International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V2I3P108
Eureka Vision Publication | Volume 2, Issue 3, 70-80, 2021

Original Article

Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption

Ram Mohan Polam[1], Bhavana Kamarthapu[2], Ajay Babu Kakani[3], Sri Krishna Kireeti Nandiraju[4], Sandeep Kumar Chundru[5], Srikanth Reddy Vangala[6]
[1]University of Illinois at Springfield.
[2]Fairleigh Dickinson University.
[3]Wright State University.
[4]University of Illinois at Springfield.
[5]University of Central Missouri.
[6]University of Bridgeport.

Abstract - *As cloud computing becomes the backbone of modern digital infrastructure, Data processing, transmission, and storage security in cloud systems has become a major worry. Because cloud systems are dynamic and multi-tenant, traditional security methods are unable to handle them, leaving them vulnerable to insider threats, data breaches as well as illegal access. The important security considerations for cloud computing are examined in this study, focusing on encryption techniques and architectural strategies to safeguard data in increasingly complex digital environments. As organizations transition to cloud-based infrastructures, protecting data confidentiality, integrity, and availability becomes a top priority, particularly in the face of dangers such insider attacks, data breaches, and illegal access. A thorough review of fundamental cloud security concepts, the functions of symmetric and asymmetric encryption, and cutting-edge the methods discussed in this article include Attribute-Based Encryption (ABE) and ABE with several authorities for more precise access control. Furthermore, it emphasizes the need for homomorphic encryption (HE) to allow secure computations on encrypted data and looks at the Zero Trust Architecture (ZTA) as a proactive security paradigm to lessen developing cyber threats.*

Keywords - *Cloud computing, data security, encryption, zero trust architecture, homomorphic encryption, access control, privacy preservation.*

1. Introduction

The technique of spreading computer services, including platforms, apps, and infrastructure, across the internet is known as cloud computing. The large-scaled distributed infrastructure that serves as the foundation for cloud computing typically virtualizes a shared pool of resources and distributes services provision of software, deployment environments, or virtual machines to clients [1]. Thus, it makes sense to believe that cloud services might be dynamically scaled in accordance with needs and workloads [2]. Because so many resources are used, they are measured, and the amount of money paid depends on how much of those resources are used.

Cloud computing's ability to provide scalable, adaptable, and affordable solutions is further redefining the technological environment, concerns surrounding data security have become increasingly prominent. Organizations migrating sensitive problems, including insider threats, unauthorized access, data breaches, and regulatory compliance, are encountered while transferring information to cloud systems [3]. These dangers are increased by cloud infrastructures' multi-tenant structure and dependence on outside providers, rendering conventional security procedures inadequate. To ensure data availability, confidentiality, and integrity across public, private, and hybrid clouds, a comprehensive, multi-layered security solution is required. This necessity has driven the adoption of advanced cryptographic techniques, access control models, and trust-based frameworks. In this context, modern innovations like encryption, Zero Trust Architecture (ZTA), and homomorphic encryption have emerged as pivotal tools to address the growing demand for secure, privacy-preserving cloud solutions.

Among the most foundational approaches to securing cloud environments is in this situation, encryption is essential because it protects protect sensitive information by transforming it from a readable format into an unintelligible one that prevents unauthorized access. Standard encryption methods, such symmetric and asymmetric cryptography, safeguard information in transit and at rest, but they are insufficient for processing since the data must be decrypted before computing, which exposes it to possible dangers. To overcome this vulnerability, Homomorphic Encryption (HE) has gained attention for its unique the capacity to do computations on encrypted data directly, keeping the original data hidden [4]. This capability makes HE especially valuable for privacy-preserving analytics [5], secure outsourcing of computations, and compliance with stringent data protection regulations. Together, these encryption techniques form a critical part of the security foundation required to build trust in cloud computing systems.

To address these growing risks, the security community has increasingly turned toward ZTA a paradigm in which no entity, is considered reliable regardless of its location within or outside the network. Zero Trust is an alternative to standard perimeter-based security measures that emphasizes constant monitoring, strict identification verification, and Less-privilege access limits. Within the realm of cloud computing, Zero Trust provides a dynamic and granular control mechanism that mitigates threats from both external attackers and insider threats. It ensures that every access request is completely verified and approved, significantly reducing the area of attack in hybrid and multi-tenant cloud environments.

1.1. Structure of the paper

The structure of this paper is as follows: Section II covers the fundamentals of cloud data security. Section III discusses encryption techniques for secure cloud computing. Section IV explores homomorphic encryption enabling secure computation. Section V examines ZTA Section VI reviews relevant literature and case studies, and Section VII concludes with future research directions.

2. Fundamentals Of Cloud Data Security

The collection of tactics, tools, regulations, and controls used to safeguard information processed, stored, and transferred is known in cloud contexts as cloud data security. The scalability and efficiency offered by cloud computing are becoming increasingly important to enterprises, protecting data availability, confidentiality, and integrity becomes essential [6]. Cloud data security relies on encryption for all three stages of data lifecycles: at rest, in transit, and in use, strong IAM, API, DLP mechanisms, regular audits, and compliance with industry standards. These elements work together to mitigate risks include unauthorized access and data leaks, and insider threats, providing users with trust and assurance in cloud-based systems.

2.1. Understanding Cloud Computing Models

The "cloud" in cloud computing is shorthand for a network of interconnected nodes, much as the water molecules that make up actual clouds. User access to cloud computing modalities is unlimited and available whenever required. Instead of establishing their own physical infrastructure, customers usually choose for an intermediary provider for cloud computing internet services [7]. Only the services that users have actually used are subject to payment. The strain may be transferred to cloud computing in order to reduce it.

Cloud computing models define the different ways computing services are delivered over the internet, each offering varying levels of control, flexibility, and security responsibilities. The three main models—PaaS, IaaS, and SaaS—all cater to different client needs and goals [8]. Understanding these models is essential for organizations to decide on using cloud-based technologies while upholding strict data security guidelines.

2.1.1. Software as a Service (SaaS)

Software as a Service, or SaaS, is the rung at the top of the CC service model hierarchy. Multiple users can use data and object code simultaneously on this platform. SaaS is different from traditional software in that it doesn't need the same gear and software. It offers the least control over data security. Users rely heavily on the provider’s security practices, making it crucial to assess SLA, data encryption policies, and compliance certifications before adopting a SaaS solution.

2.1.2.The Platform as a Service

The platform as a service model, which is CC service middleware models, provides a service-like computing platform and stack solution. Using this approach, users or clients can create their own employing software tools or libraries and continue to distribute the software and other services. it introduces security concerns such as the potential for insecure APIs or misconfigurations. Ensuring data confidentiality and application-level security within the platform becomes the user’s primary concern.

2.1.3. Infrastructure as a Service (IaaS)

The infrastructure as a service is CC's third and final service offering. Operating systems and other software can be installed and run by customers using IaaS, while the supplier supplies the processing power, network storage, and other computer resources that are required. While SaaS is the most user-friendly model, it offers the least control over data security [9]. Users rely heavily on the provider’s security practices, making it crucial to assess SLA, data encryption policies, and compliance certifications before adopting a SaaS solution. A condensed comparison of the following Table I displays the cloud computing service model.

Table 1. Summarizing the Three-Cloud Computing Services Model

Service Model	Description	User Control	Security Concerns
Software as a Service (SaaS)	provides software access online without the necessity for installation or hardware. Multiple users can access applications simultaneously.	Least control	Depends on provider's security; risk from weak SLAs or poor encryption
Platform as a Service (PaaS)	provides a development and environment. for apps built with software tools and libraries.	Moderate control	Vulnerable to insecure APIs, misconfigurations, and platform-level breaches
Infrastructure as a Service (IaaS)	provide additional computer resources, servers, storage, and networking infrastructure. Users can install and manage OS and applications.	Highest control	Requires user-managed security for OS, applications, and data

2.2. Data Security in Cloud Computing

An important part of keeping data secure in the cloud is encryption. Three separate cloud service models SaaS , PaaS, and IaaS each have their own specific security needs. [10]. The two types of data in the cloud that are frequently vulnerable to security threats are data in transit, or data being moved to or from the cloud, as well as data that is stored or at rest. The effectiveness of the security measures, rules, and processes in place determines how well data confidentiality and integrity are maintained. The primary worry is the potential for data leak in these two states.

2.2.1. Data at Rest

The term "data at rest" describes any information that is accessible online or saved in the cloud. This covers both current and backup data. If an organization is not using a private cloud, Since they do not physically manage the data, protecting it when it is at rest may be quite challenging.

2.2.2. Data in Transit

As seen in Figure 1, data entering and exiting the term "data in transit" is frequently used to describe the cloud. This information could be kept in a cloud-based database or file, and it might be asked to be used in another location. The information is referred to as "data in transit" while it is being transmitted to the cloud [11].

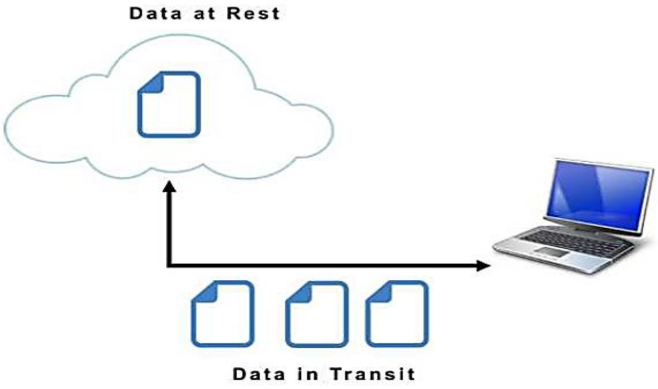

Figure 1. Data at Rest and in Transit

In some circumstances, data that must be transferred is more vulnerable to attacks than data that remains in one place. [12]. There are several ways that software used by intermediaries might intercept data and sometimes change it while it is being sent to its destination. Encryption is among the best ways to safeguard data while it's being transmitted.

2.3. Cloud Security Challenges

Cloud environments face a wide array of security threats that range from traditional cybersecurity issues to cloud-specific vulnerabilities [1]. Data breaches are among the most critical threats, often resulting from misconfigured storage, weak authentication, or insider threats. Cloud systems are vulnerable to illegal access and manipulation due to insecure interfaces and APIs.

2.3.1. Data Breaches

Sensitive information being revealed to an unauthorized person is known as a data breach. Cloud settings may experience data breaches for a variety of reasons. The sheer volume of data kept on a cloud server makes the provider an easy target for cybercriminals in the cloud computing industry.

2.3.2. Data Access Controllability

A data owner's capacity to upload their files to a cloud service might be restricted by access control measures. Intruders may be able to access the owner's personal information, but only authorized users are allowed access. However, in untrusted cloud settings, owners can only manage access authorization.

2.3.3. Insider Threats

Insider threats involve Present or past workers, subcontractors, or business associates with permission to access cloud systems and data but use that access for malicious purposes. In cloud computing, where administrative access is often centralized and extensive, the risk of insider threats is amplified. These actors can deliberately or unintentionally compromise data confidentiality and system integrity [13].

3. Encryption Techniques For Secure Cloud Computing

Cloud computing need encryption. At the moment, encryption is among the greatest data protection methods available. The technologies and procedures that control the cryptographic security services are the foundation of encryption integrity. One of the main methods for protecting data (and applications) is encryption. Cryptosystems that make use of one or more cryptography algorithms are implemented by encryption solutions [14]. These methods frequently mix symmetric and asymmetric cryptography, with After asymmetric keys are utilized to build up, symmetric keys are applied for content encryption. Both endpoints of a communication channel should have symmetric keys. The strengths of various encryption techniques vary. There are several encryption methods available to prevent data leaks. To prevent unauthorized use of the private information, several encryption techniques are employed. An encryption process is the conversion of plain text into ciphertext, as seen in Figure 2.

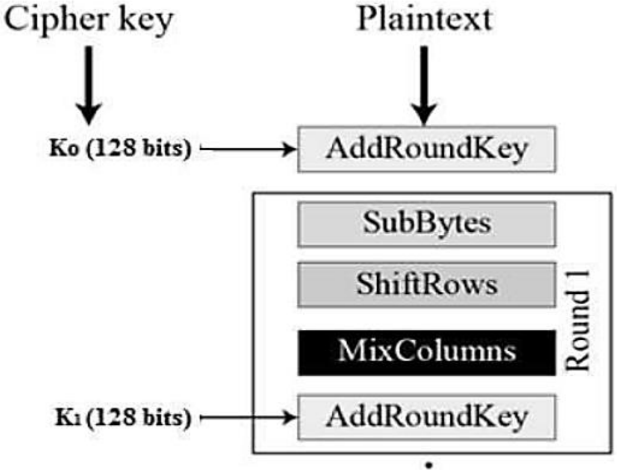

Figure 2. Encryption Process

That one round of the AES (Advanced Encryption Standard) encryption process shown in above Figure 2, where a 128-bit plaintext undergoes a series of transformations using a 128-bit cipher key. Initially, the first-round key is mixed with the plaintext. (K_0) using the Add Round Key operation. Then, it goes through the core AES functions: Shift Rows (row-wise permutation), Sub Bytes (non-linear byte replacement), and Mix Columns (column mixing for diffusion) [15]. After these steps, the output is again combined with a new round key (K_1) through another Add Round Key operation, continuing through multiple similar rounds to complete the AES encryption.

3.1. Traditional Symmetric and Asymmetric Key Encryption Techniques

The encryption process makes use of both symmetric and asymmetric key cryptography, two of the most widely used forms of cryptography. The ability to encrypt and decrypt using the same key is known as a symmetric key. When using an asymmetric key, this entails encrypting with the public key and decrypting with the private key; in other words, separate keys are utilized for both processes [16]. However, access control is not provided by these encryption mechanisms, but privacy is. A public key cryptography technology called ABE allows for safe data exchange across several users while ensuring security and confidentiality.

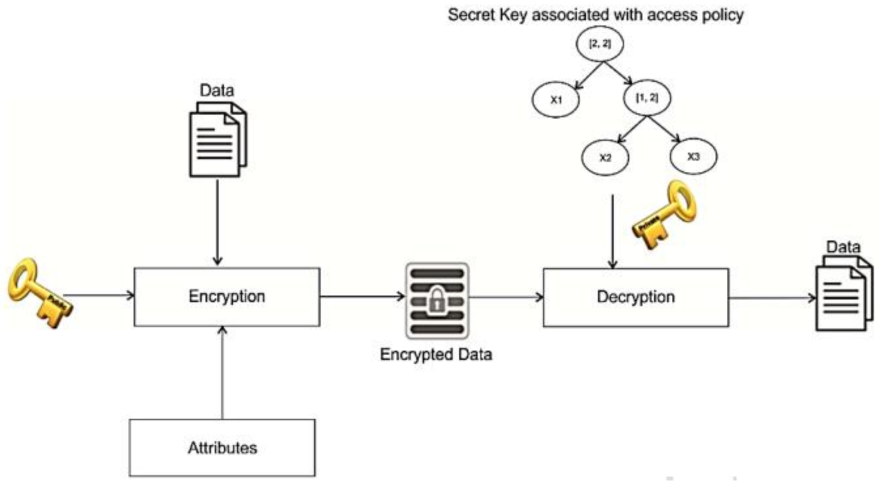

Figure 3. Key Policy Attribute Based Encryption

Figure 3 shows the relationship between an access policy and a user's private key is used to decode data encrypted using ABE characteristics. Among its many characteristics are the ability to revoke access, prevent collusion, scale, and provide fine-grained access control. The user's credentials can only be decrypted if they meet the access conditions.

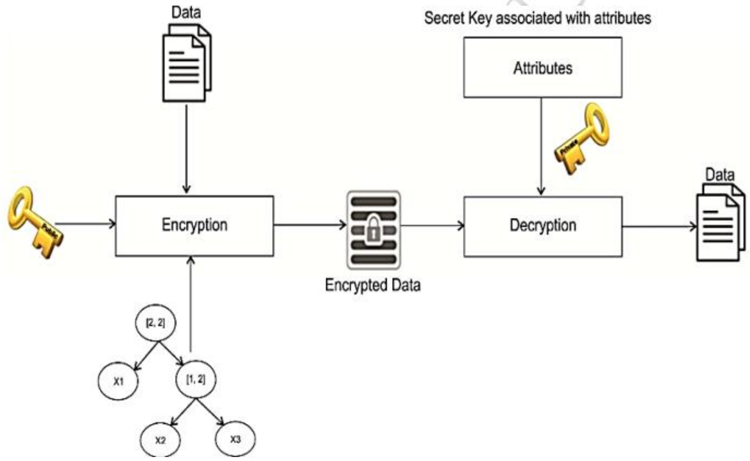

Figure 4. Ciphertext Policy Attribute Based Encryption

The KPABE and CPABE are the two main types of ABE [17]. Figure 3 illustrates how KPABE uses characteristics to determine the ciphertext and access policies to determine the user's secret keys. Figure 4 illustrates how the ciphertext in CPABE is determined by access controls and user secret keys depending on characteristics.

3.2. Multi-Authority Attribute Based Encryption

An sophisticated cryptographic approach called MA-ABE was created to offer Access control at the fine level in decentralized environments, such as cloud computing platforms [18]. Unlike traditional Attribute-Based Encryption, which relies on a single trusted authority to issue attributes and keys, MA-ABE involves multiple independent authorities, each responsible for managing a subset of user attributes.

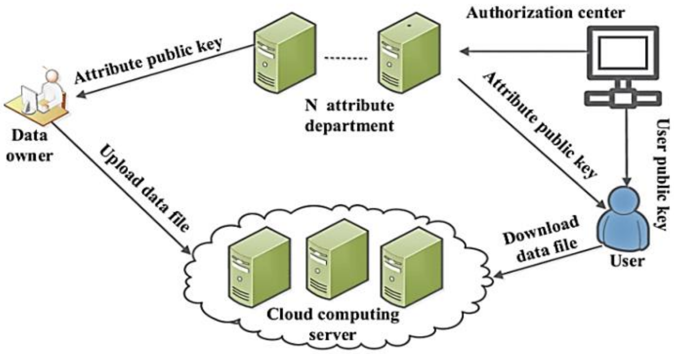

Figure 5. Multi-Authority Encryption

As illustrated in Figure 5, It makes logical for multi-authority centres to arise as the ABE technique needs each user attribute to get a private key from a trust authority, which calls for numerous authority centres and may result in increased workload and decreased efficiency for the single authority. Various authorities govern multiple traits. To stop preventing the private key from being stolen by the authority center, each characteristic creates an encrypted private key. Table II presents a technical comparison of the aforementioned encryption techniques.

Table 2. Reflect the technical distinctions among the encryption methods.

Encryption Technique	Encryption/Decryption Mechanism	Access Control Granularity	Trust and Authority Structure
Symmetric Key Encryption	The keys for encryption and decryption are identical	None	Single trusted entity
Asymmetric Key Encryption	The public key for encryption and the private key for decryption	Coarse (optional via PKI)	Public Key Infrastructure (PKI)
Key-Policy ABE (KP-ABE)	Data tagged with attributes; key has access policy	Fine-grained (key-defined)	Central authority
Ciphertext-Policy ABE (CP-ABE)	Data encrypted with access policy; user has attribute keys	Fine-grained (data-defined)	Central authority
Multi-Authority ABE (MA-ABE)	Similar to CP/KP-ABE; multiple authorities issue partial keys	Fine-grained (multi-domain)	Multiple decentralized authorities

4. Homomorphic Encryption: Enabling Secure Computation

A revolutionary encryption method called HE makes it possible to do calculations on encrypted material directly without first decrypting it. In cloud computing, where sensitive data frequently has to be handled by third-party servers, this capacity is very helpful [19]. HE effectively eliminates the conventional trade-off between privacy and data usefulness, which maintains data secrecy throughout the computing lifespan. Figure 6 below illustrates the general workings of Cloud computing with encryption that is homomorphic:

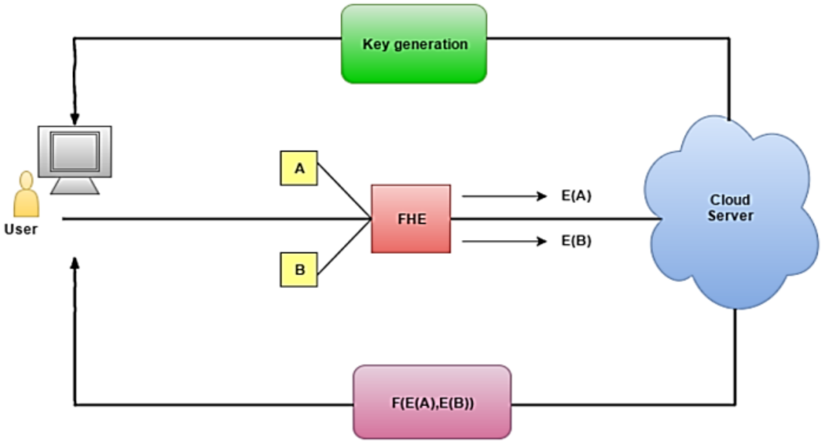

Figure 6. Homomorphic Encryption Based Secure Computation in Cloud Environment

A special kind of encryption called HE makes it possible to do certain computations on the actual non-plain material, generating an encrypted form that is associated with the results of the operations performed on the raw data upon decoding [20]. In addition to completely homomorphic cryptosystems, there exist several partially homomorphic ones. FHE is thought to be safer than encryption that is partially homomorphic.

4.1.Types of Homomorphic Encryption

The kinds and intricacies of operations that HE systems permit on encrypted data determine their categorization [4]. These types determine the practical use cases, performance overhead, and security guarantees of the encryption model. The three main types are:

4.1.1.Partially Homomorphic Encryption

PHE schemes make it possible to do specific computations on data that has been encrypted. The most common operations that PHE systems provide are addition and multiplication. Addition: Two ciphertexts can be added using PHE schemes, which is equivalent to adding the matching plaintext values. A cryptosystem is said to be it is considered partially homomorphic if it demonstrates homomorphism that is either multiplicative or additive, but not both. ElGamal, Paillier, and RSA are a few examples. RSA uses multiplicative homomorphism, whereas Paillier uses additive homomorphism.

4.1.2. Somewhat Homomorphic Encryption (SHE)

SHE systems go beyond basic addition and multiplication to allow for a wider range of operations on encrypted data. They offer a limited amount of computing power while protecting data privacy. In certain ways, restricted set of addition and multiplication operations on the ciphertext are permitted by weakly homomorphic encryption and however, the depth of computations is constrained due to the accumulation of "noise" during operations, which can eventually prevent correct decryption. SHE is useful in scenarios where only a fixed set of simple encrypted computations are required, such as statistical analysis or threshold-based evaluations.

4.1.3. Fully Homomorphic Encryption

Data that is encrypted can be subjected to arbitrary computations using fully homomorphic encryption techniques, enabling an endless number of operations without the requirement for decryption. Regarding homomorphic encryption, FHE is the most potent and flexible. If there exist both multiplicative and additive homomorphism qualities, a cryptosystem is considered completely homomorphic [21]. The lattice-based cryptosystem, which was the first (and as of right now, the sole) system previously mentioned, was created in 2010. FHE is reportedly far more effective and a great way to successfully protect the contracted-out data.

5. Zero Trust Architecture (Zta) For Cloud Security

The Zero-Trust strategy is a strategic endeavor that is governed by the maxim "never trust, always verify." People, objects, data, apps, and services operating within a company's security perimeter should not be taken for granted, according to this security threat model. Rather, the system claims that all network communications are unreliable and checks each entity before granting access to its resources. This is what it does each time a user tries to interact with the system [22]. More importantly, The ZT technique eliminates the idea of trust from a company's network architecture, preventing successful data breaches brought on by the misuse of privileged credentials.

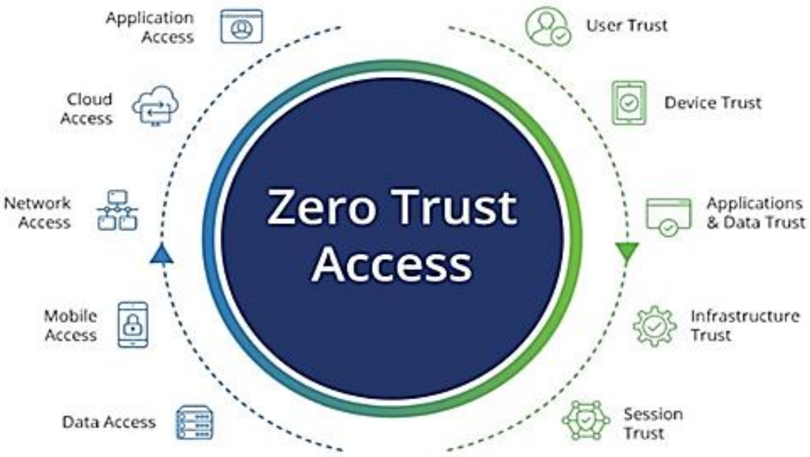

Figure7. Zero Trust Architecture

One of the most effective frameworks for device security in cloud ecosystems is ZTA. In a ZT model, every device, user, and network connection are considered untrusted by default. Instead of assuming that devices inside the network perimeter are secure, ZT continuously verifies all access requests. With ZTA, devices are authenticated, and Strict identity verification and the least-privilege principle are used to determine who is allowed access. By putting a ZTA strategy into practice, businesses may drastically lower the danger of unwanted access and ensure that devices adhere to strict security standards before interacting with cloud services. The Figure 7 shows the ZTA stressing constant verification and rigorous access limits.

5.1. Zero Trust Architecture

As the acronym might suggest, ZTA has little faith in the network itself, departing from the perimeter approach. In the event that the network has been compromised, security can take a more advanced approach by restricting accessing its assets and putting strong authentication in place and authorization guidelines to provide particular access based on characteristics unique to each user and device. ZTA, which is founded on the idea of "least-privilege access," permits users and devices to access just the information, applications, and services that are absolutely necessary for their role inside a company. When a user's duties change, an organization may quickly raise or decrease their access and more accurately distribute its resources and data. by utilizing "role" as the focal point for access determination. Although perimeter security will remain the first line of defines, relying too much on it may raise the possibility of data interception and network breaches. Through the employment of the appropriate authorizations to verify the identities of people and devices and detect network breaches at the next level of access, ZTA may bridge the perimeter security gap. and ensure that appropriate and secure access is granted.

5.1.1. Steps of Zero Trust Architecture

At the network's application and service levels, ZTA functions using three basic phases [23].

- First, it verifies the user through strong authentication mechanisms to ensure only legitimate individuals gain access.
- Second, it verifies the device being used to confirm that it is trusted, compliant, and not compromised.
- Third, it verifies access privileges through authorization checks to ensure users and devices can only access resources they are explicitly permitted to. This layered approach strengthens security by eliminating implicit trust.

6. Literature of Review

A primer on methods for keeping sensitive information safe in the cloud is given in this section, with an emphasis on ZTA, HE, and encryption methods.

Bhajantri and Mujawar (2019), explores different security challenges from each of these angles. A synopsis of infrastructure and data security challenges is also covered, as well as the idea of cloud computing's identity and access control. Examined are the many methods for preventing or reducing cloud security issues. Computing in the cloud is based on a novel concept that makes use of the internet to offer on-demand access to various resources including servers, storage, networking, apps, and more. Cloud computing enables a common pool of resources, which are overseen by third-party cloud service providers. It has a number of benefits, including minimal operational costs, effectiveness, scalability, and adaptability, among others [24].

Sun, (2019), carefully reviews and evaluates pertinent research findings. Initially, they address the design, principles, and various drawbacks of cloud computing and provide a framework for privacy protection. Next, look at and assess the fundamentals of hierarchical encryption, trust, reputation, PRE, fine-grained, multi-authority trace technique, Access structure, revocation mechanism, SE, ABE, KP-ABE, CP-ABE, and an extension of conventional access control [18].

Singh, Rishiwal and Kumar, (2018), the basis for classifying data related to cloud computing and proposing a classification based on a few crucial elements that establish the level of security of data transferred in a cloud setting. For almost ten years, the cloud computing concept has transformed the computer industry. Cloud computing has several benefits over more conventional methods of data storage and processing. The price of cloud computing is only one of its many benefits, speed, reduced setup time, pay-per-use model, robust service, 24/7 accessibility, and mobile service availability, among many others. Despite all of these benefits, cloud computing has several drawbacks and difficulties [25].

Mahmood and Ibrahem, (2018), encapsulates cloud computing security issues. The completely homomorphic encryption approach's enormous key size and poor processing efficiency make it impractical for secure cloud computing. Drawing inspiration from the multiplicatively homomorphic RSA method and the additively (single bit) homomorphic GM encryption algorithm, it creates a hybrid homomorphic encryption method. To get over these drawbacks and take advantage of their resilience to confidentiality assaults, Homomorphic encryption algorithm hybridization seems to be an effective tactic [26].

Diao et al. (2017) Implement data security for cloud storage while also developing a plan to keep it secure. Considering cloud storage systems' structural characteristics, this issue pertains to the relevant security technologies, was discussed together with the findings of previous scholarly study on the security dangers to user data stored in cloud storage. as well as cloud computing's increasing use. Cloud storage technology has gained more attention as a novel network storage technology that is developed and improved by cloud computing concepts [27].

Albugmi, Madini O Alassafi, et al. (2016), The article will go into detail on data security techniques and tactics used worldwide to provide optimal data protection by reducing risks and threats. Many applications benefit from having data available on the cloud, however there are dangers involved since data is exposed to apps that may already possess weaknesses in security. The same is true when a guest OS is used on top of a hypervisor without the user's knowledge of how reliable the guest OS is it can have a security flaw using virtualization for cloud computing may endanger data. The article will also cover elements of protecting data while it's in transit and at rest. All SaaS, PaaS, and IaaS tiers are the foundation of the study [28].

A summary of the literature review is shown in Table III, emphasizing each study’s focus, approach, key findings, challenges, and proposed future directions.

Table 3. Comparative Analysis of literature review based on data security in cloud computing

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Bhajantri and Mujawar (2019)	Cloud security issues	Review of security challenges at infrastructure, data, and access control levels	Identified infrastructure and data-level threats; emphasized identity and access control	Lack of holistic solutions for all layers	Propose integrated frameworks for multi-level cloud security
Sun (2019)	Cloud computing privacy protection	Analytical review of cloud architecture, ABE, and encryption mechanisms	Introduced privacy protection framework; analyzed ABE variants and access control	Complexity in encryption techniques; scalability issues	Enhance encryption methods (e.g., PRE, SE) for practical and scalable implementation
Singh, Rishiwal and Kumar (2018)	Data classification for cloud security	Proposed a classification approach based on data sensitivity parameters	Highlighted importance of data classification in security	No standard framework for data classification in cloud	Develop adaptive classification models integrated with cloud security policies
Mahmood and Ibrahem (2018)	Encryption homomorphic for safe cloud computing	suggested a hybrid homomorphic encryption system that blends the RSA and GM algorithms together.	Hybrid encryption overcomes individual limitations; suitable for secure data computations	Large key sizes; low computation efficiency	Improve hybrid homomorphic schemes for real-time cloud operations
Diao et al. (2017)	Data security in cloud storage	Analyzed cloud storage structural characteristics and integrated academic research to formulate a security policy	Identified key security risks in cloud storage and proposed policy frameworks based on system structure	Managing dynamic security threats; evolving attack vectors	Develop adaptive security mechanisms and real-time threat detection tailored for cloud environments
Albugmi, Alassafi, et al. (2016)	Across cloud service paradigms (SaaS, PaaS, and IaaS), data protection	Examined virtualization threats, international data protection techniques, and Problems with data security in transit and at rest.	Emphasized multi-level protection and vulnerabilities in virtualized environments	Security risks in guest OS and exposed applications	Develop secure virtualization protocols and real-time threat detection in cloud environments

7. Conclusion and Future Work

The data management, access, and storage have all been revolutionized by the rapid use of cloud computing, but with this success has come pressing security concerns. Ensuring robust security in cloud computing demands a comprehensive approach that combines advanced encryption methods with proactive architectural strategies. As reliance on cloud infrastructure grows, traditional security measures fall short against modern cyber threats. Techniques like symmetric, asymmetric, Homomorphic, and Attribute-Based Encryption help protect data and enforce secure access. The foundation of zero trust architecture is the "never trust, always verify" approach, strengthening defense against both external and internal threats. Ongoing innovation, strict policy enforcement, and a focus on data-centric security are crucial for protecting sensitive information and sustaining trust in cloud services. Despite advancements, cloud security faces limitations like high computational costs from advanced encryption and the complexity of implementing ZTA in large or legacy systems.

Future work should focus on optimizing Homomorphic Encryption schemes for practical, large-scale cloud applications, developing automated tools for ZTA deployment, and enhancing key management systems for multi-cloud environments. Additionally, more study is required on combining AI and ML to anticipate and counteract cloud risks instantly.

References

[1] M. Kaur and H. Singh, “A review of cloud computing security issues,” Int. J. Grid Distrib. Comput., vol. 8, no. 5, pp. 215–222, 2015, doi: 10.14257/ijgdc.2015.8.5.21.

[2] A. Immadisetty, “Dynamic Pricing Strategies in Retail: Leveraging Real-Time Data Analytics for Competitive Advantage,” J. Recent TRENDS Comput. Sci. Eng., vol. 13, no. 1, pp. 53–65, Feb. 2025, doi: 10.70589/JRTCSE.2025.13.1.8.

[3] S. K. Sood, “A combined approach to ensure data security in cloud computing,” J. Netw. Comput. Appl., vol. 35, no. 6, pp. 1831–1838, 2012, doi: https://doi.org/10.1016/j.jnca.2012.07.007.

[4] M. E. Zhao and Y. Geng, “Homomorphic Encryption Technology for Cloud Computing,” Procedia Comput. Sci., vol. 154, pp. 73–83, 2018, doi: 10.1016/j.procs.2019.06.012.

[5] A. Immadisetty, “Dynamic Pricing Strategies in Retail: Leveraging Real-Time Data Analytics for Competitive Advantage,” J. Recent Trends Comput. Sci. Eng., vol. 13, no. 1, pp. 53–65, 2017.

[6] M. Carroll and A. Van Der Merwe, “Secure cloud computing: Benefits, risks and controls,” in 2011 Information Security for South Africa, IEEE, Aug. 2011, pp. 1–9. doi: 10.1109/ISSA.2011.6027519.

[7] P. Srivastava and R. Khan, “A Review Paper on Cloud Computing,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., 2018, doi: 10.23956/ijarcsse.v8i6.711.

[8] E. Simmon, “Evaluation of cloud computing services based on NIST SP 800-145,” Gaithersburg, MD, Feb. 2018. doi: 10.6028/NIST.SP.500-322.

[9] T. Diaby and B. B. Rad, “Cloud Computing: A review of the Concepts and Deployment Models,” Int. J. Inf. Technol. Comput. Sci., vol. 9, no. 6, pp. 50–58, 2017, doi: 10.5815/ijitcs.2017.06.07.

[10] A. Gogineni, “Novel Scheduling Algorithms For Efficient Deployment Of Mapreduce Applications In Heterogeneous Computing,” Int. Res. J. Eng. Technol., vol. 4, no. 11, p. 6, 2017.

[11] F. Yahya, V. Chang, R. J. Walters, and G. B. Wills, “Security Challenges in Cloud Storages,” in 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, 2014, pp. 1051–1056. doi: 10.1109/CloudCom.2014.171.

[12] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, “Data security in cloud computing,” 5th Int. Conf. Futur. Gener. Commun. Technol. FGCT 2016, no. October 2017, pp. 55–59, 2016, doi: 10.1109/FGCT.2016.7605062.

[13] W. R. Claycomb and A. Nicoll, “Insider Threats to Cloud Computing: Directions for New Research Challenges,” in 2012 IEEE 36th Annual Computer Software and Applications Conference, 2012, pp. 387–394. doi: 10.1109/COMPSAC.2012.113.

[14] S. Balasubramaniam and V. Kavitha, “A survey on data encryption tecniques in cloud computing,” Asian J. Inf. Technol., vol. 13, no. 9, pp. 494–505, 2014, doi: 10.3923/ajit.2014.494.505.

[15] R. Cahya, P. Arief, A. Novriza, and A. Kohei, “Noble Method for Data Hiding using Steganography Discrete Wavelet Transformation and Cryptography Triple Data Encryption Standard: DES,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 11, pp. 261–266, 2018, doi: 10.14569/IJACSA.2018.091136.

[16] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6054 LNCS, 2010, pp. 136–149. doi: 10.1007/978-3-642-14992-4_13.

[17] P. K. Premkamal, P. S. Kumar, and A. Pja, “Attribute based encryption in cloud computing: A survey, gap analysis, and future directions,” J. Netw. Comput. Appl., vol. 108, pp. 37–52, Apr. 2018, doi: 10.1016/j.jnca.2018.02.009.

[18] P. Sun, “Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions,” IEEE Access, vol. 7, pp. 147420–147452, 2019, doi: 10.1109/ACCESS.2019.2946185.

[19] V. Biksham and D. Vasumathi, “Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey,” Int. J. Comput. Appl., vol. 160, no. 6, pp. 1–5, 2017, doi: 10.5120/ijca2017913063.

[20] [20] M. Ogburn, C. Turner, and P. Dahal, “Homomorphic encryption,” Procedia Comput. Sci., vol. 20, pp. 502–509, 2013, doi: 10.1016/j.procs.2013.09.310.

[21] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, “A survey on homomorphic encryption schemes: Theory and implementation,” ACM Comput. Surv., vol. 51, no. 4, 2018, doi: 10.1145/3214303.

[22] C. Decusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, “Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication,” Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016, pp. 5–10, 2016, doi: 10.1109/SmartCloud.2016.22.

[23] K. Delbene, M. Medin, and R. Murray, “The Road to Zero Trust (Security),” pp. 1–10, 2019.

[24] L. B. Bhajantri and T. Mujawar, “A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures,” in Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019, 2019. doi: 10.1109/I-SMAC47947.2019.9032545.

[25] K. P. Singh, V. Rishiwal, and P. Kumar, “Classification of Data to Enhance Data Security in Cloud Computing,” in 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1–5. doi: 10.1109/IoT-SIU.2018.8519934.

[26] Z. H. Mahmood and M. K. Ibrahem, “New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing,” in 2018 1st Annual International Conference on Information and Sciences (AiCIS), 2018, pp. 182–186. doi: 10.1109/AiCIS.2018.00043.

[27] Z. Diao, Q. Wang, N. Su, and Y. Zhang, “Study on Data Security Policy Based on Cloud Storage,” in Proceedings - 3rd IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2017, 3rd IEEE International Conference on High Performance and Smart Computing, HPSC 2017 and 2nd IEEE International Conference on Intelligent Data and Security, IDS 2017, 2017. doi: 10.1109/BigDataSecurity.2017.12.

[28] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, “Data security in cloud computing,” in 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), 2016, pp. 55–59. doi: 10.1109/FGCT.2016.7605062.

[29] Chinta, P. C. R., & Karaka, L. M. (2020). Agentic AI and Reinforcement Learning: Towards More Autonomous and Adaptive AI Systems.

[30] Kalla, D., Kuraku, D. S., & Samaah, F. (2021). Enhancing cyber security by predicting malwares using supervised machine learning models. International Journal of Computing and Artificial Intelligence, 2(2), 55-62.

[31] Katari, A., & Kalla, D. (2021). Cost Optimization in Cloud-Based Financial Data Lakes: Techniques and Case Studies. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(1), 150-157.

[32] Kalla, D., Smith, N., Samaah, F., & Polimetla, K. (2021). Facial Emotion and Sentiment Detection Using Convolutional Neural Network. Indian Journal of Artificial Intelligence Research (INDJAIR), 1(1), 1-13.

[33] Routhu, K., Bodepudi, V., Jha, K. M., & Chinta, P. C. R. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. Available at SSRN 5102662.

[34] Kuraku, S., & Kalla, D. (2020). Emotet malware a banking credentials stealer. Iosr J. Comput. Eng, 22, 31-41.

[35] Kalla, D., & Samiuddin, V. (2020). Chatbot for medical treatment using NLTK Lib. IOSR J. Comput. Eng, 22, 12.

[36] Routhu, K., & Jha, K. M. (2021). Leveraging Big Data Analytics and Machine Learning Techniques for Sentiment Analysis of Amazon Product Reviews in Business Insights. Available at SSRN 5106490.

[37] Chinta, P. C. R., & Katnapally, N. (2021). Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures. Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures.

[38] Karaka, L. M. (2021). Optimising Product Enhancements Strategic Approaches to Managing Complexity. Available at SSRN 5147875.

[39] Boppana, S. B., Moore, C. S., Bodepudi, V., Jha, K. M., Maka, S. R., & Sadaram, G. AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises.