iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55335

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Secure Big Data Storage on Multi-Cloud Servers with Enhanced Attribute-Based Access Control

Sandeep Gajanan Sutar[1], Dr. Manjunathswamy B E[2], Neha Sambhaji Suryavanshi[3]
[1, 2]*Department of Computer Science and Engineering, Don Bosco Institute of Technology, Bangalore*
[3]*Department of Computer Science and Engineering, Annasaheb Dange College of Engineering and Technology, Ashta, 416 301, India*

Abstract: ***Data outsourcing is now subject to additional safety and privacy concerns as a result of the rise in cloud computing demand. Because data management was moved to words an unstable cloud during the outsourcing stage of the data, data permit control identified a key problem in the cloud repository. This analysis uses the Attribute-Based Access Control method to control access to the cloud storage to solve the issue. The data is reserved in the cloud and protected by strict security before the user may access it. This model takes into account specific properties of the cloud data stored in the database authentication process in order to store the information of registered collections alongside the user-committed data. Each of the clusters has a unique set of benefits, including usernames, group names, and registry message authorization codes. Prior to sending the data to the service provider, it should be encrypted to ensure its security. However, there may occasionally be problems with the supplier's security measures. In this outcome, a variety of metrics are analyzed, such as the amount of time used for encryption, decryption, key generation, and time consumption. The numerous existing techniques, like Nth Truncated Ring Units and Cipher text. Constraints on online storage access may make policy attribute-based encryption impossible. The time of encryption is reduced by 20% and 36%, respectively, via NTRU and CP-ABE. The proposed technique decrypts data 10.64% faster than the current approach, which decrypts data 19% more slowly.***

Keywords: Cloud-computing, Big Data, Cipher text, Attribute-Based Encryption, authentication, multi-cloud.

I. INTRODUCTION

Due to its great volume, velocity, and/or increased diversity of information assets, big data demands novel types of processes to allow decision-making enhancement, discovery, and operation optimization. Big data administration is challenging with existing database management technologies because of its complexity and size. Data outsourcing to a cloud server with the capacity to hold a lot of info and quickly handle user access requests is a practical alternative.

Since a cloud server is not allowed, sensitive information may be leaked when a data owner contracts with a cloud to store their data; as a result, frequently the encrypted text of the data is stored in the cloud. However, there are still many questions about ways to make the cipher text saved into a cloud whenever the owner of the material creates an access policy. And how to validate the accuracy of a user's request for data access. Making cloud-based large data storage viable and persuasive involves two major issues. Before safely altering a cypher text in the cloud-based access policy created by the data owner, it is essential to validate that the users' access is authorized.

Based on the NTRU cryptographic system, it provides a secure and verifiable strategy for managing access to large data stores in the cloud. For massive storage data on Multi-cloud servers, our suggested architecture also offers a safe and verifiable access control method. Multi-cloud refers to the use of numerous cloud services in a heterogeneous infrastructure.

The phenomenon of the IT business has entirely transformed because to cloud computing. It gives user's access to cheap, highly scalable, on-demand computer resources that can run specified programs and store data. However, adopting and using cloud computing only works if security is guaranteed. Lack of security, secrecy, and visibility characterize cloud computing. Securing the cloud entails securing the data. Encryption provides security. To protect the security of the cloud, there are several different encryption protocols.

Users can encrypt and decode communications based on user properties using the encryption with a public key technique known as attribute-based encryption. In this implementation, the size of the cipher-text is proportional to the number of connected features, and the number of features used affects the time it takes to decode the data. Outsourced decryption is utilized in the cloud to speed up decryption. ABE cipher text is turned into simple cipher text by giving the cloud a transformation key, and recovering the plain text and trans- formed to cipher text only requires a tiny computational expense on the part of the user.

©IJRASET: All Rights are Reserved

A suggested technique is provided to ensure that the transformation conducted out by the cloud server is accurate and that the data is not manipulated by the untrusted servers. By doing this, safe and reliable outsourced decryption is provided.

Cloud computing technology concepts have significantly evolved in recent years into a new means to deliver shared services and data through the internet. Since users may export their data to public cloud storage that can offer access to data as a service, this prototype especially supports an efficient method of data sharing across cloud users. Questions about the security of the services are brought up in light of this new approach. Organizations all around the world view technology as a crucial component in lowering costs and enhancing production and efficiency. The latest developments in cloud computing technologies assist businesses in lowering computing expenses while increasing output. The demand for cloud- based technologies is escalating due to the emergence of SaaS applications and the continuously growing interest in cloud services and technology. In addition, non-enterprise consumers are increasingly utilizing cloud computing technologies due to the expanding influence of web technologies. Cloud services will dominate the current business landscape in the ensuing era. Despite the enormous potential of cloud computing, there are still several technological obstacles that prevent the widespread use of the technology.

1) Users of Apple, Google, and Amazon services have recently faced privacy risks

2) Unmistakable signs that, from the users' perspective, cloud is intrinsically insecure.

Researchers find it difficult to protect user privacy in the cloud computing environment since consumers don't have access to the internal workings of cloud service providers. The following issues with maintaining privacy in the cloud are listed by Yanbin Lu and Gene Tsudik [2]. When deploying SaaS applications on cloud computing technology, do enterprises out- source their data to cloud servers? How can user private data be protected from misuse by the cloud server?

a) How may such supplied data be protected?

b) How can I query the cloud server without disclosing my query information?

c) How can I query data coming from untrusted entities?

d) How can users have fine-grained access control at the content level?

The term "cloud computing" describes computational services that are available on demand, especially the gathering of data and execution power [3]. The idea is used to describe 'data centers; that is reachable through the Internet by several users without the user actively controlling them [4]. A growing number of companies and individuals are moving their personal information, large archive systems, and other types of data to cloud data storage because these services provides a variety of appealing features like unlimited storage, transparent pricing, and enduring services[5].

Additionally, consumers have unlimited access to services and apps. However, a number of recent studies have found that 88 percent of cloud users are concerned about the privacy of their data, and protection is commonly regarded as the main benefit of adopting cloud data storage[6]. Cloud is a technology that enables CSP to give consumers situated all over the world applications, calculations, and information collecting [7].

Recently, it has caught the interest of both academic institutions and IT companies. Platform, Infrastructure, and Software as a Service are the major service delivery methods in cloud computing [8]. The four types of clouds are private, public, community, and the hybrid. The advantages of the cloud computing include pay and use, reliability, agility, and the flexibility. The benefits of cloud computing include scalability, inexpensive information technology costs, dependability, market stability, and nearly infinite efficiency [9]. It has two significant access control and data protection problems, data and security deteriorating when examining its web-based services [10]. Users can access data stored on cloud servers using an access management approach [11]. More and more businesses and organizations are choosing servers for their databases due to the rapid development of big data systems and cloud computing [12]. The bulk of cloud data, including private medical records and internal corporate data, are incredibly susceptible [13].

II. ATTRIBUTE BASED ACCESS CONTROL SYSTEM

A security paradigm called attribute-based access control (ABAC) enables fine-grained access control based on user attributes and resource attributes. In ABAC, Attributes are used to specify access control policies, such as user roles, job titles, locations, and other contextual information. These attributes determine whether a user is permitted to use a specific resource or carry out a specified action. ABAC provides a flexible and scalable approach to access control that can handle complex security requirements and dynamic environments. ABAC systems can be used in various applications, such as cloud computing, healthcare, and finance, where the need for fine-grained access control is critical. With ABAC, organizations can ensure that their sensitive data and resources are only accessible to authorized personnel while minimizing the risk of data breaches and cyber-attacks.

The adoption of ABAC systems is on the rise. It is expected to become the dominant access control model in the future due to its flexibility, scalability, and effectiveness in managing access control policies.

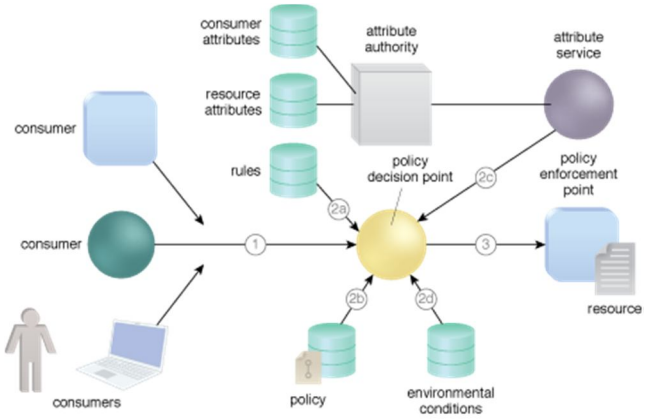


Figure 2.1: Basic Architecture of ABAC System

Figure 2.1 shows the basic architecture of ABAC System. It has the three major parts of an attribute-based access control (ABAC) system namely, the Policy Decision Point (PDP), the Policy Information Point (PIP), and the Policy Execution Point (PEP).

The PEP is in charge of implementing access control regulations and restricting access to resources in accordance with the PDP's decisions. The PEP is typically integrated into the application or system being protected and intercepts access requests from users or applications. To determine whether to allow or deny access to a requested resource, the PEP sends a request to the PDP.

The PDP, the central element of the ABAC system, is in charge of choosing which users have access to resources based on rules and attributes. The PDP receives requests for access from the PEP and compares them to the rules that are kept in its policy repository. The policies are defined using a policy language that specifies the attributes required for access, the terms and conditions that apply to entry and the actions that are permitted with respect to the resource. In order to decide on access control, the PDP also considers the user's attributes and the characteristics of the resource being sought.

The PIP provides additional information to the PDP to decide on access management. The PIP retrieves attribute values from various sources, such as user databases, identity management systems, and other external sources. The PIP then sends the attribute values to the PDP for use in evaluating access requests. The ABAC system architecture consists of the PEP, PDP, and PIP components, which work together to evaluate access requests, enforce policies, based on individual characteristics and resource characteristics, and regulate access to resources. The ABAC system provides a flexible and scalable approach to access control that can handle complex security requirements and dynamic environments.

III. LITERATURE REVIEW

For massive data in the cloud, Chunqiang Hu, We Li, and others presented a verifiable and safe access system based on the ”NTRU” cryptosystem [15]. With the help of this approach, the cloud may quickly update the cipher text whenever the owner of the data specifies a newer policy. The owner of the data can also verifies update to prevent fraudulent cloud activity [15]. Proposed system makes use of The NTRU cryptosystem presented by authors.

A new brand lattice-based cryptography structure was presented by Oded Regev [16].

Yashaswi, Farah, and Weiyi in their study published in Cloud Computing [17] contain a cost effective distribution of data, the “secured cost-effective multi-cloud storage model”. Our suggested solution would use a multi-cloud server to host data and deliver various services. A safe framework to manage massive smart grid data is based on cloud computing was presented by J. Baek, Q. H. Vu, et.al. [8] Along with providing different computer services for big data analysis and information management.

Data owners can dynamically adjust data access policies after the passphrase is generated. According to a proposal made by Wei Yuan for cipher text policy attribute-based encryption [22]. The encrypted data at the multi-cloud server will be updated using dynamic policy updates as part of our suggested strategy in response to changing access policies.

M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, et al. suggested cloud security: From one to multi-clouds [24]. The federated Multi-Cloud PaaS infrastructure proposed by Fawaz Parsio, Nicholas Haderer, and others provides a federated PaaS with a flexible architecture, an open service model for developing Multi-Cloud PaaS and SaaS programs running on it, and multi-cloud PaaS and SaaS applications [32].

AES (Advanced Encryption Standard), which introduces the symmetric cryptographic algorithm AES, was proposed by Vishal R. Pancholi and Dr. Bhadresh P. Patel to improve cloud security through secure storage. Its foundation includes a number of substitutions, permutations, and transformations [21].

Cloud computing-an overview, which N. V. Muthulakshmi suggested, provides an overview of cloud computing, demonstrates how it developed from the most widely used technologies, and tackles its deployment, service model, and problem issues [20]. Jialu Hao et al. [25] have created an EACAS with an authorized search that is well organized for controlling cloud storage. Contains the delegation mechanism required by AKP-ABE. You access that loophole using a private key issued by your cloud provider. EACAS enables data users to access valuable research and fine-tune their search strategies by focusing on their data access. However, the restriction involves further modifying the suggested approach with flexible in-formation exchanges and limited data keeping in the cloud.

The “Ethereum Blockchain” design has been used to create a modern secure cloud storage environment that includes this part, a hybrid of CPABE and authentication. Due to the decentralized nature of cloud computing systems, there are no trusted third parties. It possesses three characteristics: it was created using “Ethereum-blockchain” technology; the repository may determine the permitted use time of information. It can be stored on the "Block chain".

Xu, Q. et al. [27] said in 2018: PMDAC-ABSC is a privacy-preserving shared data management method based on the ABSC cipher text, providing a fine-grained control mechanism and privacy attribute protection while in a multi-privilege cloud storage system [19]. By sending additional bilinear pairs to the cloud server, the user's decryption overhead is significantly reduced without compromising the confidentiality of the signature. Anonymity, unforgeability, secret authentication, and public verifiability are all possible with the robust standard model.

The execution findings and asymptotic complexity comparison of the protection strategy indicate that their design would be in line with realistic computing efficiency protection goals.

A fair information access control system and a logical secret-sharing incentive exchange mechanism were implemented by Liu, H., and et al. in 2017 [28].

This scheme generates a large number of false keys. In order to swap shares outside of the prescribed plan, the customer must first transmit their shares. As a result, users are encouraged community usage of the shared data and are dissuaded from becoming egotistical. The recommended scheme’s Nash equilibrium, according to mathematical study, is that both users continue to donate their portions, allowing them to fairly rebuild the decoding key.

Furthermore, depth analysis demonstrates that the concept would effectively manage access control measures. They provide a modified version of the H-KCABE encryption method for the HABE model in order to boost performance during the re-encryption procedure.

The KCABE approach increases efficiency by cutting down on data transmission time in a fine- grained authentication method, whereas the HABE model aids users in gaining hierarchical access to information by creating traffic.

They may quickly increase productivity by employing the KCABE algorithm and the HABE paradigm, which enable them to access information in a hierarchical fashion without creating any user traffic.

Zhihua, Liangao, and Dandan (2016) [30] used a novel strategy to tackle the fundamental encryption problem while also enabling speedy user-voiding retraction. The attribute authority and authorization controllers first add an access regulator to the present strategy, which causes encrypted data to be created on a corporate level. Second, a simple revocation mechanism is provided by keys providing direct or reversible security.

According to the evaluation, the suggested solution is straightforward and trustworthy in terms of user authorization and revocation. However, a lack of precision in cloud storage encryption Lattice-based encryption technique is part of the tiered approach to securing client information proposed by Saravanan, N., and Umamakeswari, D. A.[31].It has been demonstrated that cloud data may be more securely safeguarded by integrating a twofold authentication architecture for access management This effective security measure allows users to store huge amounts of personal data in the cloud without worrying about security risks.

Operators cannot guess keys or decrypted content thanks to RSA and AES algorithms.

In the table 3.1, the RSA and NTRU algorithms are compared, based on their basis of security, strengths, weaknesses, key size, and computational efficiency.

As we can see, RSA is widely supported and has a longer track record, but requires larger key sizes and is computationally intensive. NTRU requires smaller key sizes and is faster for encryption and decryption, but is less widely supported and its security is based on an active area of research. Ultimately, the choice between RSA and NTRU depends on the specific use case and the level of security required.

Table 3.1
Comparison between NTRU and RSA algorithms

Algorithm , Security Basis	Strengths	Weaknesses	Key Size	Computational Efficiency
RSA , Factoring	Widely supported, mathematically proven security, longer track record and robust mathematical foundation	Requires larger key sizes, computationally intensive, vulnerable to attacks using quantum computers	private key (2048-bit), public key (2048-bit)	Slower for encryption and decryption
NTRU, Lattice problems	For quicker encryption requires smaller key sizes than RSA to achieve the same degree of security and decryption, resistant to attacks using quantum computers	Less widely supported, security based on an active area of research	private key (256-bit), public key (507-bit)	Faster for encryption and decryption

IV. PROPOSED WORK

A. Scope

There will be security issues during data storage and access when the data owner outsources to many cloud servers. How to authenticate user's access the data outsourced from multi- cloud is another difficult problem. User eligibility verification is not supported by existing schemes. The system we propose provides a solution to this problem by providing a new verification method, allowing data owners to dynamically change data access rules, and the corresponding external passphrase in the cloud server for efficient access to huge cloud resources should be updated accordingly. The issue with the current arrangement is that the user cannot trust the transformation carried out by a server they do not trust. The suggested solution includes a checksum to confirm the accuracy of the transformation to get around this issue. The suggested system methodology may be independently verified. The suggested approach aims to shorten the user side of the decryption process. Accordingly, the suggested approach enables a transformation to be applied to the encrypted text. The cipher text's size is decreased throughout the procedure. Even after the transformation, the file still appears as cipher text and is not in a completely decrypted state. The user can then use the private key to decrypt the files. Here, the verification issue was solved. For each file, we offer a checksum value. The user always gets the matching checksum when they get a file. The user then generates a checksum for the downloaded file and verifies whether they are identical or not. If both are identical, the transformation is accurate; otherwise, it is incorrect.

Merits:

1) The suggested approach allows the user to see how a cloud server has changed.
2) The suggested system can be verified yet its security is not jeopardized.
3) It is a novel method of outsourcing encryption that enables user verification.
4) It ensures that the opponent will be unable to decipher the encrypted cipher text in any way.

B. A work need

Multi-cloud environments are becoming increasingly popular among organizations seeking to reduce vendor lock-in, increase flexibility, and take advantage of the unique features of different cloud providers. However, multi-cloud environments pose significant security challenges, particularly when it comes to access control. In a multi-cloud environment, resources and data are spread across multiple cloud providers, making it difficult to ensure consistent access control policies and enforce them across the entire environment. Attribute-based access control (ABAC) has emerged as a promising solution to these challenges, but more work is needed to adapt ABAC to the unique requirements of multi-cloud environments.

Maintaining effective access control for big data in the cloud requires new validation methods to ensure that data owners can dynamically update data access policies and that cloud servers can successfully update their external cryptograms. These methods allow users to verify data owners and other authorized users access to data and the accuracy of data provided by each. When data owners transfer data to multi-cloud servers, a new approach to security issues is required.

C. Objectives

Our proposed system has the following objectives

1) To analyze the different ABAC models and techniques used in multi-cloud environments and compare their strengths and weaknesses.
2) To investigate the performance and scalability of ABAC in multi-cloud environments and propose methods to optimize it.
3) To evaluate the effectiveness of ABAC in protecting sensitive data and resources in multi-cloud environments and compare it with other access control models.
4) To offer an effective, scalable, and interoperable framework for executing ABAC in multi-cloud scenarios.
5) To prevent eavesdropping attacks on massive data storage during data upload, download, updating, and retry.
6) To design a secured data access control scheme.

V. PROPOSED METHOD

A. *System architecture*

As depicted in the figure.1 (the suggested system's system architecture), our system functions as follows:
Step 1: Owners signing up for several clouds Owner will sign up for credentials in the cloud by themselves.
Step 2: The owner receives the notification of registration success in response to successful registration.
Step 3: Registering Users with Multi-Clouds Before accessing data in Multi-Clouds, users must submit a registration request to the Multi-Cloud servers.
Step 4: The owner sends his/her data to the multi-cloud server, encrypts it, and stores it after successfully registering in the cloud.
Step 5: After successfully registering, User U sends the owner of the data a request for accessing the data with a token (which contains a fragment of the message certificate) via the multi-cloud server to receive the message certificate for the data.
Step 6: The data owner generates a subkey and a secret number for each user who makes a successful request for data access to the multi-cloud server after successfully registering.
Step 7: After receiving a request, with the user's secret number, the data owner encrypts the message certificate before sending it to the user. The user decrypts the message certificate before obtaining the cipher text from the data owner. It then computes the exchange certificate using its sub-key and sends it to numerous users (registered users).
Step 8: Verifying certificates following receipt of the exchange certificate, all users began to authenticate one another using the various message certificates they each possessed. If User U has all of the remaining components of the message certificate, only then is User U a legitimate user.
Step 9: data from the multi-cloud server download User U recovers the data from the multi-cloud server after receiving consent from several legitimate users. User U must be able to verify the identity of all users who possess bits of that message certificate to access data, and User U must be able to authenticate these users to use their sub-keys for data reconstruction.

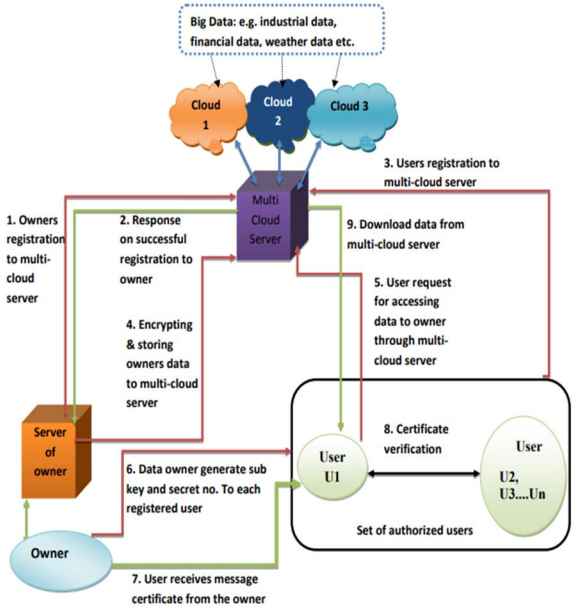


Figure5.1: System Architecture

1) Owners registration

Data owners sign up for multi-cloud server accounts. Data owner has message collection S for cloud storage. The data owner initializes the system to generate public key h and private key f using the upgraded NTRU cryptosystem. The steps below are part of it.

Algorithm 1: Initialization.

a) Selects N, p, and q as the three integer values, with q > p and gcd(p, q) = 1.

b) . Selects four sets of degree -1 polynomials in R with integer values, Lf, Lg, L, Lm;

c) Generate a key pair (f, h) where f is the private key and h is the corresponding public key according to the NTRU strong cryptography system;

d) chooses two one-way hash functions, H1 and H;

e) Publicizes p, q, and h as well as the L and Lm selection parameters.

2) Construction

The data owner creates a subkey for each authenticated user at B, a certificate for each communication at S, and stores the encrypted data on a cloud server.

a) Generating subkeys

b) To generate the following polynomial b(x) of degree t-1, the data owner randomly generates t distinct integers b0, b1, • • •, and bt-1. Where bj ∈ Z[X] /(XN-1) if j = 0, 1, • • • and t -1.

3) User's request for accessing data

Upon successful registration, user requests data from the data owner through a multi-cloud server, and the data owner responds by sending each authorized user a sub-key..

If user Ui wants to access a message or data Sj, It needs to download message certificate for Sj. This procedure consist of following stages

a) Ui asks the data provider for Sj's message certificate by sending a request to them.

b) In response to this request, the data owner encrypts the data using AES and Ui's private code, ri (Advanced Encryption Standard).

c) Ui first decrypts Cdj after receiving it from the data owner in order to acquire dj.

d) The exchange certificate Wij is then computed using its sub-key xi, and Wij is sent to other customers in B.

4) User's Verification& Message reconstruction

a) When multiple users (Uα) of Certificate Validation B receive a Wij, they use the public ej to validate the Wij. If true, Ui is seen by multiple users in B, which means that from the point of view of all users (multiple users in B), Ui is a valid consumer of the message Sj.

b) Message Reconstruction When user Ui obtains permission from several legitimate users in B, here constructs message Sj. The access policy process is shown in the following flow.

5) Performance Analysis of the system in multi-cloud server

It will analyze security of proposed system in multi-cloud server environment.

B. Ntru algorithm

No operators or distinct logarithmic problems are used in the NTRU cryptography system [9].

To reduce the number of potential polynomials, the NTRU cryptosystem truncates a polynomial ring with coefficients in a finite field to a lesser degree. Then, for encryption and decryption, Public and private keys are generated using truncated polynomial rings [15].

VI. RESULT AND ANALYSIS

This section looks into ABAC access control for cloud storage. Using Visual Studio 2010, the suggested technique is utilized with the.net programming language. This idea is most frequently utilized in relation to the healthcare system. The data sets used in the experiment come from many sources.

A. Comparative Analysis

A method is examined using a number of metrics, including encryption time as well as time utilization, and the decryption time. The traditional techniques, NTRU and CP-ABE, are contrasted with a contemporary strategy. The proposed approach and the present approach are contrasted below

1) Encryption time for ABAC, NTRU and ECC cryptosystem

Table 6.1
Encryption time for ABAC, NTRU and ECC cryptosystem

Key Size	Encryption time (in ms)		
	ABAC	NTRU	ECC
128	0.630669	0.935	1147
256	4.387736	6.254	1265
512	10.607305	15.265	1765

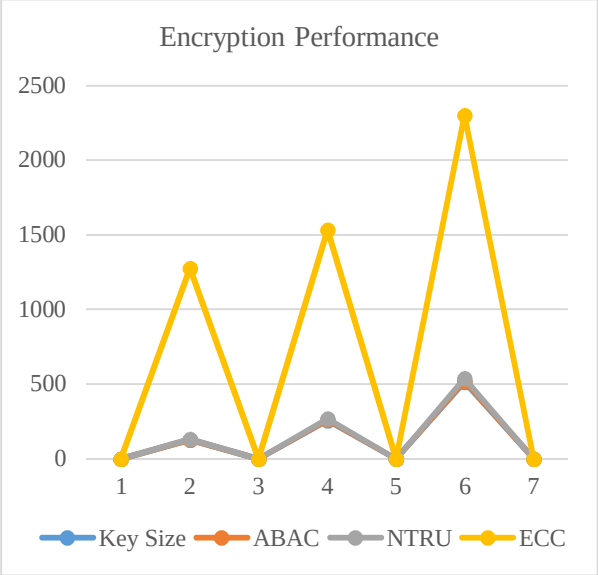


Figure 6.1: ABAC, NTRU and ECC Encryption performance

Table 6.1 and Figur6.1 shows Encryption time for NTRU and ECC cryptosystem for key size of 128,256,512 bits.

2) Decryption timing for ABAC, NTRU and ECC cryptosystem:

Table 6.2
Comparison of ABAC, NTRU and ECC

Key Size	Decryption time (in ms)		
	ABAC	NTRU	ECC
128	0.608637	2.4	15
256	1.153115	2.6	29
512	25.458823	26.88	47

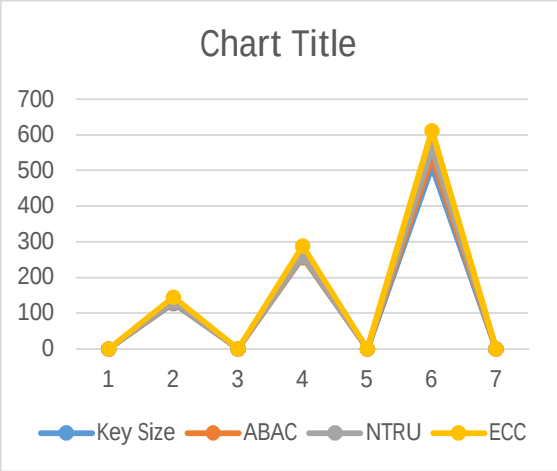


Figure 6.2: ABAC, NTRU and ECC decryption performance

Table 6.2 and Figure 6.2 shows Decryption timing for NTRU, ABAC and ECC Cryptosystem for key size of 128,256,512 bits.

Table 6.3
Comparison between ABAC, RSA, ECC, NTRU

Criteria	ABAC	RSA	ECC	NTRU
Security Strength	High	High	High	High
Key Size	Short	Long	Short	Short
Performa-nce	Fast	Slow	Fast	Fast
Scalability	Fine	Weak	Fine	Fine
Interoper-ability	Fine	Fine	Poor	Fine
Implemen-tation	Complex	Compl-ex	Simple	Complex

Security Strength: All four methods are highly secure, but the level of security varies based on the algorithm's strength, key size, and implementation.
Key Size: ABC uses short keys compared to RSA and ECC, while NTRU also uses short keys, making it a good choice for resource-limited environments.
Performance: ABAC and ECC are faster than RSA due to their simpler algorithms, making them better suited for real-time applications. NTRU is also fast but requires a larger number of computations.
Scalability: ABAC and ECC are highly scalable, making them ideal for large-scale applications. RSA is less scalable due to its complex algorithms and long key sizes.
Interoperability: ABAC and NTRU are highly interoperable, while RSA and ECC are not. RSA and ECC use different key sizes and algorithms, which makes it challenging to integrate them with other systems.
Implementation: ABAC and NTRU are complex to implement, requiring specialized expertise. RSA and ECC are also complex, but their simpler algorithms make them more accessible to implement.
In summary, ABAC and NTRU are highly secure and fast, making them ideal for real-time applications. ABAC is highly scalable and interoperable, while NTRU is highly efficient but requires specialized expertise to implement. RSA and ECC are less scalable and interoperable but are widely used and accessible to implement.

VII. CONCLUSION

Cloud computing adoption has has created new security challenges, particularly in the area of access control. Attribute-based access control (ABAC) has emerged as a potential approach for enforcing fine-grained access control rules in multi-cloud systems. In this paper, we reviewed the basic architecture of ABAC and examined its key features, such as attribute-based policies, dynamic authorization, and scalability.

We also compared ABAC with other popular encryption algorithms such as RSA, ECC, and NTRU and highlighted their strengths and weaknesses. Based on our analysis, we found that ABAC is highly scalable, interoperable, and efficient, making it an ideal solution for enforcing access control policies across different cloud providers. However, the implementation of ABAC is complex and requires specialized expertise.

Our research identified several key areas where more work is needed to improve the effectiveness and efficiency of ABAC in multi-cloud environments. These include standardizing ABAC models and techniques, addressing interoperability issues, optimizing performance and scalability, and enhancing the legal and regulatory compliance of ABAC. Moreover, future research should explore the impact of ABAC on the overall security posture of multi-cloud environments and develop guidelines and best practices for deploying ABAC in different cloud computing scenarios.

In conclusion, Attribute-based access control can enhance the security of multi-cloud environments by providing fine-grained access control policies that can dynamically adapt to changing security requirements. However, more research is needed to address the challenges and opportunities of deploying ABAC in multi-cloud environments and to enhance its effectiveness and efficiency in protecting sensitive data and resources.

VIII. COMPLIANCE WITH ETHICAL STANDARDS

This research was not funded by any external sources. The authors declare no conflicts of interest related to this study and maintain full responsibility for the integrity and accuracy of the data presented.

IX. ETHICAL APPROVAL

This Article does not contain any studies with human participants or animals performed by any of the authors.

REFERENCES

[1] K. S. Saraswathy ,S. S. Sujatha ”Using Attribute-Based Access Control, Efficient Data access in the Cloud with Authorized Search ” International Journal of Electrical and Computer Engineering System, Volume 13, Number 6, 2022

[2] Emiliano Cristofaro, Yanbin Lu, Gene Tsudik,”Efficient Techniques for Privacy Preserving Sharing of Sensitive Information Trust and Trustworthy Computing”, 2011, Volume 6740 ISBN: 978-3-642-21598-8.

[3] J. Li, W. Yao, Y. Zhang, H. Qian, J. Han, Flexible and Fine-Grained Attribute-Base data Storage in Cloud Computing, IEEE Transactions on Services Computing, Vol. 10, No.5, 2017, pp. 785796.

[4] J. Shi, J. Lai, Y. Li, R. H. Deng, J. Weng, Authorized Keyword Search on Encrypted data, Proceedings of the European Symposium on Research in Computer Security, Wroclaw, Poland, 7-11 September 2014, pp. 419435.

[5] P. Jiang, Y. Mu, F. Guo, Q.Wen, Public Key Encryption with Authorized Keyword Search,Proceedings of the Australasian Conference on Information Security and Privacy, 2016, pp.170186.

[6] H. Cui, Z.Wan, R. H. Deng, G.Wang, Y. Li, Efficient and Expressive Keyword Search Over Encrypted Data in The Cloud, IEEE Transactions on Dependable and Secure Computing, Vol.15, No. 3, 2016, pp. 409422.

[7] H. Cheng, C. Rong, K. Hwang, W. Wang, Y. Li, Secure Big Data Storage and Sharing Scheme For Cloud Tenants, China Communications, Vol. 12, No. 6, 2015, pp. 106115.

[8] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, Y. Xiang, A Secure Cloud Computing-Based Framework for Big Data Information Management of Smart Grid, IEEE Transactions on cloud Computing, Vol. 3, No. 2, 2015, pp.233244.

[9] G. Zhuo, Q. Jia, L. Guo, M. Li, P. Li, Privacy-Preserving Verifiable Set Operation in Big Data for CloudAssisted Mobile Crowdsourcing, IEEE Internet of Things Journal, Vol. 4, No. 2, 2016, pp. 572582

[10] L. Guo, Y. Fang, M. Li, P. Li, Verifiable Privacy-Preserving Monitoring for Cloud-Assisted M-health Systems, Proceedings of the IEEE Conference on Computer Communications, 26 April - 1 May 2015, pp. 10261034.

[11] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, J.-L. Huang, Cloud Based Fine Grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing ADCET,Asta,Sangli Page 47 Chapter 7. Conclusion and Future Work and Attribute Revocation, IEEE Transactions on Cloud Computing, Vol. 6, No. 2, 2018, pp.532544.

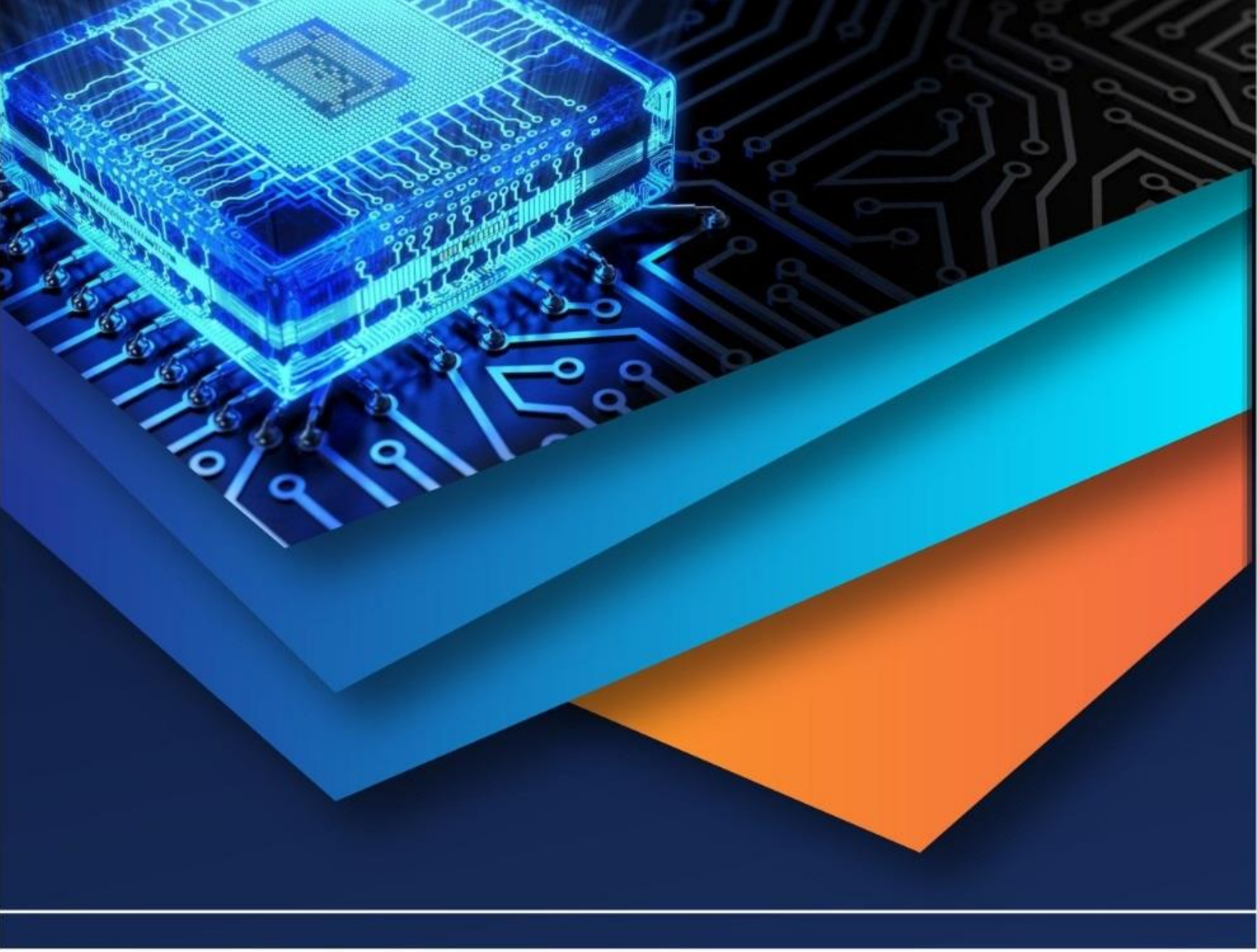
[12] Z. Yan, X. Li, M. Wang, A. V. Vasilakos, Flexible Data Access Control Based On Trust And Reputation In Cloud Computing, IEEE Transactions On Cloud Computing, Vol. 5, No.3, 2017, pp. 485498.

[13] K. Yang, K. Zhang, X. Jia, M. A. Hasan, X. Shen, Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms, Information Sciences, Vol. 387, 2017, pp. 116131.

[14] "Secure File Sharing Mechanism and Key Management for Mobile Cloud Computing Environment". Indian Journal of Science and Technology 9(48), January 2017.
[15] Chunqiang Hu, We Li, metal A secure and verifiable access control scheme for big data storage in clouds, IEEE Transactions on Big Data, 2016
[16] OdedRegev,New lattice based cryptographic constructions, Journal of the ACM 51(6), pp. 899-942, 2004. Preliminary version in Proc. of STOC 2003.
[17] Yashaswi Singh, FarahKandah, Weiyi Zhang, A Secured Cost-effective Multi-Cloud Sto- rage inCloud Computing, Department of Computer Science, 2011.
[18] Mohammed A. Alzain, Eric Pardede, metal, Cloud computing security from single to multi-clouds, 2012.
[19] M. A. Beyer and D. Laney, The importance of big data: a definition, Stamford, CT:Gartner, 2012
[20] N.V. MUTHU LAKSHMI, Cloud Computing-An OverviewPublications of Problems Application In EngineeringResearch - Paper, Special Issue01; 2013, ISSN: 2230-8547; e-ISSN: 2230-8555, 2012, Pages 324-330
[21] Vishal R. Pancholi,Dr.Bhadresh P. Patel, Enhancement of Cloud Computing Security with Secure Data Storage using AES , JIRST International Journal for Innovative Research in Science Technology, Vol 2 ,February 2016.
[22] Wei Yuan, Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption, Parallel and Distributed Systems, 2016
[23] S. Salinas, X. Chen, J. Ji, and P. Li, A tutorial on secure outsourcing of large-scale computations for big data, IEEE Access vol. 4, 2016.
[24] M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, "Cloud Computing Security: Single to Multi-clouds," 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 2012, pp. 5490-5499, doi: 10.1109/HICSS.2012.153.
[25] J. Hao, J. Liu, H. Wang, L. Liu, M. Xian, X. Shen, Efficient Attribute-Based Access Control with Authorized Search in Cloud Storage, IEEE Access, Vol. 7, 2019, pp.182772182783.
[26] S. Wang, X. Wang, Y. Zhang, A Secure Cloud Storage Framework with Access Control based on Blockchain, IEEE Access, Vol. 7, 2019, pp. 112713 112725.
[27] Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, F. Cheng, Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption, IEEE Access, Vol. 6, 2018, pp. 3405134074.
[28] H. Liu, X. Li, M. Xu, R. Mo, J. Ma, A Fair Data Access Control Towards Rational Users In Cloud Storage, Information Sciences, Vol. 418, 2017, pp. 258271.
[29] M. Sangeetha, P. Vijayakarthik, S. Dhanasekaran, B. S. Murugan, Fine Grained Access Control Using HKCABE in Cloud Storage, Materials Today: Proceedings, Vol. 37, 2021, pp. 27352737
[30] Z. Xia, L. Zhang, D. Liu, Attribute-based Access Control Scheme With Efficient Revocation In Cloud Computing, China Communications, Vol. 13, No. 7, 2016, pp.9299.
[31] N. Saravanan, D. A. Umamakeswari, Lattice Based Access Control for Protecting User Data in Cloud Environments with Hybrid Security, Computers Security, Vol. 100, 2021, p.102074.
[32] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy and L. Seinturier, "A Federated Multi-cloud PaaS Infrastructure," 2012 IEEE Fifth International Conference on Cloud Computing, Honolulu, HI, USA, 2012, pp. 392-399, doi: 10.1109/CLOUD.2012.79.

Referred Websites

https://www.cloudsecurity.com
It includes what is mean by cloud security, mechanisms for cloud security.
https://en.m.wikipedia.org/wiki/multi-cloud
It includes what is multi-cloud services provided by multi-cloud



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)