Framework For Data-Centric Multi-Authority Attribute-Based Encryption in a Secure Cloud Data Environment

Surbhi Joshi[1] Indore, India, Dr. Gurveen Vaseer[2,] Indore, India
Department of Computer Science, Oriental University, Indore[1,2]
Email-ID: Joshisurbhi789@gmail.com[1], gurveenv@yahoo.com[2]

Abstract- This study introduces a safe and effective method for protecting data stored in the cloud. It utilizes a Data-Centric Multi-Authority Attribute-Based Encryption (DC-MAABE) architecture, incorporating RSA encryption and one-time password authentication. The proposed solution improves system performance while limiting access to sensitive data to authorized individuals. By analyzing the system's authentication process, which includes success rates and response time, the framework can optimize response time with repeated use and attain near-perfect authentication dependability. For safe cloud settings, this strikes a good compromise between security and usability.

Keyword Used- *Data-Centric Multi-Authority Attribute-Based Encryption (DC-MAABE), RSA Encryption, OTP Authentication, Cloud Data Security and Response Time Optimization.*

1. Introduction

Cloud computing provides scalability, flexibility, resources, storage, databases, communication, software, analytics, intelligence, and speedier invention by transmitting computer services over the internet (called "the cloud"). Cloud technology has proven essential to modern web interactions by lowering user engagement and latency. Their cloud services simplify infrastructure management, save operational expenses, and let them grow with your organization. The strongest IT application platform is cloud computing [1]. Its appealing features" such as Infrastructure as a Service (IAAS), Software as a Service (SAAS), and Platform as a Service (PAAS)"drive its rapid adoption. The platform is more dynamic, scalable, and resilient. This platform delivers on-demand processing and storage, making it perfect for resource-constrained applications. These qualities make the platform dynamic, scalable, and resilient. Since it offers on-demand computing and storage, this platform is perfect for resource-constrained applications. This research uses Multi Authority Attribute-Based Encryption to secure cloud storage in response to these vulnerabilities. By allowing access control policies to be established by attributes rather than user IDs, MAABE improves data confidentiality between users and cloud service providers. The cloud deployment model determines the cloud environment based on ownership, size, access, features, and purpose. Your cloud deployment model determines your servers' locations and administrators. It describes your cloud architecture, what they can change, and whether they can buy services or create anything from scratch. Your users and infrastructure are also connected by cloud deployment types [2]. Many cloud computing deployment strategies are listed below. Three clouds exist: public, private, and hybrid.

A public cloud, such as Google Workspaces, is a cloud computing architecture in which third-party providers control and run the infrastructure and services, providing access to individuals and enterprises worldwide, frequently with pay-per-use pricing. Usually administered by the company's IT staff in a secure setting, a private cloud is an internal cloud system utilized by a single organization that offers more control and protection. By managing some workloads in a private cloud and utilizing public cloud resources for others, a hybrid cloud mixes public and private clouds, enabling enterprises to make use of both features, including improved security and cost-effectiveness.

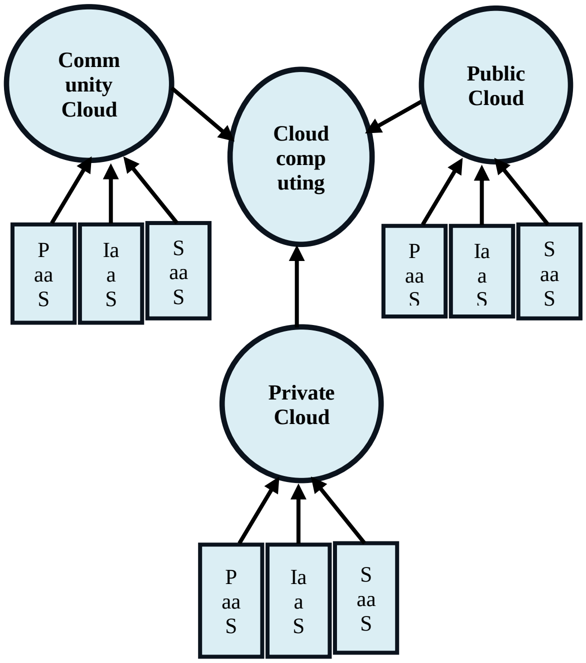

Figure 1: Cloud Computing Deployment Models

1.1 Significance of Multi-Authority Attribute-Based Encryption

MA-ABE was developed to address the challenges associated with a single centralized authority in traditional ABE schemes. In ABE, encryption and decryption are based on attributes, but a single central authority in charge of managing all attributes may lead to scalability and trust issues.

1.2 Multi-Authority Attribute-Based Encryption Work

MA-ABE is an advanced encryption scheme where several attribute authorities govern various user attribute subsets. Data is encrypted using a policy connected to user traits like employment or organization, comparable to Attribute-Based Encryption (ABE). By combining contributions from several authorities based on their qualities, MA-ABE decrypts using a composite key. This architecture improves scalability, fault tolerance, and privacy over traditional ABE because no authority has full visibility into all user attributes.

Data-centric security focuses on data location, collecting, storage, and visibility. Data-centric security protects data throughout its lifecycle, unlike traditional solutions that protect servers, networks, and apps. Since they were not designed for expansion, traditional procedures may pose considerable risks. Data-centric security may protect data in dynamic cloud environments regardless of who shares it or how it is accessed. Data-centric security includes identification, comprehension, control, protection, and auditing. These characteristics help an organization preserve its most essential data, prevent data loss, and analyze data for malicious intent.

1.4 The role of the DC-MAABE framework includes the following main components

- **Data Owner (DO):** The entity that creates and outsources data to the cloud. The DO establishes data access regulations based on user characteristics.
- **Cloud Service Provider (CSP):** Stores encrypted data and implements access control restrictions set.
- **Users:** Entities that seek access to data stored in the cloud. Access is provided depending on their qualities.
- **Attribute Authorities (AAs):** Multiple semi-trusted authorities in charge of providing attribute keys to users. Each AA controls a unique collection of properties.

1.5 Data Encryption and Decryption of Data

An example of a Boolean expression over user attributes that the Data Owner (DO) can use to construct an access policy in this system is "((Role: Doctor AND Department: Cardiology) OR (Role:

1.3 Role of Data-Centric Security in Cloud Environments

Nurse AND Department: ICU))". We encrypt the data with symmetric encryption, and then we encrypt the symmetric key with Attribute-Based Encryption (ABE) and the access policy. With both the data and the encrypted symmetric key stored by the CSP, the data is secure. The CSP grants the user access and data when they ask for it. After that, the user's gadget will try to decode the symmetric key by utilizing its attribute keys. The decryption of the symmetric key and subsequent data access is granted if the user's qualities match the policy[3].

2. Review of Literature

Chandra Ajay (2024) [4]examined the many techniques and substantial hurdles to privacy-preserving cloud computing information sharing. By exploring advanced cryptography, anonymization, and accessibility control paradigms, the diversified arsenal protects sensitive data and facilitates user contact and collaboration. This session provided a detailed roadmap for negotiating the complex Internet of Things context of sensitive data sharing.

Suneetha, et al. (2024) [5] created a secure cloud environment for consumers and service providers to process and transmit data safely. Security concerns prevent some businesses, such as business, banking, the military, and healthcare, from using cloud storage. This research addresses these difficulties and attracts more users by providing secure cloud solutions. The Scalable and Expanded Key Aggregate System of cryptography (SEKAC) improves healthcare data security with double encryption. This strategy secures medical data storage and retrieval better than previous methods. The second solution uses the Improved

Diffie-Hellman Key Exchange Algorithm to secure cloud server-to-user data. This method improves security by generating secure keys.

Kathleen Atul B et al.(2024) [6]suggested gathering medical data and encrypting it using ABE using the best key generated by the Hybridised Mexican Axolotl and Energy Valley Optimiser (HMO-EVO). This continues until all medical data is encrypted. Securely storing encrypted data on a permission block chain ensures access control and data breach prevention. The system predicts diseases using federated learning, multiple scales Bi-Long Short-Term Memory, and gates recurrent units (MBiLSTM-GRU). This streamlines healthcare monitoring. This federated solution allows decentralized deep learning model training, preserving patient data while using collective learning. Scientific studies show that the suggested technology outperforms standard methods in safety, efficiency, and predicted accuracy.

Zhang, Leyou, et al. (2023) [7] addressed this by proposing attribute-driven encryption (ABE) on a smart grid that is based on an accountable multi-authority access control framework. Along with supporting securely fine-grained control over access to real-time data sharing, the suggested scheme also fixes the smart grid's single-point failure problem. Lastly, the proposal outperforms the current one in terms of efficiency and security, according to theoretical examinations and performance evaluations.

Irshad, and Reyazur Rashid (2023) [8]The Internet of Things with cryptography created a secure and scalable cloud computing architecture. Multicast clever Broadcasting keying Algorithm safeguards user data. A combined MBRA, PQC, and blockchain cryptography system does this. The solution secures distributed sensor data via Internet of Things devices using powerful MBRA-PQC encryption. Blockchain distributed ledger immutability protects data privacy. We tested the approach on numerous datasets and found it efficient. The metrics are reliability, capacity, security, throughput, and response time. The suggested SSCA outperforms MHE-IS-CPMT. The response time fell 1.67 seconds for 250 devices and 0.97 seconds for 1000. AUC figures improved significantly for the SSCA, surpassing the MHE-IS-CPMT, EAM, SCSS, and SHCEF models at 25 users by 6.30%, 6.90%, 7.60%, and 7.30%, respectively. It rose 5.20%, 9.30%, 11.50%, and 15.40% at 50 users.

SingamaneniKranthi Kumar, et al.(2023) [9]suggested CP-ABE, which used ciphertext rules and multi-qubit quantum key distributions. The quantum key distribution protocol in the multi-qubit QKD model can generate an encrypted public for encrypting and extracting, which might secure cloud data using quantum cryptography. Next, the key is used to encrypt and decode data using CP-ABE. No key exchange is needed for attribute-based knowledge encryption and decryption using this method. The simulation model's positive results show quantum cryptography could be used in cloud data security.

KalaiyarasiR et al.(2023) [10]used "key exchange between Various algorithms to boost security and reduce assaults. This algorithm creates a cloud-based engineering learning model. This model improves user data security. Security goals including confidentiality, data integrity, and individualization are met by the design. Cryptography, which hides sensitive data with regular data, is implemented using the innovative DHP Key technique. This approach combines public key advantages with private key exchange. Users might encrypt confidential text messages with a key or passcode. Even if a hacker gets the encrypted message, they cannot decrypt it without the key. This approach securely transmits secret messages, preventing outside intervention. To ensure only the intended receiver may decrypt publicly published ciphertext, it is rendered incomprehensible to unauthorized users.

Dhanalakshmi, G. and G. Victo Sudha George (2023) [11] used hybrid cryptography to improve data security and privacy by combining symmetrical and asymmetric key techniques. The system incorporates modern data integrity methods like hash functions and checksums to assure data reliability, integrity, and lack of repudiation. The suggested system uses various dependable security features to prevent unauthorized entry and data leakage. These include advanced encryption, role-based accessibility control, hashing validation, audit trails, and administrator access to information. Cloud architecture enables scalable and cheap healthcare storage solutions. The proposed solution outperformed alternatives in privacy, security, and efficiency, according to experiments. It could improve healthcare by protecting patients' privacy and confidentiality.

Paul, N. R., and D. Paul Raj et al.(2021)[12]developed a model for trust-based access control in a multi-cloud environment that takes into account server and user characteristics. Data encryption using the Cyclic Shift Transposition, also known Algorithm and a trust-based authentication method makes up the proposed methodology. Cloud users are given trust values according to their direct trust degrees in this framework for a trust-based access control mechanism. As a result of every user's access control policy is adjusted according to their trust level. Another appropriate server will be chosen if the current one does not satisfy the minimal trust level. When tested in a multi-cloud setting, the suggested system proved to be superior to competing solutions".

Aarthi, A.and R. Pradeep (2020) [13] combined Distributed Publisher program-driven IC IoT with Cipher Content Policy Attribute-Based Encryption. We have also proposed a Time centered Publisher Driven Algorithm to ensure that only authorized users can access pristine data. Only registered users will have access to the data stored in the cloud server, thanks to the Time-Based Publisher Driven Algorithm's (DSA) introduction of DSA to deal services between users and publishers. Time required for encryption and decryption as measured by performance evaluation

Raj, J. Joshua Daniel, and J. Samson Immanuel et al. (2020) [14] employed to protect various kinds of information, the standard CP-ABE scheme. To generate keys for data encryption and decryption, the CP-ABE consults the access policy, which is presented as an access tree. It takes a long time to process each node of the access structure and encrypt the data when using an explicit accessing structure with multiple nodes, which increases the computational requirements. In this paper, they offered a simplified scheme for multimedia application the ciphertext policy attributes-based cryptography that does not include an access structure. This makes it more practical to secure data with less overhead and overcomes these challenges. In this proposed solution, the data owner meticulously constructs the attribute string according to specific guidelines, which are then utilized in the encryption and decryption procedures. Measurements of the suggested scheme's performance show that our system is very secure while using very little computing power.

S.no	Author name	Techniques	Research gaps	Findings
1.	Chandra Ajay (2024) [4]	Cryptographic methodologies, anonymization strategies, access control.	Lack of practical implementations and evaluations in real-world IoT environments.	Identified trends and challenges in secure information sharing;
2.	Suneetha, et al. (2024) [5]	Scalable and Expanded Key Aggregate Cryptography (SEKAC)	Absence of a comprehensive framework to address scalability and performance in multi-industry cloud adoption.	Improved healthcare data security and transmission efficiency;
3.	Kathleen Atul B et al. (2024) [6]	Hybridised Mexican Axolotl and Energy Valley Optimiser(HMO-EVO),	Limited exploration of healthcare. Federated learning scalability and efficiency in multi-cloud settings unaddressed.	Demonstrated enhanced security, efficiency, and predictive accuracy.
4.	Zhang, Leyou, et al. (2023) [7]	Attribute-Based Encryption (ABE), multi-authority access control.	Insufficient emphasis on interoperability with heterogeneous IoT devices and energy efficiency in smart grid environments.	Improved fine-grained control, accountability, and security in smart grid data sharing.
5.	Irshad and Reyazur Rashid (2023) [8]	Multicast advanced Broadcasting keying Algorithm (MBRA).	Lack of focus on reducing computational overhead for resource-constrained IoT devices.	Achieved higher reliability, capacity, and response times; showed superior performance metrics.

3. Research Gaps:

- There is a lack of integration of Advanced Cryptographic Techniques to improve data security, privacy, and integrity.

- There is a lack of Scalability in Diverse Cloud Environments to handle larger, more complex, and diverse cloud infrastructures to ensure they remain efficient and practical.
- The computational and storage overhead associated with DC-MAABE for better performance in resource-constrained environments.
- There is a lack of exploring the methods to handle and resolve potential conflicts in access control policies across multiple authorities.

These research gaps highlight opportunities to refine the DC-MAABE framework, ensuring it remains robust, scalable, and user-friendly in addressing security challenges in cloud environments.

4. Research objectives

- Design a secure, scalable framework that integrates Multi-Authority Attribute-Based Encryption to decentralize trust and eliminate reliance on single-authority systems.
- To Implement mechanisms to enforce dynamic, attribute-based access control policies that adapt to varying user roles and permissions while ensuring data confidentiality and integrity
- To Ensure the framework could handle large-scale and diverse cloud environments, accommodating increasing numbers of users, attributes, and authorities without performance degradation
- To Create a flexible and adaptable solution that could evolve with advancements in cloud technology, cryptographic methods, and data security requirements.

5. Background study

Computing in the cloud has emerged as an adaptable strategy that could be used to deliver commercial as well as personal services through internet connections with minimal interaction. This solution also improves traditional web interaction and reduces the amount of latency that is experienced when accessing information. Attribute-Based Encryption (ABE), an effective approach for enhancing the security of information between customers and cloud service providers, is the focus of this research, which aims to address these vulnerabilities through the use of ABE. An Information-Centric Multi-Authority Attribute-Based Encrypted (DC-MAABE) approach is going to be proposed to protect cloud data from being accessed by unauthorized individuals. Through the implementation of our strategy, a system for controlling access is combined with a Multiple Authorities scheme. According to the findings of the experiments, the DC-MAABE architecture performs similarly to other approaches during the encryption process phase as well as demonstrates greater time efficiencies during the key extraction phase when compared to the conventional methods. The results of this study highlight the uniqueness and efficiency of our provided design, which provides a solution that is safe, scalable, and efficient for the protection of data in cloud-based environments [15].

6. Problem Formulation

The rapid “adoption of cloud computing has introduced significant challenges in securing sensitive data, particularly in environments where multiple stakeholders with varying levels of trust require access to shared resources. Existing encryption frameworks often rely on single-authority systems, which are prone to bottlenecks, scalability limitations, and single points of failure. Moreover, many current approaches lack robust mechanisms to enforce fine-grained access control policies that adapt to dynamic user attributes while ensuring data integrity and confidentiality. To

Encryption to decentralize trust, enhances scalability, and enables granular access control. Such a framework must also incorporate advanced cryptographic techniques and user-friendly interfaces to ensure usability and adaptability in diverse, secure cloud environments. This research aims to design a scalable and secure framework that overcomes these challenges, providing a robust solution for protecting sensitive data in modern cloud “infrastructures.

7. Research methodology:

Improve the safety of your data stored in the cloud by following these best practices. To better secure data stored in the cloud, it is recommended to familiarize oneself with the shared accountability paradigm, inquire about cloud providers' security measures in detail, utilize management of access and identity solutions, encrypt and mask data, and so on. Implementing monitoring and detection techniques, conducting security assessments regularly, and training employees to be aware of security threats are other recommended practices. Companies could strengthen their security measures by reducing the likelihood of breaches of information and illegal access through the efficient implementation of these practices.

In the first research paper, the focus is primarily on introducing the Data-Centric Multi-Authority Attribute-Based Encryption (DC-MAABE) framework, defining the core problem of single-

address these issues, there is a need for a data-centric framework that integrates Multi-Authority Attribute-Based

authority system limitations, and proposing a novel solution to enhance security, scalability, and fine-grained access control in cloud environments. While the paper outlines the conceptual design, it likely leaves gaps in detailed implementation, comprehensive performance evaluation, and addressing potential challenges such as authority collusion, attribute revocation, or scalability with a large user base. Additionally, practical validation through experimental setups, real-world case studies, and comparisons with existing frameworks remain unexplored. These areas will naturally transition into the second paper, focusing on implementation, optimization, and validation to provide a complete and robust solution.

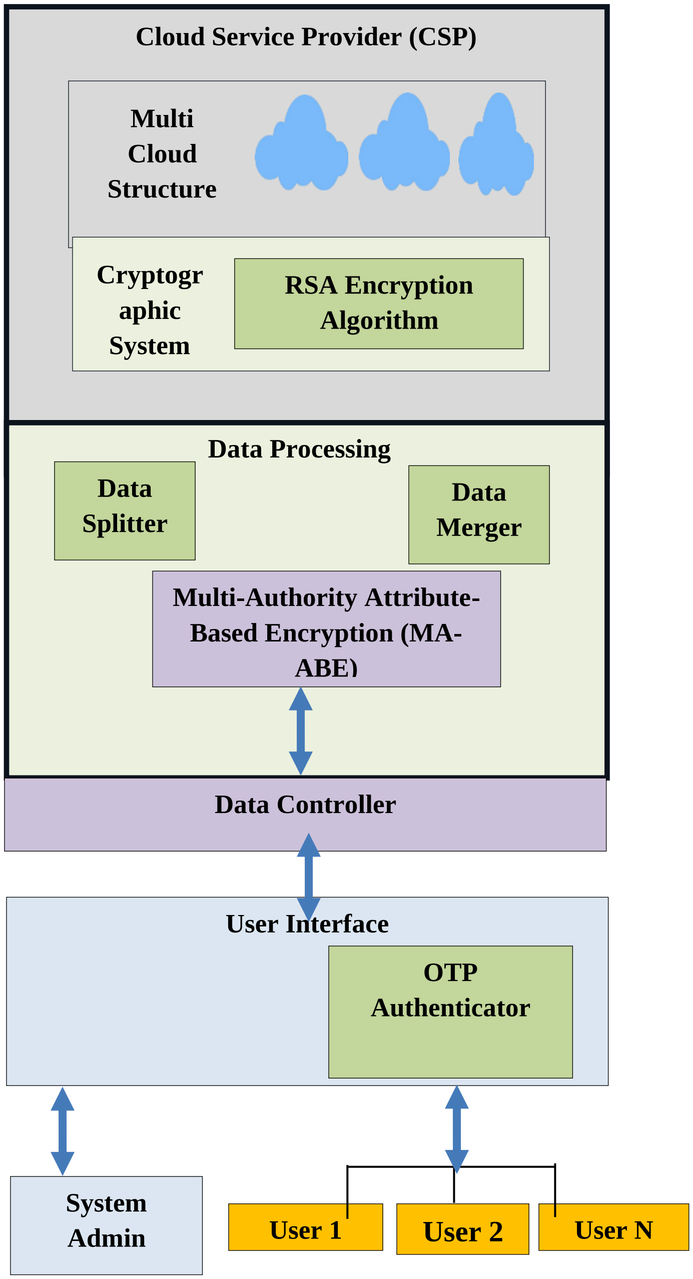

Figure 2: Proposed Methodology diagram

7.1 Research methodology

1. Cloud Service Provider (CSP)

- **Multi-Cloud Structure**: The system utilizes multiple cloud environments to distribute and store data, increasing security and reliability.
- **Cryptographic System**: A layer dedicated to encryption and decryption of data. It employs the **RSA Encryption Algorithm**, a public-key cryptographic method used to secure communication and ensure data confidentiality.

2. **Data Processing**

- **Data Splitter**: Divides the data into smaller parts or fragments before storing them in the cloud. This improves security by making it harder for attackers to access complete data.
- **Data Merger**: Reassembles the split data fragments when needed, ensuring the user retrieves the original data seamlessly.
- **Multi-Authority Attribute-Based Encryption (MA-ABE):** Implements the Advanced Encryption Standard for encrypting the data fragments before storing them in the cloud, adding another layer of security.

3. **Data Controller**

- Acts as an intermediary between the user interface and the data processing layer.
- Manages the flow of data, ensuring secure interactions between users, the data processing system, and the cloud.

User Interface

- **OTP Authenticator**: A security feature that uses One-Time Passwords for authenticating users. It ensures that only authorized user scan access the system.

4. **Users and System Admin**

- **Users** (User 1, User 2, User N): Individuals or entities that interact with the system to store, manage, or retrieve data.

System Admin: Responsible for managing and monitoring the entire system, including user authentication, data security, and cloud operations.

5. Proposed Algorithm and its Complexity

```
1. Initialization:
   - Generate RSA Public Key (K_pub) and Private Key (K_priv)
   - Initialize Multi-Authority Attribute-Based Encryption (MA-ABE)
   - Define attributes for authorized users
2. Data Splitting:
   Input: Data (D)
```

```
  Output: Data Segments (D_1, D_2, ..., D_n)
  FOR each segment D_i in D:
    Split D into n equal parts
  END FOR
3. RSA Encryption:
  Input: Data Segments (D_i), RSA Public Key (K_pub)
  Output: Encrypted Segments
  FOR each segment D_i:
    Encrypted_Segment[i] = RSA_Encrypt(D_i, K_pub)
  END FOR
4. MA-ABE Encryption:
  Input: Encrypted Segments, Attributes (A)
  Output: Ciphertext
  FOR each Encrypted_Segment[i]:
    Ciphertext[i] = MA_ABE_Encrypt(Encrypted_Segment[i], A)
  END FOR
5. Store Data in Cloud:
  Input: Ciphertext, Cloud Servers (CSP)
  FOR each Ciphertext[i]:
    Store Ciphertext[i] in Cloud Server C_j
  END FOR
6. User Authentication:
  Input: User Request
  IF OTP_Authenticate(User) == TRUE:
    Allow access
  ELSE:
    Deny access
  END IF
7. Retrieve Data:
  Input: Cloud Servers
  Output: Encrypted Segments
  FOR each Cloud Server C_j:
    Retrieve Ciphertext[i]
  END FOR
8. MA-ABE Decryption:
  Input: Ciphertext, User Attributes
  Output: Decrypted Segments
  FOR each Ciphertext[i]:
    Decrypted_Segment[i] = MA_ABE_Decrypt(Ciphertext[i], User_Attributes)
  END FOR
9. RSA Decryption:
  Input: Decrypted Segments, RSA Private Key (K_priv)
  Output: Original Data Segments
  FOR each Decrypted_Segment[i]:
    Original_Segment[i] = RSA_Decrypt(Decrypted_Segment[i], K_priv)
  END FOR
10. Data Merging:
  Input: Original Segments
  Output: Original Data (D)
```

```
Original_Data = Merge(Original_Segment[i])

11. Output:

   Provide Original_Data to the authenticated user
```

8. Implementation Layout

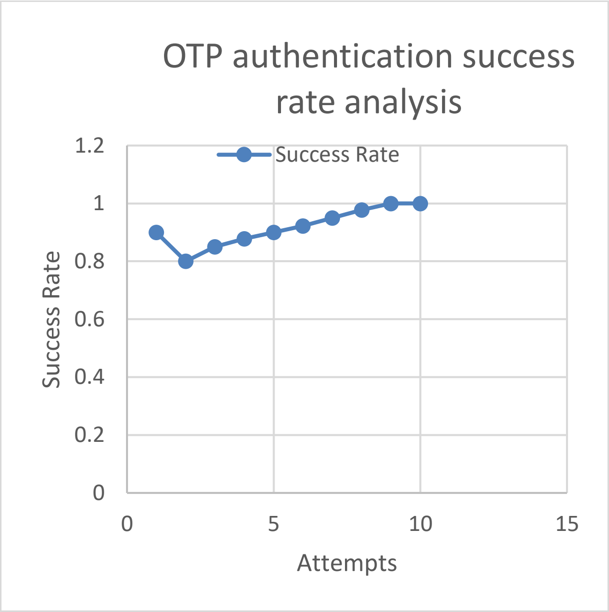

Figure 3: Proposed Success Rate Comparison

Integrating RSA encryption, Data-Centric Multi-Authority Attribute-Based Encryption (DC-MAABE), and one-time password (OTP) authentication, the framework displayed in Figure 3 offers an efficient and safe way to protect data kept in the cloud. Strong encryption is guaranteed during data transfer via RSA, and data security is enhanced by the DC-MAABE mechanism, which limits access to authorised individuals based on predetermined criteria. An additional safeguard is the use of one-time passwords (OTPs) for real-time authentication of system administrators. Figure depicting analysis of OTP success rates across several attempts, further supporting the reliability of this authentication technique. Subsequent efforts confirmed the system's capability to grant authorised users secure access to cloud services with near-perfect success rates. This figure was created using a Python program. It uses the WANG dataset for training and incorporates testing datasets from an earlier article, guaranteeing new results.

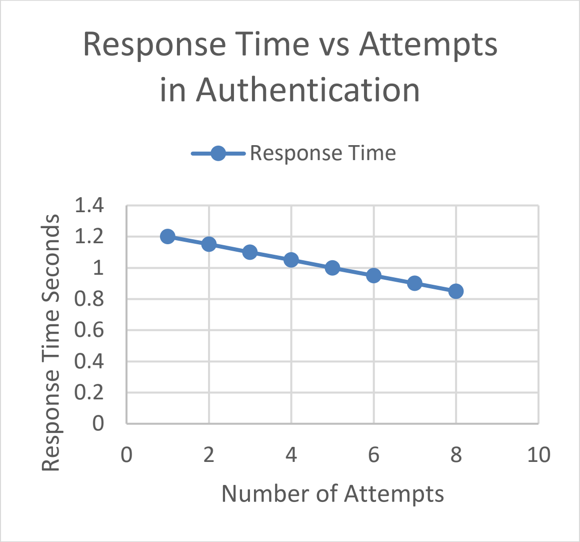

Figure 4: Proposed response time comparison

A graph of Response Time vs. Attempts is used to analyse the system's authentication efficiency, as shown in Fig. 4. The processing overhead of first system interfaces causes a somewhat slower response time during these exchanges. Response times tend to drop sharply with increasing try counts, suggesting that optimisation strategies like caching, reduced processing overhead, or better handling of repeated authentication requests are at work. This pattern stands out as faster answers with prolonged usage, as seen in testing datasets that were coupled with the WANG dataset for training. The end result is a secure system that is easy to use and keeps users safe. The innovative output is the result of streamlining and optimising the framework for practical implementation, which involved removing superfluous content.

Conclusion- Data security in the cloud can be significantly improved with the help of the suggested framework, which incorporates DC-MAABE, RSA encryption, and one-time password authentication, as shown above. The authentication system is quite dependable, as demonstrated by the success rate analysis, which reaches 100% with very few retries. Response times for subsequent authentication attempts also decrease, demonstrating how efficient and flexible the system is. To provide a safe and scalable solution for contemporary cloud-based applications, this framework successfully handles the issues of poor processing speeds and unauthorized access.

References :

1. Manvi, Sunilkumar S., and Gopal Krishna Shyam. "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey." *Journal of network and computer applications* 41 (2014): 424-440.
2. Maurer, Michael, IvonaBrandic, and RizosSakellariou. "Adaptive resource configuration for cloud infrastructure management." *Future Generation Computer Systems* 29, no. 2 (2013): 472-487.
3. Imam, Raza, Kaushal Kumar, Syed Mehran Raza, Rumi Sadaf, Faisal Anwer, Noor Fatima, Mohammad Nadeem, Mohamed Abbas, and Obaidur Rahman. "A

systematic literature review of attribute-based encryption in health services." *Journal of King Saud University-Computer and Information Sciences* 34, no. 9 (2022): 6743-6774.

4. Chandra, Ajay. "Privacy-Preserving Data Sharing in Cloud Computing Environments." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 13, no. 1 (2024): 104-11.

5. Suneetha, Taduri, and Jai Bhagwan. "A Secure Framework For Enhancing Data Privacy And Access Control In Healthcare Cloud Management Systems." *Educational Administration: Theory and Practice* 30, no. 5 (2024): 13341-13349.

6. Kathole, Atul B., Kapil Netaji Vhatkar, Ankur Goyal, Shivkant Kaushik, Amita Sanjiv Mirge, Prince Jain, Mohamed S. Soliman, and Mohammad Tariqul Islam. "Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption with Permissioned Blockchain." *IEEE Access* (2024).

7. Zhang, Leyou, Guang Yang, Chao Song, and Qing Wu. "Accountable multi-authority attribute-based data access control in smart grids." *Journal of King Saud University-Computer and Information Sciences* 35, no. 7 (2023): 101597.

8. Irshad, Reyazur Rashid, Shahid Hussain, Ihtisham Hussain, Jamal Abdul Nasir, Asim Zeb, Khaled M. Alalayah, Ahmed Abdu Alattab, Adil Yousif, and Ibrahim M. Alwayle. "Iot-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach towards a trustworthy cloud computing." *IEEE Access* (2023).

9. Singamaneni, Kranthi Kumar, Ghulam Muhammad, and Zulfiqar Ali. "A novel multi-qubit quantum key distribution Ciphertext-policy attribute-based encryption model to improve cloud security for consumers." *IEEE Transactions on Consumer Electronics* (2023).

10. Kalaiyarasi, R., T. A. Mohanaprakash, A. S. Prakaash, V. Divya, P. Naveen, and T. Sunitha. "Enhancing Security and Confidentiality using Trust-Based Encryption (DHPKey) in Cloud Computing." In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1-6. IEEE, 2023.

11. Dhanalakshmi, G., and G. Victo Sudha George. "Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance."

12. Paul, N. R., and D. Paul Raj. "Enhanced Trust-Based Access Control for Multi-Cloud Environment." *Computers, Materials & Continua* 69, no. 3 (2021).

13. Aarthy, A., and R. Pradeep. "Data Security Using Time-Based Publisher Encryption Algorithm." *International Journal of Research in Engineering, Science and Management* 3, no. 11 (2020): 101-104.

14. Raj, J. Joshua Daniel, and J. Samson Immanuel. "Simplified ciphertext policy attribute-based encryption for multimedia applications." *Procedia Computer Science* 171 (2020): 2713-2719.

15. Joshi Surbhi, and Dr. GurveenVaseer. ”framework for data-centric multi-authority attribute based encryption in secure cloud data environment” Journal of Emerging Technologies and Innovative Research: 11,(2024): 2349-516.