# Private Cloud with Enhanced Security

SNEHA SACHDEVA[1], OMRAJ SHARMA[2]
[1, 2] *Student, Maharaja Agrasen Institute of Technology*

***Abstract-*** ***This research paper examines the challenges arising from the rapid technological advancements in cloud computing and the unresolved security concerns associated with private cloud environments. It offers a comprehensive analysis of the necessary security measures to protect private cloud platforms, with a specific focus on addressing data governance difficulties. The study proposes effective strategies to mitigate potential risks and safeguard sensitive data. The primary objectives of the research include secure data uploading to the cloud, ensuring that even the administrator cannot access it. The upload module enables users to securely upload encrypted files to their cloud document directory, while the download module allows users to retrieve and decrypt their data using their private secret key. Additionally, the research emphasizes the importance of maintaining data integrity during secure downloads. The proper utilization and exchange of public, private, and secret keys for data encryption and decryption are also explored in detail. This research contributes valuable insights and practical solutions to enhance the security of private cloud environments and protect data confidentiality and integrity.***

## I. INTRODUCTION

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers, data storage, development tools, and networking capabilities hosted at a remote data center managed by a cloud services provider. Cloud Computing provides various benefits like lower IT costs, and easy and efficient scalability [1]. Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Most cloud service providers do not offer sufficient security measures to maintain the security of the data, which makes clients hesitant to store their data somewhere that is very easy for someone else to access.

Deploying robust identity and access management controls are crucial steps to take. Applying cryptography algorithms is one of the most popular methods to ensure the security of data in cloud storage and in transmission processes.

## II. LITERATURE REVIEW

S. Liu, et al presented an analysis of the state-of-the-art research on security challenges, security requirements, and security mechanisms in private clouds. Peter Mell and Timothy Grance have analysed the security hurdles encountered in both public and private clouds [3]. It delves into essential security aspects, including safeguarding data, securing networks, managing identities, and ensuring compliance. Additionally, the paper offers valuable insights into emerging security standards and recommended approaches to enhance security practices. Siani Pearson has discussed a diverse range of security issues and obstacles in cloud computing, encompassing aspects such as data privacy, integrity, availability, and access control [4].

Security concerns, according to B. R Kandukuri and V.R.Paturi, are one of the primary reasons why large businesses would still not move their data to the cloud [5]. Creators have given extraordinary examinations on information security and security insurance issues connected with the cloud. Subashini S, and Kavitha V, provide a comprehensive overview of security concerns and resolutions in cloud computing [6]. They have addressed various areas such as safeguarding data, securing networks, protecting virtual machines, and managing security in cloud environments.

Almass Abbassi and Shahab S.Band focused on enhancing the security of private clouds using software-defined networking techniques [7]. It highlights the integration of SDN with private clouds, virtual network isolation, traffic monitoring, and access control mechanisms. Ahmed Albugmi, Mandini O. Alassafi, Robert Walters, and Gary Wills

discussed the details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats [8].

## III. SAFETY MECHANISMS

Safety mechanisms in cloud security refer to the various measures and protocols implemented to ensure the protection, secrecy, reliability, and availability of data and resources in cloud environments. These mechanisms encompass a range of security controls such as encryption, access management, authentication, firewalls, intrusion detection systems, data backups, and disaster recovery plans.

By employing robust safety mechanisms, cloud security aims to mitigate risks, prevent unauthorized access, detect, and respond to threats, and maintain the overall safety of cloud-based services.

### *A. Authentication*

Authentication is the process of verifying the identity of a user or entity trying to access a system or resource. It involves confirming the validity of the credentials provided, such as usernames and passwords, digital certificates, or biometric information. By authenticating users, systems can ensure that only authorized individuals or entities gain access to sensitive information or resources.

### *B. Authorization*

Authorization involves granting or denying permissions to authenticated users or entities based on their roles, privileges, or other predefined criteria. It determines what actions or operations an authenticated user can perform within a system or on specific resources. Authorization controls ensure that users have appropriate levels of access and are restricted from accessing unauthorized data or functionalities.

### *C. Encryption Technology*

Encryption technology is always evolving, from simple substitution encryption to complicated public-key systems. It ensures that even if data is intercepted or accessed unlawfully, it remains confidential and cannot be understood without the corresponding decryption key [9].

Encryption algorithms employ complex mathematical algorithms and keys to transform plaintext into ciphertext, which is the encrypted form of the data. Strong encryption algorithms and secure key management practices are essential to ensure the effectiveness of encryption in preserving data confidentiality. There are three types of encryption technology: symmetric key cryptography, public-key cryptography, and hash function.

A symmetric key means that the encryption key is the same as the decryption key.
Public key cryptography is the technique that uses different public and private keys to encrypt and decrypt data. The hash function is a cryptographic algorithm that converts input data into a unique fixed-size output.

### *D. Decryption Technology*

Decryption refers to the procedure of transforming encoded data into its original, understandable format. By utilizing a decryption key or algorithm, the encrypted information is reversed to its original state. The primary objective of decryption is to guarantee the privacy and accuracy of data, enabling authorized individuals to access and comprehend the encrypted content.

Robust encryption algorithms and secure management of decryption keys are vital for ensuring effective decryption and upholding data security and confidentiality.

## IV. ENCRYPTION AND SAFETY ANALYSIS

This research undertakes an analysis of encryption security and network safety within open-source cloud platforms. These platforms incorporate their own security mechanisms, which can be evaluated using criteria like Virtual Machine (VM) security and Virtual Machine Monitor (VMM) [10]. The primary focus of this study is on examining encryption security and network security, encompassing techniques such as data encryption for safeguarding sensitive information and securing communication channels to prevent unauthorized access and network attacks.

By conducting this analysis, the aim is to enhance comprehension and identify effective measures that

ensure the confidentiality, integrity, and availability of data within open-source cloud environments.

*A. Encryption Key Generation*

Using two large prime numbers, P and Q, the RSA algorithm generates a public key (E) and a private key (D) pair. The public key is calculated by multiplying P and Q to obtain the value of N. Let us denote the Euler's totient function as "phi" (Φ), where Φ = (P - 1) * (Q - 1) [11].

We will use a BigInteger value, "E," with a length of length(N) - 1. To ensure that E is relatively prime to Φ (gcd(E, Φ) = 1), we iterate by incrementing E by 1 until this condition is met[12]. Let's consider two variables, "E" and "D."

We want to find a value for "D" such that the equation E * D ≡ 1 (mod PHI) holds true. To calculate "D," we can use the modular inverse function (modInverse) with inputs E and PHI. The modInverse(E, PHI) function will compute the modular multiplicative inverse of E with respect to PHI, ensuring that E * D ≡ 1 (mod PHI).

Iterate until the length of the AES_key is achieved. During each iteration, perform above mentioned two steps repeatedly until their length matches the specified length.

Concatenate the AES_key with the random number to generate the key "x."

Convert the obtained number to a large integer by utilizing the function stringToBigInteger(AES_key). Assign the resulting value to a variable called "S," which will serve as the secret key [13].

## V. FLOWCHART

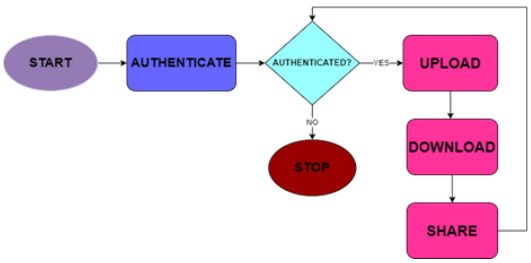


Fig. 1. This shows the flow of the process.

The flowchart depicts a simple process where user authentication is checked at the beginning. Authenticated users are then given access to upload, download, or share resources on the cloud platform, while unauthenticated users are stopped from progressing any further.

## VI. USE CASE DIAGRAM

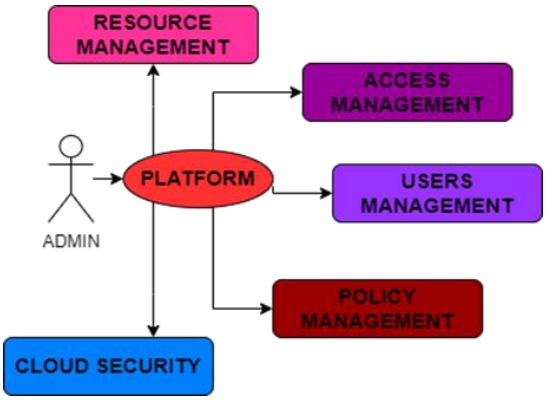


Fig. 2. This depicts the administrator roles.

The administrator plays a vital role in managing and allocating storage capacity within the private cloud. With the authority to make decisions, the administrator ensures that storage resources are distributed effectively according to user requirements, organizational policies, and other relevant factors.

Having privileged access, the administrator holds control over the private cloud environment, enabling them to implement and oversee security measures, configure settings, enforce access controls, monitor security events, and carry out other security-related responsibilities.

The administrator's crucial role lies in maintaining and managing the security of the private cloud infrastructure to ensure its protection and integrity.

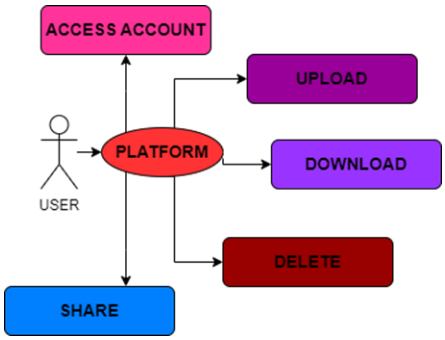


Fig. 3. This depicts the user roles.

In a cloud service, users are assigned distinct roles with corresponding permissions that grant them the ability to perform specific actions. These roles empower users to carry out tasks like accessing their own accounts, uploading, and downloading files, and sharing resources with others [14].

Through the allocation of roles and permissions, the cloud service ensures that individuals possess appropriate access and capabilities aligned with their specific requirements and responsibilities.

## VII. RESULT

Authenticated users benefit from a centralized platform that effectively manages applications, devices, and data while prioritizing security. The private cloud environment created offers a safe space for authenticated users to access specific privileges. Advanced encryption technologies such as RSA and AES are employed by the platform to guarantee data security. All data stored within the cloud undergoes encryption, and only the user's private key, which is kept confidential even from the administrator, can decrypt the encrypted data.

This robust encryption methodology significantly bolsters the overall security of the cloud platform, ensuring that users' data is highly safeguarded.

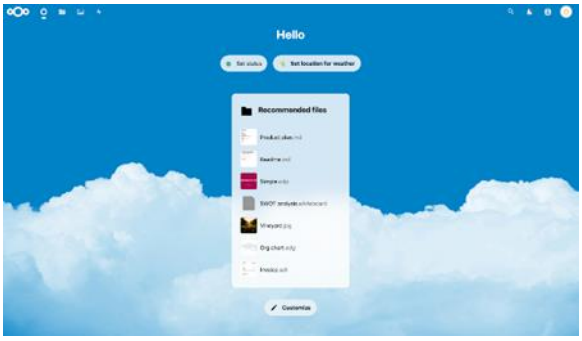


Fig. 4. This figure depicts the user dashboard which shows activity and authentication status

Located in the upper left section of the private cloud platform, users are presented with convenient options that are easily accessible. They can access their personalized dashboard, offering a comprehensive overview of their account and activities.

Furthermore, users can effortlessly upload files or photos, enabling efficient storage and organization of their data within the cloud. In addition, users can review their activity log, which provides a detailed record of their interactions and engagements within the platform.

On the top right side of the private cloud platform, users are provided with convenient options. These options include managing notifications, customizing profile settings, and performing actions such as searching, logging in, and logging out. These user-friendly features empower individuals to control their notification preferences, personalize their profile, and seamlessly navigate the platform by easily searching for specific content.

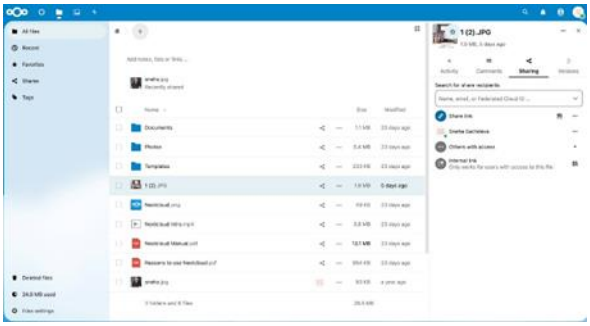

Fig. 5. This figure depicts user roles like uploading, deleting, and sharing files

The platform offers a graphical representation of the storage space in use, enabling users to monitor their storage utilization visually.

Furthermore, users can conveniently track the files they have uploaded or deleted, providing transparency in their file management activities.

The platform provides a user-friendly option to share selected files, facilitating collaboration by allowing users to grant access to specific files to others.

## CONCLUSION

The robust platform offers a secure and user-friendly solution that effectively tackles data security concerns. Through features like secure file uploading, storage management, and intuitive sharing options, users can efficiently handle their data while maintaining top-notch security.

The encryption keys generated based on system time ensure the utmost protection of user data against potential threats. This enhanced system prioritizes information security, and data integrity, and provides users with a seamless platform for a wide range of activities.

## REFERENCES

[1] I. Bojanova, and A. Samba, “Analysis of Cloud Computing Delivery Architecture Models,” in Proc. IEEE International Conf. on Advanced Information Networking and Applications (WAINA), Biopolis, Singapore, 2011, pp. 453-458.

[2] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” ACM Trans. On Communications, vol. 21, no. 2, pp. 120-126, Feb 1978.

[3] Peter Mell and Timothy Grance,The NIST Definition of Cloud Computing https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] Siani Pearson,”Privacy , Security and Trust in Cloud Computing”, Jan 2013, In book: Privacy and Security For Cloud Computing (pp.3-42).

[5] Kandukuri B R, Paturi V R, Rakshit A. Cloud security issues[C]//Services Computing, 2009. SCC'09. IEEE International Conference on. IEEE, 2009: 517-520.

[6] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing[J]. Journal of Network and Computer Applications, 2011, 34(1): 1-11. House, October 2008.

[7] Alams Abbassi, Shahab S.Band, “Software-Defined Cloud Computing”:A systematic Review on Latest Trends and Developments. July 2019, IEEE Access PP (99):1-1.

[8] Ahmed Albugmi, Mandini O. Alassafi, Robert Walters, and Gary Wills, “Data Security in Cloud Computing”, 2016 Fifth International Conference on Future Generation Communication Technologies, IEEE, Luton, UK Volume 1.

[9] OpenStack Security Guide URL: http://docs.openstack.org/securityguide/security-guide.pdf

[10] Peng J, Zhang X, Lei Z, et al. Comparison of several cloud computing platforms[C]//Information Science and Engineering (ISISE), 2009 Second International Symposium on. IEEE, 2009: 23-27.

[11] Google URL: https://appengine.google.com

[12] Faraz Fatemi Moghaddam; Omidreza Karimi; Maen T. Alrashdan,2013 IEEE 2nd International Conference on Cloud Networking (CloudNet).

[13] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DES, and Other Systems,” in Proc. 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'96), London, UK, 1996, pp. 104-113.

[14] S. A. Vanstone, “Next Generation Security for Wireless: Elliptic Curve Cryptography,” Elsevier Trans. on Computers & Security, vol. 22, no. 5, pp. 412-415, Jul 2003.