International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 12, Issue 4 (JULY-AUGUST 2024), PP. 64-73

DEVELOPMENT AND ANALYSIS OF FRAMEWORK FOR CLOUD COMPUTING SECURITY

Anurag Singh[1], Prachi Chauhan[2],
[1]M.Tech (CSE) Scholar, Department of Computer Science and Engineering, B. N. College of Engineering & Technology
[2]Assistant Professor, Department of Computer Science and Engineering, B. N. College of Engineering & Technology
Lucknow, Uttar Pradesh, India

***Abstract*— Cloud computing is the result of the newlinepooling of many adaptable computing resources, including servers, networks, storage, and services, to provide users with suitable and on-demand access to the cloud. Identity and access management (IAM) is a critical component of the cloud infrastructure that allows cloud-based service approval. Cloud computing is a readily manageable technology whereby the apps we use are supplied by an unidentified node that does not announce its ownership, so retaining total control of the application. Data storage has become a key problem due to the rise in computer and mobile users in all corresponding industries. These days, a lot of newlinescale firms, both big and little, are expanding quickly in relation to their data. Additionally, they are incurring significant costs for data maintenance. By using this newline technique, With cloud computing, users' need for combinational models of hardware and software are significantly reduced. Chapter 1 of this thesis provides an overview of cloud computing. fresh line This part also covered the benefits and drawbacks of newline cloud computing, as well as the necessity of cloud computing. The required literature for protecting the newline communication between the service provider and service user in a cloud environment from newlinevarious sorts of attacks is then reviewed in Chapter 2. The suggested newlinesystem in this thesis is then explained in detail in Chapter 3, which also offers the method for protecting the cloud environment using group key management newlinetechniques. Subsequently, Chapter 4 addresses a newlineaccess control mechanism for safe cloud communication between the cloud provider and newlinethe user. The work's conclusion and some potential future improvements are finally offered in Chapter 5.**

***Index Terms*— Cloud Computing, Framework, access management, necessity of cloud computing etc.**

I. INTRODUCTION

A. Fundamental Characteristics of Cloud Computing Technology

The five characteristics of cloud computing technology by NIST [2].

(i) **On-demand self-service**: A user can provide a sovereign provision of the efficiency of computing i.e. resources of the cloud must be available every time and the client firm should be able to access their resources of the cloud without providing the company's interaction.

(ii) **Broad network access:** Cloud computing is based on the network and used from anywhere and from any standardized platform (i.e. mobile devices, desktop computers, etc.) which means the capabilities are contained over the network and clients can access virtual servers and make use of their resources.

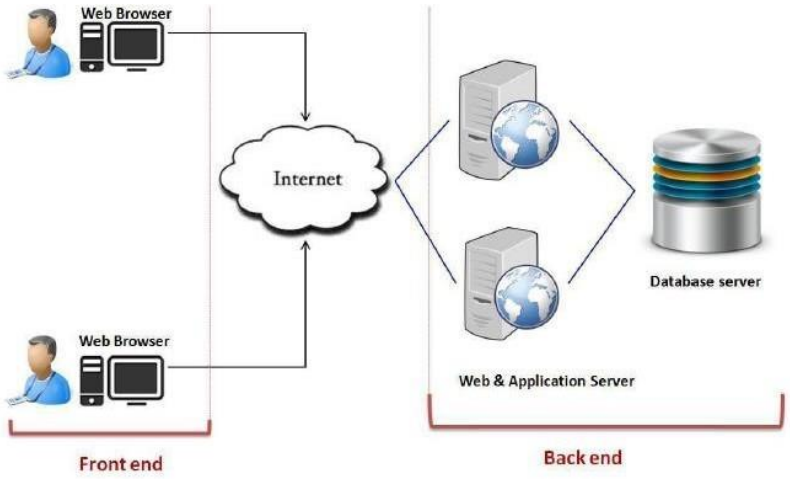
(iii) **Resource pooling:** The resources are shared in the cloud and meanwhile, the users may use the same set of resources. So, to avoid the capital outlay the provider follows the pay-as- go policy and provides the computing resources to many consumers.

(iv) **Rapid elasticity:** The response of the cloud is very quick and it can maintain a huge memory like an elastic structure. In some cases, the reactive time automatically alters to quickly scale out and quickly released to quickly scale in.

(v) **Services measured:** The cloud supplier must maintain and improvise the resource in terms of utilization of electricity and measures the amount of service provided and responds accordingly (both in terms of updating and software and hardware billing the client as appropriate).

B. Cloud Computing Architecture

The components that are employed and the way that cloud computing operates now are derived from its architecture. There are two parts to cloud computing: the front end and the back end. The front end of the cloud computing system contains the client component. It is made up of the applications and interfaces required to work with the cloud computing platform [3].



igure 1.1: Cloud Computing Architecture.

Moreover, the phrase "back end" specifically denotes the cloud infrastructure that contains the essential resources required for delivering cloud computing services. The management of the system is handled by the provider and includes servers, virtual machines, data storage, security measures, and other components. Cloud computing enables the sharing of files across several computers and disc drives. Due to the decentralised nature of the data storage, in the event of a failure in one unit, the other unit will autonomously assume control. The user's disc space is divided among the distributed system files, and an additional crucial consideration is the resource allocation mechanism. Cloud computing is primarily powered by the newest technique, which is widely recognised as a resilient distributed system [4].

"Cloud computing encompasses applications delivered as services over the Internet, with datacenters housing the necessary hardware and software models to facilitate the provision of these services." The presentation introduced a utility-oriented distributed computing system, as defined by Armbrust et al., which consists of networked and virtualized PCs that are installed dynamically. The service-level agreements between the service provider and the consumers determine the computer resources that are shown as a consequence. The notion proposed by Buyya et al. pertains to the first iteration of the ongoing evolution of distributed systems. Private distributed systems use a variety of resources, such as third-party data centres, to support their computing infrastructures and software applications. Access to these resources is provided over the Internet.

C. Problem Statement

The cloud computing also known as cryptographic attacks. In the cloud, the integrity and data security are believed to be the most difficult issue among the main security problem that could limit the cloud computing usage. Actually, key management and access control are all issues involved in data security [8].

D. Necessity of Cloud Computing

Data storage has grown to be a key problem in all related industries due to the rise in computer and mobile users. Nowadays, a lot of firms, both big and little, are expanding quickly in relation to their data. Additionally, they are incurring significant costs for data maintenance. This successively trusts on a very rigid help of IT and storage point. Every business could not afford this great expenditure sustained on the in-house infrastructure of IT and support of backup services. The cost-effective solution for them is seen as cloud computing. Maybe its capability and effectiveness in the computational area, data storage, and less maintenance cost have made this technique attractive even for large- scale businesses [9]. The user's requirements for combinational models of hardware and software are greatly reduced by using this Cloud computing technology. The user must be proficient to operate cloud computing and that is the single thing offered by the consumer side, which should be simple as that of browsing the Web. The cloud network handles the balance matters, at some moment of time and an interesting insight are that what we experience in cloud computing. Some of the cloud services that are commonly known are mail services like Gmail, Hotmail or Yahoo, etc. Our data is essentially stored on the server of the cloud and not on our PCs when using E-mail services. The technology and infrastructure which is the backbone of the cloud are unseen. It is considered to the minimum as by which the cloud services are based on XML (extensible mark-up language), HTTP (Hypertext transfer protocol), Ruby, PHP, or other corresponding languages moreover it is easy to use and functional. The cloud system can be accessed by the cloud user by their personal devices like desktop, mobile, or laptop.

Cloud computing holds the skills of perfectly managing micro-level businesses by means of possessing some amount of resources; it provides technological access to small companies the technology that was out of range already [10].

Cloud computing allows small-level businesses to transfer the cost of maintaining their business into profits. We have to pay a lot of attention to the in-house IT services to make sure that there are no errors in the system such that it works finely. We are completely responsible in case of any technical bugs. Thus it proves that a lot of focus is needed for an effective and efficient operation of the system without any flaws. Thus we can fix that both time and money are to be invested in excess for high success. In cloud computing, the service provider is completely responsible for the complications issues and the technical faults that arise.

II. LITERATURE REVIEW

The chapter addresses a number of technical difficulties in putting cloud computing into practice as well as security problems related to cloud computing, namely those involving data security, integrity, and authentication. Security problems such malware code injection, worms, viruses, Denial of Service, password cracking, and scanning are frequent in cloud systems. Ignoring these assaults may cause financial losses and damage to a company's image. This chapter reviews and suggests a taxonomy for the current issues with authentication and access control arising from the cloud computing pattern viewpoint.

In order for the user to get the aforementioned services from the service provider over the Internet, they must submit a request, and the service provider allots and maintains the resources necessary to fulfil the user's demands [39, 40]. The service providers who manage resources and schedule incoming requests in order to optimise income via resource allocation are the scheduling algorithms and resource allocation. The two main concepts in a real-time cloud computing environment that need approval are scheduling and resource allocation [41, 42]. "A paradigm for facilitating on-demand, convenient network access to a shared pool of framed computing resources that can be provisioned rapidly and liberated with a nominal management effort or the contact of the service provider" is how the National Institute of Standards and Technology (NIST) defines cloud computing [43]. The NIST cloud computing model has five key components: access, rapid elasticity, sample network resource pooling, evaluated service assessment, and service on-demand self-service. There are four deployment models—Private, Public, Community, and Hybrid—and three service models—Software, Platform, and Infrastructure. The SPI model is another name for the models already discussed. Among these three SPI models, the Infrastructure as a Service (IaaS) model has the greatest intrinsic standard since it offers a wide range of goods and innovative features like pay-per-use, on-demand provisioning, and self-regulating scalability [44–47]. The business transition is carried out by several organisations across the cloud. The primary goal is to implement their strategy at the lowest possible cost and to get quick approval for applications pertaining to exceptional company [48]. The cloud offers several advantages, including widespread network access, quick service updates, quick stationing, scalability, quick provisioning, flexibility, notable elasticity, data storage options, affordable catastrophic restoration, metered services, etc. [49].

Flexibility and Multi-tenancy are the two key components of the cloud concept. Flexibility in the cloud refers to the capacity of the system to scale up or down in response to current service needs. Multi-tenancy allows tenants to share comparable service instances among themselves [50]. The earnings from companies and academies to drive cloud use are attracting the curiosity of new customers. While the cloud provides these services, there are a lot of challenges in adjusting to them. Numerous academics have focused their attention on this particular context, considering security from multiple angles, including application, data transfer, data storage, third-party software, user authentication, etc. Going back to each service, cloud computing provides a shared and accountable security approach.

Both cloud users and providers are responsible for the infrastructure of cloud residents as well as the security of applications distributed via the cloud. The security needs differ for each delivery type. In terms of data security, the client has responsibility for some services such as user access and identity management, regardless of the delivery type (IaaS, PaaS, and SaaS). Prior to release, the patches or security updates need to be thoroughly checked, repacked, and stored in the repository [51–53]. When it comes to system maintenance, the primary function is to support user collaboration with the supplier. They need to apply the fixes on the stack application and operating system (OS). Furthermore, patching and upgrading the operating system and several other apps should be the system administrator's primary responsibility inside the cloud architecture [54].

III. EFFECTIVE ACCESS CONTROL MECHANISM IN CLOUD FRAMEWORK: AES-LIGHT WEIGHT CP-ABE BASED PRIVACY PROTECTION FRAMEWORK

Cloud computing is a kind of computing where a variety of adaptable computing resources, including servers, networks, storage, and services, are combined to provide users with suitable and on-demand access [111]. Cloud computing is used in many business domains and is often brought up in conversation. The cloud framework's cloud service providers (CSPs) are accountable for the administrational modules and equivalency. Numerous incidences of data leakage are caused by the liabilities inherent in identity management systems [112]. Identity and access management (IAM) is a critical component of the cloud infrastructure that allows cloud-based service approval. As of right now, the identity management procedure falls within the purview of the CSP, and it seldom

ever faces the limitation of a user's flexible and granular access control policy. Data secrecy in cloud computing is uncertain [113,114]. Personal information may be leaked to any third party if data is kept according to its original format. As a result, the private information of the data owners is kept off the public cloud. Thus, a new approach to access control is needed for the public servers. Data encryption is done utilising a variety of encryption techniques to accomplish this. Encryption is used to regulate access to data, ensuring data confidentiality. Malicious individuals are prohibited from accessing personal information without authorization.

A. PROPOSED FRAMEWORK

1) Preliminaries

a) Bilinear maps

The two multiplicative cyclic groups are G1 and GT with the prime order p[121]. The initiator of G1 be g and the bi-linear map is e, e : G1 ×G1 → GT , having the subsequent features:

$$Bilinearity: for \text{ all } g, g \in G_1 \text{ and } a, b \in Z_p, e(g^a, g^b) = e(g, g)^{ab}$$

$$Non-degeneracy: e(g, g) \neq 1$$

2) CP-ABE background

Setup: The universal attributes are considered as a parameter by this setup algorithm and use the key authority for execution which creates a public parameter and master key [122].

KeyGen: The key authority executes this KeyGen algorithm and produces the secret key.

Encrypt: A message M is achieved by this encryption algorithm and encrypts with the help of the public parameters.

Decrypt: The user executes this algorithm by user secret key and the cipher text obtained from the cloud.

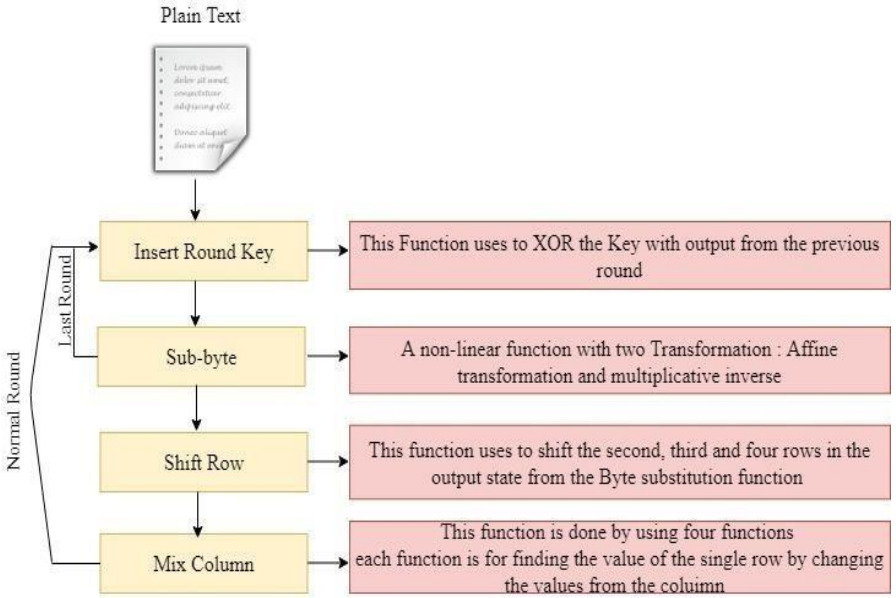


Figure 3.1.Framework designed for securing data privacy

3) Communication of Data Owner

The data is uploaded in the cloud system through the data owner that can be used by many legitimate users. For uploading the communication an evaluation was conducted for the proposed method with different user numbers. After validation, it was found that the communication of the data owner upsurges with a surge in the number of users. When compared with the existing ABE approach the proposed method attained improved performance with an 895 KB value whereas ABE attained 989 KB, as presented in Figure 3.2.

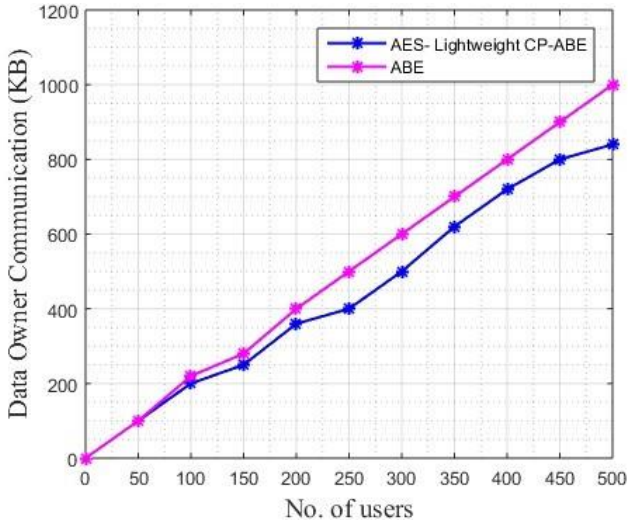


Figure 3.2. The data owner's upload communication graph

4) Encryption and Decryption Time Cost

Tables 3.1 and 3.2 presents the Encrypting and decrypting time and costs with distinctive- sized information and aggregate cipher-text attributes. The proposed approach attained a rise in the encryption and decryption time when compared with the Improved-CP-ABE (I-CP- ABE) [32] with fewer attributes. The time gets minimized when there is an increase in the attributes. With the attributes of more than 40 KB, the proposed scheme executes in a better way.

Table 3.1. Proposed and obtainable scheme's Encryption time concerning different data sizes.

Size of data	**No of attributed**	**Encryption time (ms)**				
		10	**20**	**30**	**40**	**50**
10kb	I-CP-ABE	100	200	450	550	650
	Proposed	215	277	395	475	555
50 Kb	I-CP-ABE	190	400	500	650	750
	Proposed	287	435	560	585	695
100Kb	I-CP-ABE	275	445	650	750	1000
	Proposed	365	485	598	645	855

Table 3.2. Presented and related methods Decryption time of the concerning various data sizes

Size of data	**No of attributed**	**Decryption time (ms)**				
		10	**20**	**30**	**40**	**50**
10kb	I-CP-ABE	80	95	115	155	195
	Proposed	115	120	130	155	175
50 Kb	I-CP-ABE	115	135	155	250	350
	Proposed	135	145	155	185	250
100Kb	I-CP-ABE	300	400	450	550	750
	Proposed	300	385	420	530	620

B. SUMMARY

In the cloud storage space to guard data privacy the new encryption scheme named, AES Lightweight CP-ABE was proposed. Double encryption was performed by the proposed scheme on the cloud data. Initial encryption was done by the *Lightweight* CP-ABE, and using AES the secondary encryption was accomplished. Based on the digital signature the access control was given. The user and the owner acquire authentication in the cloud framework. When the user tries to access the cloud, with a certain question the attribute set was made that appears randomly. The simulation outcomes revealed that the proposed scheme achieved improved performance than the existing approach with minimum execution time and communication of the data user. As a future enhancement, a multi-user cloud environment could be focused on to offer robustness and improved security features.

Moreover, the proposed approach can be boosted to deal with the user groups and multi-owner character in the cloud more professionally.

IV. DATA SHARING SCHEME THAT IS SECURE AND RELIABLE IN A CLOUD ENVIRONMENT USING AES WITH WEIGHTED ATTRIBUTE-BASED ENCRYPTION

The cloud storage service is regarded as a wonderful tool with efficient methods that can manage a vast volume of data. This facility allows for the storage of both personal and commercial data, which is why many businesses, places, and individual users utilise it.

Information is uploaded to the cloud via the cloud data provider and thereafter accessed by the user with the assistance of the cloud server. The cloud storage identifies the multi-regional, multi-domain, and comprehensive data exchange. The advantages of cloud storage include minimal resource requirements, cost-effectiveness, easy maintenance, and user storage management. [123, 124]. The primary concern with cloud storage services, despite their many benefits, is security. Since the information stored in the cloud is accessible to many geographically dispersed data centres, the user's data in the cloud's database is not under their control. When using cloud computing, users have issues with data confidentiality and privacy [125]. Owing to the difficulties in using this [126,127], only authorised users have access to the cloud-based data resources. In order to address this, data should be encrypted prior to being uploaded to cloud infrastructure; nevertheless, this method restricts data exchange and processing beyond that point [128]. Typically, the data owner downloads the encrypted data from the cloud storage to re-encrypt it before sharing it. Furthermore, cloud users may take on the role of content suppliers. They broadcast the data on cloud servers, using fine-grained data access control to distribute and access those contents. [129–132]. Furthermore, the CSP must keep the data's contents private in order to protect it from cloud users [133].

The suggested AES-WABE technique achieves a safe and effective data connection. The current ABE techniques deal with both the secret and public keys via unique access. In a particular scenario, the consumers of the attributes manage the attributes from various authorizations of the attributes, and the data holders share the consumer data under the jurisdiction of various authorities. Several attribute-based multi-authority access control systems are offered to address this issue. In this research, the AES is used to offer attribute weighting in order to produce secure data. This system takes into account five fundamental modules: As seen in Figure 4.1, the process involves the following: (a) a cloud server that stores the data; (b) the data holder who uploads the data to the cloud after encoding it using an access control policy; (c) a weight attribute Authority (WAA) based authorization that verifies and updates the user's attributes; (d) the Central Authority (CA) that provides a consumer public key and global user identifier to WAA for each consumer; and (e) the data users. The AES is merged with the weighted ascribed authority and is shown in Figure 4.1.

The suggested method encrypts and decrypts the data using the AES, which then randomly creates the keys. Additionally, an image-matching approach is used for security reasons. Afterwards, the algorithm assigns each user a weight value depending on their qualities.

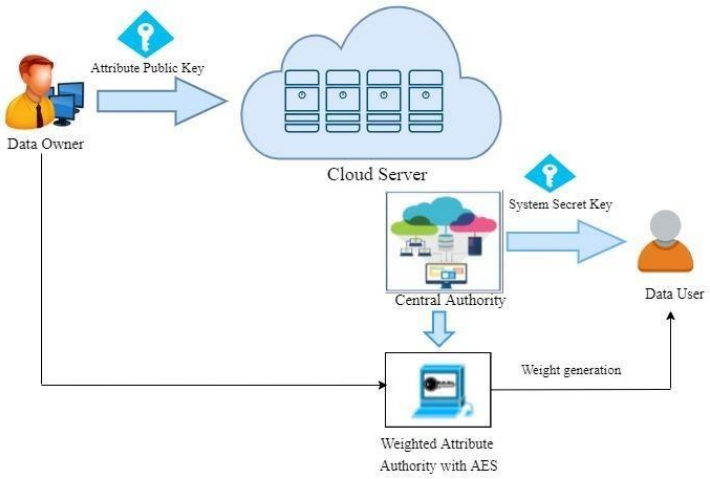


Figure 4.1.The Proposed Framework (AES-WABE)

In contrast to traditional approaches, this system is safe and dependable, making it appropriate for real-time applications. The suggested encryption takes into account fine-grained access control, collusion resistance, and multi-authority security. The suggested approach consists of two phases: the algorithm phase and the system phase. The AES algorithm is used to specify the system-level operations in this phase of the algorithm. When there is a disagreement, the most important operations—like user cancellation, system setup, granting access to new users, creating new files, file access, and deletion—are explained at the system level.

1) Operations in Algorithm Level

a) AES Encryption

According to the substitution-permutation network, AES [137] is an alliance of permutation and substitution that offers great hardware and software efficiency. Unlike DES and AES, this method does not make use of a Feistel network. As shown in Figure 4.2, AES is a variation of Rijndael with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

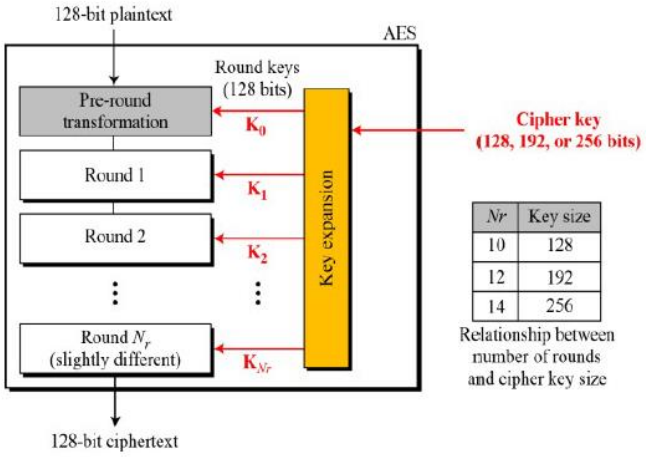


Fig. 4.2. AES Encryption process

The number of replications of transformation rounds that convert the input, or plaintext, into the final result, or cypher text, is indicated by the key size employed in an AES cypher. The number of cycles in the repeat are as follows:

- 12 cycles for keys with 192 bits;
- 14 cycles for keys with 256 bits.
- For 128-bit keys, 10 cycles.

There are four linked but distinct phases in each of the specific processing steps for all-around. Two reverse rounds are used with an encryption key that is comparable to convert the cypher text into plaintext. AES uses the four sorts of transformations listed below to give the security.

- **Permutation:** This step exchanges states by moving each row to a certain number of stages.
- **Substitution:** Each byte is changed at this step in accordance with the lookup table.
- **Mixing:** Four bytes are merged in each state column at this step, which works with those columns.
- **Adding keys:** At this point, the state unifies the partial key, and Rijndael's key schedule produces a sub key from the chief key that is about the same size as the state.

B. Results and Analysis of the Experiment

We have tested and evaluated the suggested work's performance in this part. Java is used in this study, and an Intel Core i3 CPU with 8GB of RAM is used for data processing. Both encryption and decryption have computational costs. These systems provide data security even though they are able to regulate encrypted data access in the cloud network. The suggested approach's data cooperation schemes are compared with those of the CP-ABE [34] and HABE [35] approaches. The suggested method enables lightweight key management by achieving complete delegation and partial signing in a large-scale consumer with minimal effort (WAA and data user). The AES technique used in this work generates weight and keys in addition to encrypting and decrypting several input files of varying sizes (in kb). The primary purpose of this AES algorithm is security. This technique takes relatively little time to execute and does both encryption and decryption. The end outcomes of the suggested system's approach are shown in the table.

Table 4.1. 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)	Through put (bps)
I_1	1	120	115	0.00850
I_2	2	235	226	0.00870
I_3	3	344	600	0.00876

Time of Encryption: The amount of time needed to encrypt data is called the "time of encryption." It is used to verify system performance and evaluate an encryption method's throughput. The amount of time needed to convert plaintext into ciphertext is known as the encryption time. We can see the encryption time in Figure 4.3.

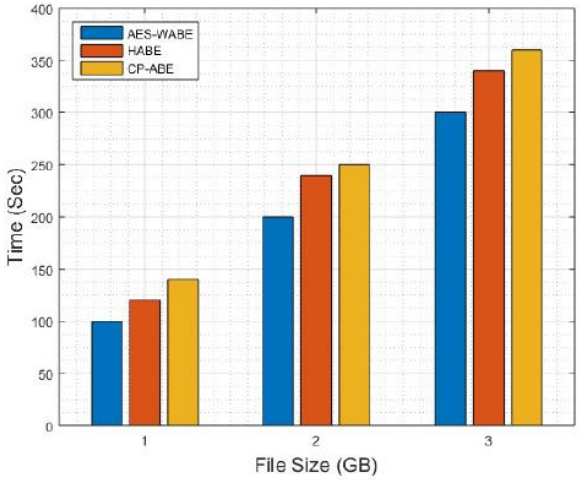


Figure 4.3. Proposed scheme Encryption time compared to Existing

Time needed for decryption: Decryption is the opposite procedure of encryption. The decryption time is the amount of time needed to extract plaintext from a ciphertext. The decryption time of the suggested approach is shown in Figure 4.4 in comparison to the traditional approaches.

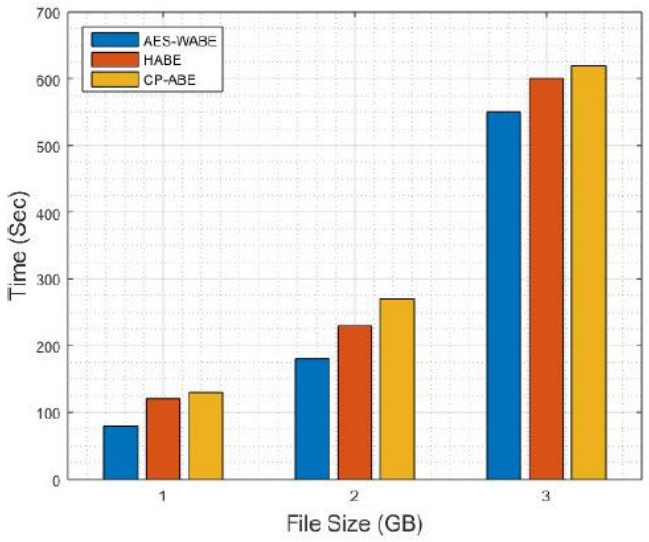


Figure 4.4.: The decryption time of the suggested approach in comparison to the current methods.

Throughput: The ratio of the encrypted data file to the encryption time is known as throughput. Figure 4.5 illustrates the high throughput that the suggested method produces.

$$Throughput = \frac{\text{Size of the file (Kb)}}{\text{Encryption Time (s)}} \quad (1)$$

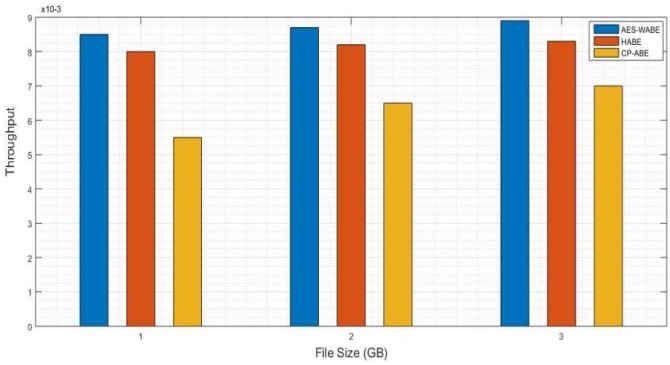
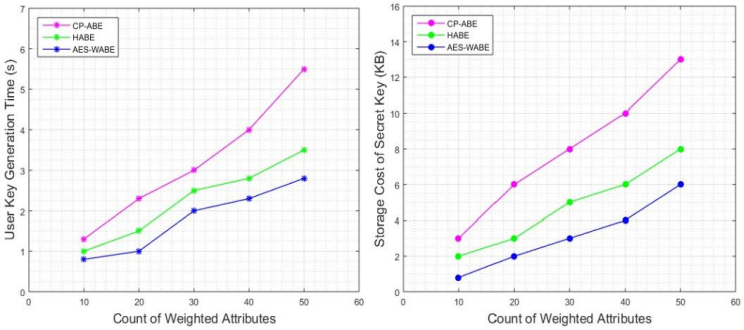


Figure 4.5. Throughput Comparison of CPABE, HABE and AES-WABE

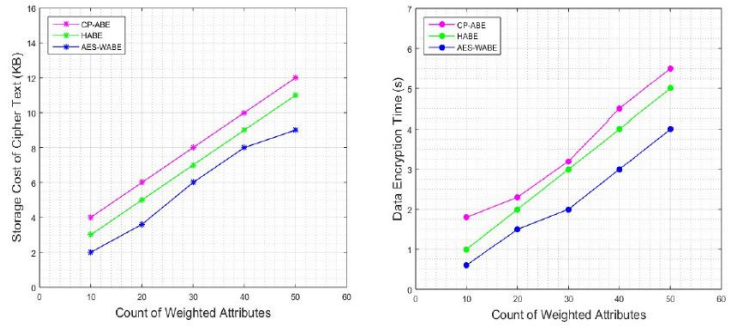
Rate of analysis for the secret key: Figure 4.6 shows a plotted analysis of the overhead storage and secret key calculation costs. The X and Y axes show the total number of weighted characteristics as well as the storage overhead or time cost.



(1) (2)

Figure 4.6: Cost analysis of time 2 storage analysis and cost production of user secret key:1

Cost of cypher text analysis: The compute and storage elevation cost of data encryption is shown in Figure 4.7. The amount of weighted characteristics and the time or storage overhead associated with data encryption are shown by the X and Y axes.



(a) **(b)**

Figure 4.7. Cipher text cost. (a) Analysis of Storage cost; (b) Analysis of Time cost

1) Security Analysis

AES-WABE, as suggested, encrypts shared data. The following analysis is done on the protective properties of the suggested scheme:

2) Fine-Grained Access control:

Individual data may have adjustable differential access permissions thanks to this method. This kind of access control is implemented using the AES-WABE scheme. The data owner enforces a flexible and expressive access policy throughout the encryption phase of the suggested approach, and a symmetric key is utilised to encrypt the data. The AND and OR gates, which stand for any desired access criteria, are applied to the

stated access policy in the tree during access essential procedures.

3) Data confidentiality:

Access policies are used to encrypt data, providing a safeguard against users who comply with the policy but fail to retain the specified properties. The value A = e (h, h)gt cannot be retrieved in a cypher text in order to get the expected value of the global key (GK), since the set of attributes cannot satisfy the access policy during the decryption phase. As a result, the user decrypts cypher text with appropriate properties that adhere to the access policy. A random symmetric key called CK is used to encrypt the data. AES-WABE is used to safeguard it. Due to the security of the symmetric encryption system and AES-WABE, the confidentiality of the outsourced data is guaranteed against unauthorised users.

V. CONCLUSION AND FUTURE WORKS

A. Conclusions

Its main objective is to provide a solution to the problem of data security that is the main concern of anyone looking to adopt cloud services. An attack protection framework has been created in the cloud environment that will shield data, messages, and information from a variety of attacks. Authentication is done in three stages, data access is secured, and it is publicly verified. In addition to protecting against unauthorized access and untrusted servers, the method is also protected against third-party verification.

As a result of experiments, the proposed method shows to be very efficient, but there is one disadvantage, during data modification, the tags and blocks must be updated, incurring computation and communication costs. With a decentralized double encryption mechanism, scalability, and data confidentiality, it is possible to work in a more secure manner.

In addition to delegating computation-intensive tasks to cloud servers, the proposed system protects the content of the data without disclosing it to the data owner or information about user privileges, as well as accountability. It is observed that sharing medical information on cloud platforms is feasible, economical, efficient, flexible and more beneficial to human beings. Defence data privacy is the primary goal of the "Advanced Encryption Standard with Lightweight Cipher-text-Identity and Attribute-based Encryption" (AES–Lightweight CP-ABE).

B. Future Works

In the near future, the effective functioning of the system will be the primary focus of our efforts to produce a clear and suitable standard. Additionally, we'll concentrate on standardisation and developing a policy-based access control system for users, giving them access to data that will raise the security of the cloud. The tiered pooling of resources will give rise to various security problems. Nevertheless, this has been somewhat mitigated by the work completed so far, and further developments may be provided on this as well.

Our objective is to expand on the work we have presented for real-time apps integrated into public clouds that provide public auditing services as well. We will also investigate the possibilities of putting the suggested plan into practice in a federated cloud, which integrates various clouds and offers clients access to numerous cloud service providers. Additionally, to improve the access control solution so that real-time apps may use it, and to include the data auditing capability into the recommended plan to make sure the data is accurate. Higher-level research in this area may lead to solutions that have a significant positive impact on the organisations in terms of lower operating costs, transparency, virtual availability, mobility, and portability.

REFERENCES

[1] Fithri, D.L., Utomo, A.P. and Nugraha, F., 2020. Implementation of SaaS cloud computing services on E-learning applications (case study: PGRI foundation school). In Journal of Physics: Conference Series (Vol. 1430, No. 1, p. 012049). IOP Publishing.

[2] Mrozek, D., 2020. A review of Cloud computing technologies for comprehensive microRNA analyses. Computational Biology and Chemistry, 88, p.107365.

[3] Murthy, C.V.B., Shri, M.L., Kadry, S. and Lim, S., 2020. Blockchain-based cloud computing: Architecture and research challenges. IEEE Access, 8, pp.205190- 205205.

[4] Loubière, P. and Tomassetti, L., 2020. Towards cloud computing. TORUS 1– Toward an Open Resource Using Services: Cloud Computing for Environmental Data, pp.179-189.

[5] Alshouiliy, K. and Agrawal, D.P., 2021. Confluence of 4g LTE, 5g, fog, and cloud computing and understanding security issues. In Fog/Edge Computing For Security, Privacy, and Applications, pp. 3-32. Springer, Cham.

[6] Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V. and Hossain, E., 2020. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access, 8, pp.118433-118471.

[7] Jeevitha, J.K. and Athisha, G., 2021. A novel scheduling approach to improve the energy efficiency in cloud computing data centers. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6639-6649.

[8] Kaur, J. and Sidhu, B.K., 2017. Task Scheduling in Cloud Computing using Various Techniques. International Journal of Advanced Research in Computer Science, 8(5).

[9] Sadhasivam, N. and Thangaraj, P., 2017. Design of an improved PSO algorithm for workflow scheduling in cloud computing environment. Intelligent Automation & Soft Computing, 23(3), pp.493-500.

[10] Munguti, S. and Opiyo, E., 2018. Factors influencing the adoption of cloud computing in software development companies in Kenya. International Academic Journal of Information Systems and Technology (IAJIST), 2(1), pp.126-144.

[11] Gundu, S.R., Panem, C.A. and Thimmapuram, A., 2020. Real-time cloud-based load balance algorithms and an analysis. SN Computer Science, 1, pp.1-9.

[12] Liu, S., Yue, K., Yang, H., Liu, L., Duan, X. and Guo, T., 2018, May. The Research on SaaS Model Based on Cloud Computing. In 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 1959-1962). IEEE.

[13] Hadi, F., Aliouat, Z. and Hammoudi, S., 2020. Efficient Platform as a Service (PaaS) Model on Public Cloud for CBIR System. Ingénierie des Systèmes d Inf., 25(2), pp.215-225.

[14] Malla, S. and Christensen, K., 2020. HPC in the cloud: Performance comparison of function as a service (FaaS) vs infrastructure as a service (IaaS). Internet Technology Letters, 3(1), p.e137.

[15] Al-Ahmad, A.S. and Kahtan, H., 2018, July. Cloud Computing Review: Features And Issues. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-5). IEEE.

.