and effectiveness is done.

Xuechao Yang [13] I suggest an online voting approach that takes these issues into account: ranked choice. It removes all inbuilt constraints on the potential distribution of points among competitors in accordance with the preferences of the voters. Each ballot cast is encrypted using the polynomial ElGamal encryption algorithm before submission in order to maintain the privacy of the votes. Additionally, the system makes sure that proofs are created and saved for each component of the cast ballot during voting. The performance and safety analyses presented in this research show that our technique has significantly outperformed the earlier systems. The results of our tests also demonstrate the viability of our suggested techniques for actual use.

Jian Zhang [14]we provide a Generic technique to create a Secure Cloud Storage protocol, abbreviated as G-SCS, utilizing any rsa algorithm encryption scheme. This is the first attempt to study the intrinsic relationship between secure cloud storage and homomorphic encryption strategy (HES). According to a definition that satisfies the security prerequisite for cloud storage, the proposed G-SCS is secure. We further extend the protocol to support predetermined and randomly allocated auditing, data dynamics (i.e., data insertion, deletion, and modification), as well as third-party public auditing, while maintaining the efficiency and security of the protocol, to address various issues in real application scenarios.We build different concrete secure cloud storage mechanisms employing RSA-based, Paillier-based, and DGHV-based HESs, which are computational complexity, composite, and entirely HESs, respectively, by inserting a new all abstract semantics in G-SCS.

Y. Lu, M. Zhu [15] explores the secure execution of a dispersed projected gradient-based algorithm by a system operator and a group of agents. Each participant, in particular, is in possession of a set of problem coefficients and/or states, the values of which are known only to the data owner. Two issues are brought up by the topic at hand: how to safely generate the given functions, and which functions should even be computed at all.

V. CONCLUSION

A group of rules, controls, methods, and technologies come together to form cloud security, often referred to as cloud computing security, in order to safeguard the infrastructure, data, and systems that are hosted in the cloud. The different kinds of cloud settings and the value of cloud security are discussed in this study. In addition, we went over an overview of the symmetric encryption method utilized for securing data.

REFERENCES

[1] Sari, Arif (2015). A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security, 6(2), 142–154. doi:10.4236/jis.2015.62015

[2] Al-Issa, Yazan; Ottom, Mohammad Ashraf; Tamrawi, Ahmed (2019). eHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering, 2019(), 1–15. doi:10.1155/2019/7516035

[3] Doshi, R., &Kute, V. (2020). A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models. 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). doi:10.1109/ic-etite47903.2020.37

[4] Sinanc, Duygu; Sagiroglu, Seref (2013). [ACM Press the 6th International Conference - Aksaray, Turkey (2013.11.26-2013.11.28)] Proceedings of the 6th International Conference on Security of Information and Networks - SIN '13 - A review on cloud security. , (), 321–325. doi:10.1145/2523514.2527013

[5] Ardagna, Claudio A.; Asal, Rasool; Damiani, Ernesto; Vu, QuangHieu (2015). From Security to Assurance in the Cloud. ACM Computing Surveys, 48(1), 1–50. doi:10.1145/2767005

[6] Alloghani, Mohamed; M. Alani, Mohammed; Al-Jumeily, Dhiya; Baker, Thar; Mustafina, Jamila; Hussain, Abir; J. Aljaaf, Ahmed (2019). A systematic review on the status and progress of homomorphic encryption technologies. Journal of Information Security and Applications, 48(), 102362–. doi:10.1016/j.jisa.2019.102362

[7] Peralta, Goiuri; Cid-Fuentes, Raul G.; Bilbao, Josu; Crespo, Pedro M. (2019). Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges. Electronics, 8(8), 827–. doi:10.3390/electronics8080827

[8] Syed, Dabeeruddin; Refaat, Shady S.; Bouhali, Othmane (2020). Privacy Preservation of Data-Driven Models in Smart Grids Using Homomorphic Encryption. Information, 11(7), 357–. doi:10.3390/info11070357

[9] Alabdulatif, Abdulatif; Khalil, Ibrahim; Yi, Xun (2019). Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption. Journal of Parallel and Distributed Computing, (), S0743731519300887–. doi:10.1016/j.jpdc.2019.10.008

[10] Gao, Weichao; Yu, Wei; Liang, Fan; Hatcher, William G.; Lu, Chao (2018). Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption. IEEE Transactions on Network Science and Engineering, (), 1–1. doi:10.1109/TNSE.2018.2846736

[11] Martins, Paulo; Sousa, Leonel; Mariano, Artur (2017). A Survey on Fully Homomorphic Encryption. ACM Computing Surveys, 50(6), 1–33. doi:10.1145/3124441

[12] Kucherov, Nikolay N.; Deryabin, Maxim A.; Babenko, Mikhail G. (2020). [IEEE 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) - St. Petersburg and Moscow, Russia (2020.1.27-2020.1.30)] 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) - Homomorphic Encryption Methods Review. , (), 370–373. doi:10.1109/EIConRus49466.2020.9039110

[13] Yang, Xuechao; Yi, Xun; Nepal, Surya; Kelarev, Andrei; Han, Fengling (2018). A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2018.2817518

[14] Zhang, Jian; Yang, Yang; Chen, Yanjiao; Chen, Jing; Zhang, Qian (2017). A General Framework to Design Secure Cloud Storage Protocol Using Homomorphic Encryption Scheme. Computer Networks, (), S1389128617303328–. doi:10.1016/j.comnet.2017.08.019

[15] Lu, Yang; Zhu, Minghui (2018). Privacy preserving distributed optimization using homomorphic encryption. Automatica, 96(), 314–325. doi:10.1016/j.automatica.2018.07.005