International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *10 July 2023* ***Revised:*** *12 August 2023* ***Accepted:*** *28 August 2023*

Developing a Trustworthy Cloud Service Framework for Cloud Computing Security

Himanshu Kalra,
Salesforce Technical Manager, Technology Department, Fox Corporation at 1211 6th Ave, New York, NY 10036

Corresponding mail: hkalra.gkg@gmail.com

Abstract

Cloud computing is quickly becoming an essential platform for sharing infrastructure, software, apps, and corporate resources. Cloud computing has many advantages, but users still have a lot of questions about the dependability and safety of cloud services. Concerns about the hazards associated with the possible exploitation of this technology to undertake criminal operations might threaten the undeniable success of cloud computing. To ensure happy customers, the cloud model must prioritize safety, openness, and dependability.Its main purpose is data security, which concerns everyone contemplating cloud services. A cloud-based assault protection system will safeguard data, communications, and information.According to studies, the recommended technique is successful, however updating tags and blocks when data is amended requires computation and communication expenses. Scalability, data secrecy, and decentralized double encryption improve security.The proposed method employs cloud servers for computation-intensive tasks and protects data content by depriving data owners and users of privilege information. Also ensures responsibility. Sharing health data on the cloud is feasible, cost-effective, efficient, adaptive, and better for individuals. This"Advanced Encryption Standard with Lightweight Cipher-text-Identity and Attribute-based Encryption" (AES-lightweight CP-ABE) aims to protect sensitive data.

Keywords: Cloud Computing,Virtualization,Cloud Security, Trusted CloudService, Privacy.

1. Introduction

In today's IT industry, cloud computing is a hot subject. With its new Internet-based environment, it is possible to dynamically provide reconfigurable computer resources on demand. An important concern about this is the privacy and security concerns that arise from its multi-tenancy feature and the outsourcing of infrastructure, sensitive data, and important applications[1]. Despite the rapid growth and widespread usage of cloud computing, no universal standards exist for the management of trust and security inside these environments. Some individuals are still wary of using cloud services because they worry about privacy, security, and the safety of their data[2].Protecting the continued robust growth of cloud platforms becomes dependent on trust and security. For both users and service providers (SPs), it has been a game-changer when it comes to managing and using computer resources. Power distribution networks and banking systems are two examples of crucial societal sectors that have relied heavily on the important cloud infrastructure. Computing that can be relied on in the future, despite the presence of both current and future dangers and an ever-increasingly complicated working environment, is known as trustworthy computing. Reliability, security, privacy, and ease of use are essential for trustworthy functioning[3].

Computational resources are made available ‘as a service’ via cloud computing, which is a method of distributing computing that makes use of high-speed networks and scalable distributed computing platforms. As a service, it makes available via the web infrastructure that may be expanded or contracted on demand, or virtualized resources. The term ‘cloud computing’ refers to a relatively new idea that encompasses the transformation of several preexisting computer technologies and methods into something new[4]. It is a paradigm for making available a shared pool of customizable computing resources that can be made available globally and released with little involvement from cloud service providers and with the ability to scale on demand. Data storage, networks, and computing power are all part of the shared resources that it offers. Security and privacy are major concerns due to the revolutionary nature of cloud computing[5]. Considering these advantages, customers continue to oppose cloud computing adoption for security grounds. New security holes are appearing because of cloud computing's rapid expansion. At this time, the virtualized cloud environment cannot be adequately protected by the conventional security procedures such as authentication, identification, and authorization. The grossly uneven distribution of resources is the root cause of this shortfall. Due to the sensitive nature of the data kept in the cloud, security has emerged as a top concern for cloud computing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 10 July 2023 **Revised:** 12 August 2023 **Accepted:** 28 August 2023*

environments. An exhaustive investigation revealed that most of these gadgets could operate independently. Therefore, it is not possible to gather and evaluate their detection data in a systematic manner since they are separated. They reasoned that this was the perfect opportunity to unveil a new security strategy that would make it possible to spot DDoS and other widespread assaults[6]. With cloud computing, users can access data, save it, retrieve it, and run programs without necessarily having to understand the specifics of the system's setup or location.

With cloud computing, remote resources are better used, combined for increased throughput, and large-scale calculation challenges are solved. Using the Internet, "cloud computing" makes available virtualized resources that can be expanded or contracted on demand. Among other things, it makes use of grid computing, service-oriented software, and virtualization. Customers' needs can shift over time; therefore, it is important to remain flexible. The next step is to use virtualization to dynamically set up and aggregate resources on cloud computing systems. Through the negotiation of service-level agreements (SLAs), providers and customers work together in a cloud computing system, it is made up of a network of linked and virtualized computers that are offered as a computer resource pool on an as-needed basis. [7].

The paper presents a convictionvaluation methodology that mixes safety and repute to evaluate the reliability of a cloud facility. It tackles concerns related to cloud service reliability and offers the following contributions:

- To estimate the reliability of cloud services, it provides a new approach that combines security and reputation metrics. By evaluating the reliability of cloud services, the suggested framework safeguards the cloud-based IoT environment [8].
- A proposed security-based confidence evaluation technique uses cloud-specific security metrics to evaluate the security of cloud services, making it possible to trust these services more when it comes to data protection. Our proposal is a reputation-based trust evaluation approach that uses review ratings on cloud services' QoS so that you can evaluate the reliability of cloud providers based on their reputation.
- To get a quantifiable measure of cloud services' reliability, it uses an objective weight assignment method to give each degree of security and reputation the weight elements that are most important to them[9].

1.1.Function, Auditability, Governability, and Interoperability (FAGI) Framework

This security framework is designed to help organizations determine the level of security they need and then aid them in choosing a reliable cloud service provider (CSP). There are four factors that determine how trustworthy a certain CSP is in terms of security: 1) the certainty that the CSP can fulfil the organization's security requirements in terms of delivered security functions; 2) the verifiability of the claimed security capabilities through independent audits or assessments; 3) the transparency of the information conveyed to the organization regarding the cloud service's security, also known as governability; and 4) the ease with which an organization can switch to a different CSP for any reason.

Building on top of widely used security standards as ISO27001/2 (ISO/IEC, 2013), NIST SP800-53 (NIST SP800-53), CSA CCM (Cloud Security Alliance, CCM3.0, 2013a, b), and PCIDSS (PCISSC, 2013), the FAGI model adheres to industry best practices. On the one hand, the FAGI model offers comprehensive security protection to enterprises. By switching to a single framework instead of a patchwork of disparate standards, businesses may simplify and expedite their security management. With the help of governance and operational mechanisms, the Cloud Service Provider Security Framework is shown in Figure 1.

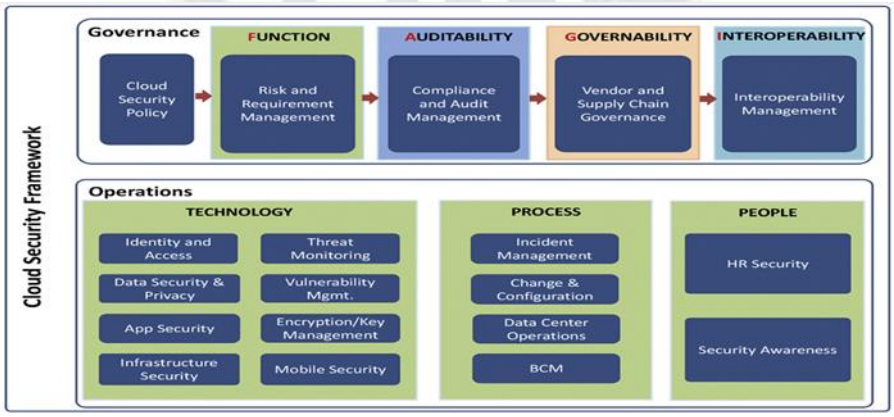

Figure 1: CSPs Security Framework

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 10 July 2023 **Revised:** 12 August 2023 **Accepted:** 28 August 2023*

The precise dangers posed by each SaaS application are different. Some businesses could skip every single FAGI component that has been suggested. An organization's unique SaaS risk posture, mostly dictated by the data transmitted to the cloud, necessitates a logic approach to assist identify the necessary security measures. There are three potential positions that may emerge from an organization's evaluation of its SaaS risk profile, as shown in Table 1: low, medium, and high. The study of security risk posture arrived to this conclusion that three tiers of controls should be implemented: basic, strong, and advanced[10].

Table 1: Assessment of security risk

Component	Description
Company industry	Based on NAICS 2012. Profile the industry such as public administration, finance and insurance, or health care, etc
Company Type	Private company and public company.
Data & Compliance	The criticality of the data stored/processed in the cloud. Profile compliance requirements such as PCIDSS, PIPEDA, HIPAA/HITECH, SOX, GLBA, FISMA, Bill198, and NERC etc.
Applications in the Cloud	The types of applications operated by the organizations
Security risk management	Organization's risk tolerance level; Risk visibility to the senior management and investors
User community size	How many users will use cloud apps

The following is the outline of the paper: Section 2 examines the summaries of cloud service-related papers published by different writers. In Section 3, an FAGI structure and related procedures are suggested for ensuring the security of Cloud Service. Section 4 delves into the technique and algorithm of the proposed framework, offering the most reliable approach to security and Section 5 concludes this study.

2. Literature of Review

As stated prior to, cloud computing's security is a big concern and the main object that might prevent it from being extensively adopted. The various frameworks were described in depth in the papers of several writers; some of these authors are mentioned below.

Huang et al., (2021)[11]created a novel architecture for instant on-demand security known as a 'policy-customized trusted cloud service' (PC-TCS). It has two main parts: a remote-attestation scheme that uses attribute-based signatures (ABS) to achieve reliable remote attestation utilizing personalized security guidelines, and a virtual machine migration protocol that uses ABS and blockchain to aid in policy-customized important migration. First, PC-TCS can be a reliable computing foundation in the cloud. Second, users of the cloud could create security policies for their computing environments and show how they are implemented with PCTCS. Third, PC-TCS can support policy-customized remote verification and policy-customized migration with little impact on performance. This architecture is available.

Li et al., (2019)[12] provide a new approach to evaluating the reliability and safety of cloud services. This methodology aims to evaluate cloud services with the purpose of safeguarding the cloud-based IoT ecosystem by merging privacy- and reputation-based trust assessment methodologies. When evaluating the safety of a cloud service, the security-based trust evaluation technique uses metrics tailored to the cloud for security.The proposed trust assessment framework outperforms previous trust assessment approaches in trials done using a real-world web service dataset and a synthetic dataset of security indicators, demonstrating efficient and effective trustworthiness evaluation of cloud services.

Sindhu et al., (2017)[13] suggested trust assessment framework assesses CSPs' reliability by means of the compliance monitoring mechanism. The author said that, collecting full and accurate quality of service data for cloud

services could prove a real challenge. Furthermore, cloud services' QoS statistics might not be accurate. And hence, the QoS value alone cannot be used to accurately assess the reliability of CSPs.

Tang et al., (2017)[14] introduced a reliable selection methodology. Built into this framework is a way to evaluate trust that considers both quantitative measures (quality of service monitoring) and qualitative ones (feedback ratings) all in one place. One problem is that the universal method for detecting dishonest users could unintentionally leave out reliable users and their actual ratings in the feedback section.

Liu et al., (2017)[15]provide a Data Integrity Service architecture that utilizes blockchain technology. Without the need for a Third-Party Auditor (TPA), this system would allow for more trustworthy data integrity certification for data owners and consumers. This paper presents the necessary protocols and a prototype system that we used to test the viability of our ideas. Here, do tests on the prototype system that was put into action and talk about the outcomes. This study establishes the groundwork for our next efforts to verify the dynamic integrity of data in a decentralized setting.

Wang et al., (2015)[16] deduced that the cloud model might be used to provide a lightweight reputation measuring technique for cloud services. Using fuzzy set theory, this approach calculates cloud service reputation rankings based on CSC feedback evaluations. Unfortunately, CSPs' reputations take a serious hit in the real world due to malicious users and unfair feedback ratings. Similarly, user ratings cannot be used in isolation to determine the genuine reliability of CSPs.

Noor et al., (2015)[17]propose creating and launching CloudArmor, a framework for trust management that relies on reputation and provides a set of tools to deliver Trust as a Service (TaaS). These features include: a unique protocol to safeguard user privacy while proving the credibility of trust feedbacks; a flexible and strong credibility model to measure the credibility of trust feedbacks to safeguard cloud services from harmful users and to compare their trustworthiness; and an availability model to control the decentralized implementation of the trust management service's uptime. They demonstrated the technique's viability and benefits using a prototype and conducted experimental studies utilizing a set of real-world trust feedbacks on cloud services.

Ding et al., (2014)[18] suggested a new approach for assessment of cloud service reliability, which integrates forecasts of quality of service with estimates of consumer happiness. Estimating client happiness with a certain cloud service and enhancing the precision of QoS value estimates of quantitative trustworthy features were the primary goals of this methodology. Nevertheless, it failed to consider how time and unjust feedback ratings affected the QoS projections.

3. Background Study

Cloud computing uses pooled computer resources to deliver services. Internet users may access these items. Along with new obstacles, it provides benefits over traditional computer services. Information confidentiality, availability, authentication, security, privacy, access control, scalability, and lock-in are included. Cloud technology poses security issues due to its openness, multi-tenancy, and resource outsourcing. Access control is necessary for security, but mandatory, discretionary, and role-based systems fail. Traditional access control approaches are unsuitable for cloud computing. This research presents a novel access control architecture for cloud security and privacy. This cloud access control architecture focuses on user trustworthiness over time and works well. The framework contains access control, rules, and multi-layer security. Access control is based on static and dynamic trust proof of the user's trustworthiness. Dynamic trustworthiness reduces undesired activities by restricting cloud resource access to permitted users. The proposed framework's Net Logo-based Linux prototype has test cases. The suggested solution is both efficient and resistant to security risks, according to the simulation findings. [19].

4. Problem Formulation

There is an urgent need for strong security measures to protect sensitive data, apps, and services due to the growing dependence on cloud computing. Cloud computing environment security, with an emphasis on building a trustworthy cloud service architecture, is at the heart of the current issue. There are growing worries about the security, privacy, and accessibility of data with the increasing number of companies shifting their activities to the cloud. A thorough strategy is required to build a reliable cloud service architecture considering current security concerns such unauthorized access, data breaches, and possible weaknesses in cloud infrastructures. The main objective is to create and execute a reliable cloud service architecture that can handle both the present and future security issues. By fixing these problems, businesses will be able to trust their cloud-based operations and adopt cloud computing with confidence.

5. Research Objectives

- Develop and provide a trustworthy cloud service architecture that has strong security features. To provide a safe groundwork for activities in the cloud, it is necessary to define security protocols, encryption standards, and access restrictions.

- Verify the established trustworthy cloud service architecture's viability and efficacy in a simulated cloud setting. Make sure the framework can handle security risks and vulnerabilities by testing it thoroughly.
- Examine the trusted cloud service framework's data protection features and make any necessary improvements. Determine if the framework complies with data protection standards and can guarantee the security of sensitive information.

6. Research Methodology

The core of security is assessing the capability of suppliers. Typically, cloud service companies provide voluminous documentation covering every imaginable topic. Experts in information technology security need to be able to make sense of all this noise and identify the elements that are important to meeting security standards.

The cloud, a remarkable service with excellent approaches, can manage massive amounts of data for storage. Many businesses, organizations, and individuals make use of this service since it allows them to keep both personal and corporate data.Any user could receive access to and make use of their cloud-based data at any time by using the services offered by cloud data providers. Cloud storage can identify the substantial data sharing that occurs across several regions and domains.

This paper provides Advanced Encryption Standard-weighted attribute-based encryption (AES-WABE), a combination of AES and WABE, as a means of safe data access management. Using the access control rules and assigning weights based on the importance of separately characteristic, the data is encrypted. Cloud providers and attribute authorities both retain the data that is outsourced; the latter is based on the weight that updates the attributes. To reduce the computational burden, the receiver accesses the data file according to its weight. The suggested method offers defence against collusion, security for numerous users with management over granular access predicated on protection, as well as effectiveness and dependability. The (CP-ABE) and the Hybrid attribute-based Encryption (HABE) scheme are used to rate the performance in terms of data cooperation and secrecy. Other factors considered include adaptability of control access, restricted decryption, complete delegation, verification, and partial signature.

The owner of the encrypted material often downloads it from cloud storage, re-encrypts it, and then shares it with others. Additionally, there are instances when cloud users take on the role of content providers themselves. They employ fine-grained data access control to broadcast the data on the cloud servers, which allows users to share and access the contents. Furthermore, the CSP must maintain the confidentiality of the data contents in opposition to the cloud users.

6.1.Attribute-Based on Hierarchical Encryption

Hybrid attribute-based encryption (HABE) is a product of merging hierarchical identity-based encryption (HIBE) with CP-ABE. Compared to other methods, HABE is more scalable, allows for granular control of access, and yields trust among attribute authorities. It also signifies the establishment's hierarchical structure and is suitable for an outsourcing organization.

CP-ABE: In CP-ABE, the user clears the access strategy on all attributes for the data consumer to decipher the encrypted information. This method is a reversal of the previous encryption methodology. Confidentiality and control of data access are therefore guaranteed.

HIBE: This method is an extension of IBE and is called HIBE. Private key generators (PKGs), also known as 1-HIBE, employ the primitive IDs (PIDs) of public keys to generate private keys. Like this technique, this method makes extensive use of key management. To address this, a 2-HIBE strategy is used, which comprises a root PKG and a domain PKG. The secret key and domain secret are both generated by the domain PKG, which is accessed via the private key generator's root. A root certificate grants hierarchy of certificates inside the cryptosystem. On top of that, HABE is not up to snuff when it comes to helping compound characteristics or multi-valued jobs. This paper presents a new AES-WABE approach to address this limitation.

7. Proposed Methodology

A secure and effective data connection is achieved by the suggested AES-WABE method. The current ABE techniques handle secret and public keys via unique access. Attribute consumers in one scenario oversee several attribute authorizations, whereas data holders in another scenario share consumer data under the jurisdiction of many authorities. Several control structures for multi-authority accesses based on attributes have been suggested to address this issue. This work uses the AES to produce safe data by weighting qualities. In this system, five fundamental modules are taken into account: (a) A server in the cloud to store the data (b) The person or organization responsible for encoding the data using a policy for controlling access and storing it in the cloud (c) An authorization system based on weight attribute authority (WAA), that checks and changes the user's properties (d) A central authority (CA) that assigns a unique identifier and public key to each user who uses WAA (e) The people actually using the data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *10 July 2023* ***Revised:*** *12 August 2023* ***Accepted:*** *28 August 2023*

By encrypting and decrypting data, the AES used in the suggested method randomly produces keys. In addition, an image-matching approach is used for security considerations. Afterwards, the algorithm uses the users' characteristics to calculate a weight value. Figure 2 depicts the five basic modules of the Cloud Security which combines the weighted attribute authority with the AES.

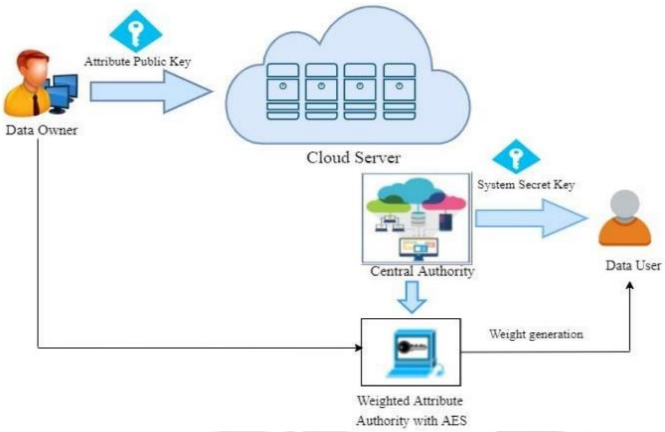

Figure 2: The Proposed Framework of (AES-WABE)

This system is trustworthy and safe, it is an improvement over the old ways and works well for real-time applications. The suggested encryption considers granular access control, resistance to collusion, and multi-authority security. The suggested technique involves of dual parts: the system phase and the algorithm phase. Using the AES algorithm, the algorithm's phase defines the system-level operations. Basic processes like User Annulment, System Setup, and admitting are in odds with one another. Instructions for enrolling a fresh user, making a fresh document, accessing, and deleting files, and so on are all detailed at the system level.

7.1.System Phase

This process is defined below in following stages:

1) System Setup

To attain the worldwide public criteria, the challenger processes the algorithm for global setup. The data bearer can select an encryption parameter that will provide the secret key SK by submitting an inquiry message to the interfaces of the algorithm's phase setup. After each encryption module and data bearer provide their SK components, the Central Authority (CA) gets them all. Regardless, the CA verifies the signature of the holder. In addition, if everything checks out, the CA generates public and master keys for the system, which a new user may use to access their private information. According to the WAA in the organization, the weight of the traits is calculated.

2) Key Generation

As soon as the new user is linked to the system, CA assigns them a unique user ID. The opposite is true when it comes to the WAA receiving encrypted data from the attribute set consumer. Once the buyer signs, the attribute authority verifies their identity. If this is correct, WAA will generate the new consumer's weight and the decryption keys for the relevant characteristics. After that, the WAA and CA will each provide the new customer their own secret key—the attribute key and the system key. Public keys for the hacker are being provided at the same time, the challenger emerges victorious in key-related algorithm configuration and the central authorities.

3) Encryption

The data holder uses an unusual ID to log in and employs a symmetric data file key for encryption before publishing the data file. For every user and data file, the data holder specifies a weighted minimum access structure (W), and its use is encrypted, as seen in Figure 3.

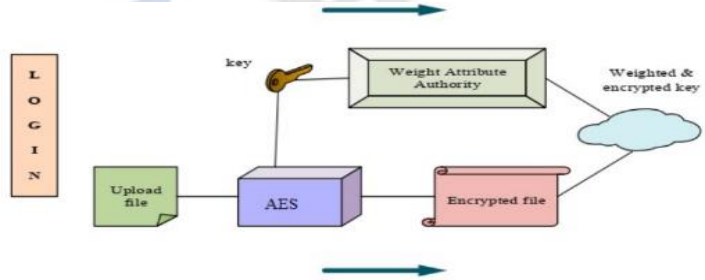

Figure 3: Process of encryption on the owner side data

4) Decryption

Customers access their data via cloud storage, download it, and use a decryption method to access encrypted data. Assuming the data consumer's associated secret key is validated, the system assigns varying weights based on their level.The next step is for the user to decrypt the individual data file in relation to W. Figure 4 shows that data file decryption fails if the user is invalidated.

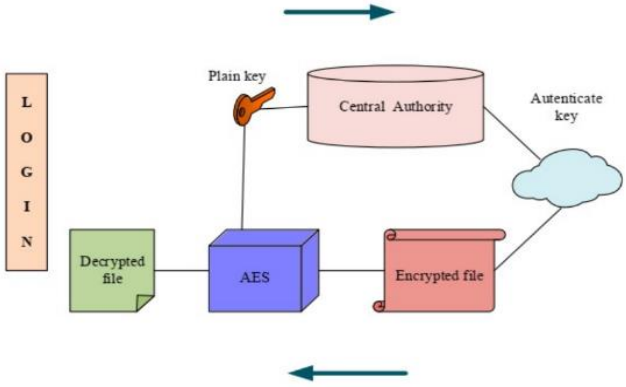

Figure 4: Decryption process of the data user side

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: *10 July 2023* ***Revised:*** *12 August 2023* ***Accepted:*** *28 August 2023*

7.2.Algorithm Phase

The two-step process that every text goes through is determined by the algorithms that are outlined below: encryption and decryption.

AES Encryption Algorithm	AES Decryption Algorithm
Key Expansion	**Key Expansion (Reverse)**
Input:	**Input**
Original key (128, 192, or 256 bits).	Original key schedule.
Procedure:	**Procedure:**
Initialize the key schedule with the original key.	Generate round keys in reverse order:
For each round key (rounds vary based on key size):	Apply byte substitution to the last 4 bytes of the key.
Apply byte substitution to the last 4 bytes of the key.	Rotate the entire key in the opposite direction.
Rotate the entire key.	Perform a bitwise XOR with a round constant.
Use a round constant to execute a bitwise XOR.	Perform a bitwise XOR with the key from (rounds - key size).
Take the key from (rounds - key size) and use it to do a bitwise XOR.	Continue the process for each 4-byte block in the key.
Continue the process for each 4-byte block in the key.	**Output:**
Output:	Reversed key schedule with round keys.
Key schedule with round keys.	**Initial Round (Reverse)**
Initial Round	**Input:**
Input:	Ciphertext (state matrix).
State matrix (plaintext).	Round key (from the reversed key schedule).
Round key (from the key schedule).	**Procedure:**
Procedure:	Use the round key to do a bitwise XOR on the state matrix.
Perform a bitwise XOR of the state matrix with the round key.	**Output:**
Output:	Intermediate state matrix.
Intermediate state matrix.	**Main Rounds (Reverse)**
Main Rounds	**Input:**
Input:	Intermediate state matrix.
Intermediate state matrix.	Using the key schedule in reverse, come up with the round key.

Round key (from the key schedule).	**Procedure for Each Round:**
Procedure for Each Round:	**AddRoundKey:**
SubBytes:	Perform a bitwise XOR of the state matrix with the round key.
Swap out all of the bytes in the state matrix with their matching S-Box values.	**MixColumns (Reverse):**
ShiftRows:	Inverse mix columns of the state matrix using matrix multiplication.
Shift rows of the state matrix:	**ShiftRows (Reverse):**
Place a one-byte shift on the second row.	Shift rows of the state matrix in the opposite direction:
Move the third column over two bytes.	Move the second row three bytes to the left.
Move the fourth column up by three bytes.	Two bytes should be moved to the third row.
MixColumns:	Place a one-byte shift on the fourth row.
Mix columns of the state matrix using matrix multiplication**.**	**SubBytes (Reverse):**
AddRoundKey:	Put the relevant byte from the inverse S-Box into place of every byte in the state matrix.
To apply the round key to the state matrix, use a bitwise XOR.	**Output:**
Output:	Updated state matrix after each main round.
Updated state matrix after each main round.	**Final Round (Reverse)**
Final Round	**Input:**
Input:	After the last major round, the state matrix is set.
After the last major round, the state matrix is set.	Round key (from the reversed key schedule).
Round key (from the key schedule).	**Procedure:**
Procedure:	**AddRoundKey:**
SubBytes:	Add the last round key to the state matrix and then do a bitwise XOR on it.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 10 July 2023 **Revised:** 12 August 2023 **Accepted:** 28 August 2023*

Substitute the S-Box bytes for their state matrix equivalents. **ShiftRows:** Shift rows of the state matrix. **AddRoundKey:** Combine the state matrix with the last round key using a bitwise XOR operation. **Output:** Ciphertext (final state matrix). **Overall Output** The final state matrix is the ciphertext.	**ShiftRows (Reverse)** Shift rows of the state matrix in the opposite direction. **SubBytes (Reverse):** Put the relevant byte from the inverse S-Box into place of every byte in the state matrix. **Output:** Plaintext (final state matrix). **Overall Output** The final state matrix is the decrypted plaintext.

For security and end-to-end encryption, the cipher text is encrypted and decrypted using the algorithms mentioned above.

8. Results

In this instance, have tested and evaluated how well the suggested task works. Encryption and decryption both include computing costs. While these systems provide secure data access control on the cloud network, they do so in an encrypted form. The suggested method's data cooperation strategies are contrasted with those of CP-ABEand HABE. With the suggested method, lightweight key management is achieved by complete delegation and partial signature with minimal strain for WAA and data users, even in large-scale consumers. In this work, it employs an AES technique to generate keys and weights, as well as encrypt and decode several input files of varying sizes (in kb). This AES method is mostly used for security functions. With little processing time, this technique performs encryption and decryption. The ultimate outcomes of the proposed system's methodology are shown in Table 2.

Table 2: Experimental outcomes of throughput, encryption/decryption, and execution time for AES-WABE.

Input data	Size of the File (kb)	Encryption Time (s)	Decryption Time (s)	Throughput (bps)
I_1	1	122	116	0.00852
I_2	2	254	227	0.00872
I_3	3	345	601	0.00878

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
***Article Received:** 10 July 2023 **Revised:** 12 August 2023 **Accepted:** 28 August 2023*

Encryption time: The encryption time must be provided when data is encrypted. One can employ it to check whether your system is fast enough and to see how well an encryption method works. As shown in Figure 5, the encryption time is the amount of time required to transform plaintext into ciphertext.

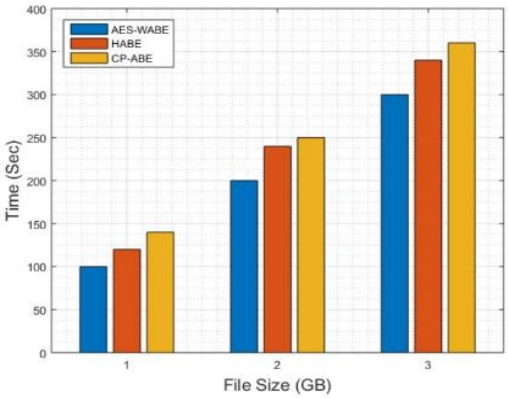

Figure 5: Encryption time of the proposed method in comparison to the current

Decryption time: The process of decryption is the inverse of encryption. The decryption time is the amount of time it takes to get the plaintext out of a cipher text. Figure 6 compares the proposed method's decryption time to that of the conventional methods.

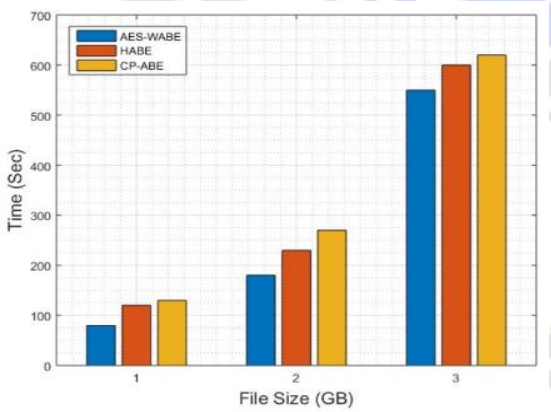

Figure 6: The suggested approach's decryption time in comparison to the current method

Throughput: The encryption time as a percentage of the total encrypted data file size is called throughput. As seen in figure 7, the suggested method accomplishes a high throughput.

$$Throughput = \frac{Sizeof the File(kb)}{Encryptiontime(s)} (1)$$

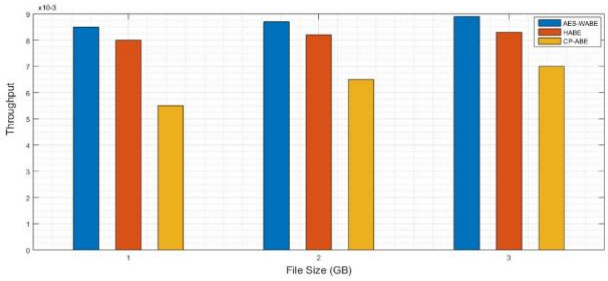

Figure 7: Throughput comparison of CP-ABE, AWS-WABE, and HABE.

9. Conclusion

Problems with user authentication and data security in a cloud setting are common. An effective and extensible system for controlling access is suggested in this research. In this study, an AES Hybridized weight attribute-based encryption method is used for data security. Data encryption and decryption are handled by AES for safe transmission. The consumer gets the encrypted files matching to the authenticated user's requests depending on their weight. The data consumer uses the key that was formed using the AES technique to decrypt the data. The experimental findings demonstrate the effectiveness and reliability of the proposed approach. Additional features, such as encryption and re-encryption depending on quality and protection-saving properties, possible future additions that might be made to this piece. Here is where a variety of approaches might be used to facilitate the exchange of data.Standards that improve cloud computing security are crucial. The cloud offers several advantages for data security, but none are a complete solution. To address this problem, create new criteria for all prior approaches and require them to be met for termination.

References

1. Youssef, Ahmed E., and Manal Alageel. "A framework for secure cloud computing." International Journal of Computer Science Issues (IJCSI) 9, no. 4 (2012): 487.
2. Bhadauria, R. and Sanyal, S. (2012) ‘A survey on security issues in cloud computing and associated mitigation techniques’, International Journal of Computer Applications, June, Vol. 47, No. 18, pp.47–66.
3. Merabti, M., Kennedy, M. and Hurst, W. (2011) ‘Critical infrastructure protection: a 21st century challenge’, in International Conference on Communications and Information Technology (ICCIT), pp.1–6.
4. H. TOUMI, A. EDDAOUI and M. TALEA.” Cooperative Intrusion Detection System Framework Using Mobile Agents for Cloud Computing”. Journal of

Theoretical and Applied Information Technology 10th December 2014. Vol.70 No.1

5. A. Pandey, et al." An Approach for Virtual Machine Image Security". International Conference on Signal Propagation and Computer Technology (ICSPCT), 2014
6. K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing, " Journal of Internet Services and Applications, 4:5, 2013.
7. Jean-Henry Morin, Jocelyn Aubert, Benjamin Gateau. "Towards Cloud Computing SLA Risk Management: Issues and Challenges", 45th Hawaii International Conference on System Sciences, 2012.
8. S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, ''Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems,'' Knowl.-Based Syst., vol. 56, pp. 216–225, Jan. 2014
9. L. Huang, S. Deng, Y. Li, J. Wu, J. Yin, and G. Li, ''A trust evaluation mechanism for collaboration of data-intensive services in cloud,'' Appl. Math. Inf. Sci., vol. 7, no. 1L, pp. 121–129, 2013.
10. Tang, Changlong, and Jiqiang Liu. "Selecting a trusted cloud service provider for your SaaS program." Computers & Security 50 (2015): 60-73.
11. Huang, Chenlin, Wei Chen, Lu Yuan, Yan Ding, Songlei Jian, Yusong Tan, Hua Chen, and Dan Chen. "Toward security as a service: A trusted cloud service architecture with policy customization." Journal of Parallel and Distributed Computing 149 (2021): 76-88.
12. Li, Xiang, Qixu Wang, Xiao Lan, Xingshu Chen, Ning Zhang, and Dajiang Chen. "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach." IEEE access 7 (2019): 9368-9383.
13. J. Sidhu and S. Singh, ''Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers,'' J. Grid Comput., vol. 15, no. 1, pp. 81–105, 2017.
14. M. Tang, X. Dai, J. Liu, and J. Chen, ''Towards a trust evaluation middleware for cloud service selection,'' Future Gener. Comput. Syst., vol. 74, pp. 302–312, Sep. 2017.
15. Liu, Bin, Xiao Liang Yu, Shiping Chen, Xiwei Xu, and Liming Zhu. "Blockchain based data integrity service framework for IoT data." In 2017 IEEE International Conference on Web Services (ICWS), pp. 468-475. IEEE, 2017.
16. S. Wang, L. Sun, Q. Sun, J. Wei, and F. Yang, ''Reputation measurement of cloud services based on unstable feedback ratings,'' Int. J. Web Grid Services, vol. 11, no. 4, pp. 362–376, 2015.
17. Noor, Talal H., Quan Z. Sheng, Lina Yao, Schahram Dustdar, and Anne HH Ngu. "CloudArmor: Supporting reputation-based trust management for cloud services." IEEE transactions on parallel and distributed systems 27, no. 2 (2015): 367-380.
18. S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, ''Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems,'' Knowl.-Based Syst., vol. 56, pp. 216–225, Jan. 2014
19. Banyal, R. K., V. K. Jain, and Pragya Jain. "Dynamic trust based access control framework for securing multi-cloud environment." In Proceedings of the 2014 international conference on information and communication technology for competitive strategies, pp. 1-8. 2014.