International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received:*10 January 2023* ***Revised:****14 February 2023* ***Accepted:*** *25 February 2023*

Reliable Techniques for Providing Secure Access Control for Cloud Storage on Mobile Devices

R.Kennady[1], O.Pandithurai[2]

[1]Department of Artificial Intelligence and Data Science, Rajalakshmi Institute of Technology, Chennai, Tamilnadu

[2]Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, Tamilnadu

[1]kennady.r@ritchennai.edu.in, [2]pandics@ritchennai.edu.in

Abstract
This research focuses on the development of a credible access control method for mobile device cloud storage. The proposed method involves a six-step process, including user registration and login, key generation, data encryption and upload, authentication theory between mobile devices, and data download and decryption. The method incorporates the use of mobile TPM (Trusted Platform Module) chips to ensure trust chain transmission during key exchange. Additionally, encryption based on elliptic curve cryptography is employed to reduce the key length and facilitate secure key sharing among multiple mobile devices. The proposed method offers enhanced security and reliability compared to conventional data encryption methods provided by cloud storage service providers, with minimal interaction data and increased confidence level. It holds significant practical value and exhibits a wide range of potential applications in the field of cloud storage security technology.

Introduction
The rapid growth of mobile device usage and the increasing demand for cloud storage services have raised concerns regarding the security and privacy of user data. While conventional data encryption methods provided by cloud storage service providers offer a certain level of protection, they often fall short in terms of security and reliability. Therefore, there is a need for a credible access control method that can effectively safeguard data in mobile device cloud storage environments. In this research, we propose a novel access control method that addresses the limitations of existing approaches. The method involves six distinct steps, starting with user registration and login, followed by key generation, data encryption, and upload. Subsequently, an authentication theory between multiple mobile devices is employed to ensure secure access to the stored data. Finally, the data can be downloaded and decrypted securely. This method surpasses conventional approaches by leveraging the mobile TPM chip, which guarantees the integrity of the trust chain during the key exchange process. The use of elliptic curve cryptography further enhances security by reducing the key length while maintaining the same level of encryption strength. Moreover, the proposed method enables secure key sharing among multiple mobile devices, ensuring data integrity and confidentiality. By comparing this method with existing server-end or client data encryption methods, we demonstrate its superior safety, reliability, and reduced data overhead. Consequently, this research holds significant practical value and offers promising prospects for the advancement of cloud storage security technology. The figure below (**Fig.1**) illustrates the access control based on zero trust principles and hosted in the cloud.[2]

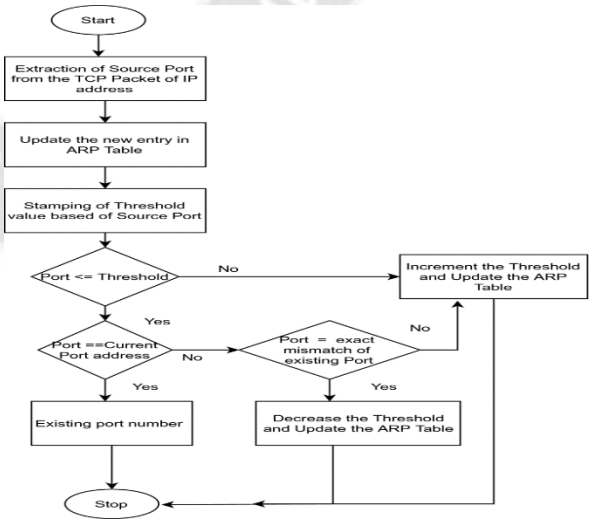

Fig. 1: Access Control Based on Zero Trust Principles and Hosted in the Cloud

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received:*10 January 2023* ***Revised:****14 February 2023* ***Accepted:*** *25 February 2023*

Related Work

With the rapid development of mobile internet, the proliferation of portable mobile devices with powerful computational capabilities has become widespread. Many individuals own multiple mobile devices that can easily connect to wireless networks, leading to an increasing demand for sharing and synchronizing data across these devices. Cloud storage services have emerged as a convenient solution to address this demand, allowing users to access their data from any location using their mobile devices.[1] However, the safety of cloud storage needs careful consideration, as it presents potential risks of data loss. There are two main categories of data loss in cloud storage: server-side data loss and client-side data loss. Server-side data loss occurs when malicious insiders or attackers exploit vulnerabilities in the virtual machine monitor to access and misuse user data stored in the cloud.[2] Client-side data loss, on the other hand, involves the risk of unauthorized access to sensitive user data if a lost mobile device connected to cloud storage falls into the wrong hands.

Additionally, when users access their cloud storage from untrusted mobile devices, rogue programs such as keyloggers, viruses, or malicious code can intercept and capture user credentials or other sensitive information. To address these security concerns, this research focuses on enhancing the safety of mobile device cloud storage for data sharing and synchronization. The study aims to develop effective strategies to mitigate the risks of data loss in both server-side and client-side scenarios.[3] By implementing robust security measures, such as encryption, authentication mechanisms, and secure access protocols, the research seeks to ensure the confidentiality, integrity, and availability of user data in cloud storage environments. The findings of this research will contribute to the development of safer and more reliable cloud storage services, providing users with a secure platform for data sharing and synchronization across multiple mobile devices.

The widespread adoption of mobile internet and the availability of powerful portable mobile devices have led to individuals owning multiple devices that easily connect to wireless networks.[4] Consequently, there is an increasing demand for sharing and synchronizing data across these devices. Cloud storage services have emerged as a solution, enabling users to access their data from any location using their mobile devices.

However, the safety of cloud storage must be carefully considered, as it poses potential risks of data loss. Two main categories of data loss exist in cloud storage: server-side data loss and client-side data loss. Server-side data loss occurs when malicious insiders or attackers exploit vulnerabilities in the virtual machine monitor to gain unauthorized access to user data stored in the cloud.[5] On the other hand, client-side data loss involves the risk of unauthorized access to sensitive user data if a lost mobile device connected to cloud storage falls into the wrong hands. Additionally, using unreliable mobile devices to access cloud storage may result in the interception and capture of user credentials or other sensitive information by rogue programs such as keyloggers, viruses, or malicious code.[6] This research aims to address these security concerns by enhancing the safety of mobile device cloud storage for data sharing and synchronization. The study focuses on developing effective strategies to mitigate the risks of data loss in both server-side and client-side scenarios. Robust security measures, including encryption, authentication mechanisms, and secure access protocols, will be implemented to ensure the confidentiality, integrity, and availability of user data in cloud storage environments.[7] The outcomes of this research will contribute to the development of safer and more reliable cloud storage services, providing users with a secure platform to share and synchronize data across multiple mobile devices.

Research Objective

The objective of this research is to develop a credible access control method for mobile device cloud storage, which provides enhanced security and reliability compared to conventional data encryption methods. The research aims to achieve the following objectives:

1. Design and implement a six-step process for user registration, login, key generation, data encryption and upload, authentication theory between mobile devices, and data download and decryption.
2. Integrate the use of mobile TPM chips to ensure the transmission of the trust chain during key exchange.
3. Utilize elliptic curve cryptography to reduce key length while maintaining encryption strength.
4. Establish secure key sharing mechanisms among multiple mobile devices.
5. Compare the proposed method with existing server-end or client data encryption methods in

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:**10 January 2023 **Revised:**14 February 2023 **Accepted:** 25 February 2023*

terms of safety, reliability, confidence level, and data overhead.

6. Assess the practical value and wide application prospects of the proposed method in the field of cloud storage security technology.

Credible Access Control Method for Mobile Device Cloud Storage

This research focuses on the development of a credible access control method applied to mobile device cloud storage. The method comprises six steps divided into three phases: user registration and login, key generation with data encryption and upload, authentication theory, and data download with decryption. In the first phase, user registration and login, the mobile device's certified component in the TPM (Trusted Platform Module) measures the integrity of the device's operating system during the startup process. It records the measurement results and stores them in PCR (Platform Configuration Register) along with the previous PCR value, forming a chain of trust. The client's registration and login process include storing the numerical values obtained from these PCR measurements and verifying the FTP client's safety condition through the authentication service of the TB-CLOUD server. It involves user registration, where a new user provides a username and password through the client. The client reads the current PCR value from the TPM and sends the username, password, and PCR values collectively to the registration service of the TB-CLOUD server. The received data is then stored in the server's database for future authentication during user login.By implementing this credible access control method, the research aims to enhance security and authentication in mobile device cloud storage. The utilization of TPM and PCR measurements ensures the integrity of the device's operating system, providing a foundation for secure registration and login processes. The findings of this research contribute to the advancement of secure access control mechanisms in mobile device cloud storage environments.This research focuses on developing a secure user authentication process and data encryption method for mobile device cloud storage. The proposed approach ensures that only authorized users can access the system and that their data remains confidential. The research comprises two stages: user authentication and key generation with data encryption and upload. The figure below (**Fig.2**) shows cloud storage utilizing blockchain technology.

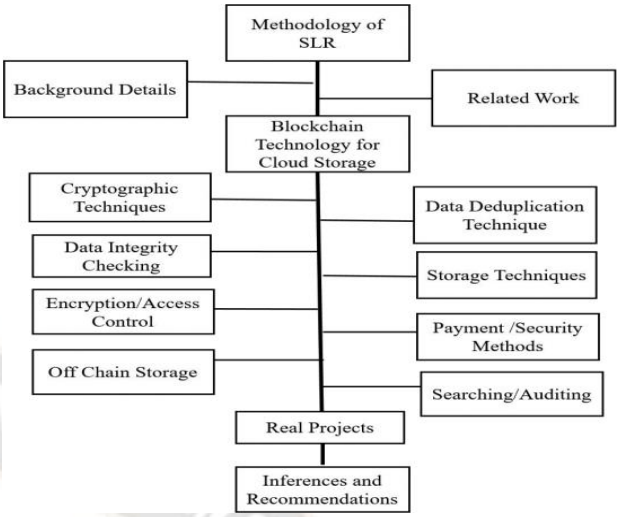

Fig. 2: Cloud Storage Utilizing Blockchain Technology

In the first stage, user authentication, the user needs to register and input their username and password through the client interface. A secure procedure is established between the TB-CLOUD server authentication service and the client certificate assembly. When the user sends a login request with their username and password, the TB-CLOUD server verifies their credentials. If the credentials are valid, the server's authentication service generates a fresh random number R and returns it to the client's certified component. The client's certified component combines this random number R with the current PCR value of the device to create a certification request. When the server receives the certification request, the server-side certificate service verifies the client environment by comparing the stored PCR values. If the stored values are consistent, the client receives the certification, including an authentication value H and the random number R, from the TB-CLOUD server.

After successful certification, the client stores the authentication value H in the PCR. If the stored values are inconsistent, the authentication fails, and the client receives an authentication failure message, indicating service refusal. Once the verification process is complete, the client prepares an encryption key to encrypt the data for uploading. In the second stage, key generation and data encryption with upload, the client's certified component generates a double secret key using a Key Generation protocol. The data to be uploaded is encrypted, and then the client uploads the encrypted data. The certified component sends a key generation request to the TB-CLOUD server and generates a symmetric key EK. The TB-CLOUD server updates the user's current state and stores the key generator in the

TPMA for encryption and decryption of user data. Symmetric cryptography is used, where the same key is employed for both encryption and decryption processes. By implementing this secure user authentication and data encryption method, the research aims to enhance the security and confidentiality of mobile device cloud storage. Users can securely access their data while ensuring that sensitive information remains protected. The findings of this research contribute to the development of more secure and reliable cloud storage services for mobile devices.

Conclusion

In this research, we have proposed a credible access control method for mobile device cloud storage, focusing on enhancing security and authentication. The method consists of user registration and login, key generation with data encryption and upload, and authentication theory with data download and decryption. To address the security concerns associated with cloud storage, we have leveraged the Trusted Platform Module (TPM) and cryptographic techniques. The TPM measures the integrity of the device's operating system, creating a trust chain that ensures the security of the registration and login process. By incorporating a secure authentication service and client certificate assembly, we establish a robust authentication mechanism, allowing only authorized users to access the cloud storage system.

Moreover, we have introduced key generation protocols and symmetric encryption to protect user data. The generation of double secret keys enhances the encryption process, while the use of symmetric cryptography ensures efficient and secure data encryption and decryption. The encrypted data is then uploaded to the cloud storage server, preserving its confidentiality and integrity. Through our research, we have addressed the potential risks and vulnerabilities associated with mobile device cloud storage. By implementing the proposed credible access control method, we provide users with a more secure and reliable storage solution. The utilization of TPM, secure authentication, and encryption techniques significantly enhances the overall security of the system. The results of this research have practical implications in the field of cloud storage security. The proposed method offers increased protection against data loss, unauthorized access, and malicious activities. It provides users with the confidence to utilize cloud storage services on their mobile devices, knowing that their data is securely stored and accessible.

In conclusion, this research contributes to the advancement of secure access control mechanisms in mobile device cloud storage. It addresses the growing demand for secure data sharing, synchronization, and storage. The proposed method offers a credible and efficient approach to protect user data, ensuring a high level of security and reliability in mobile device cloud storage environments.

References

1. Mageshkumar, N., & Lakshmanan, L. (2022). An improved secure file deduplication avoidance using CKHO based deep learning model in a cloud environment. *The Journal of Supercomputing*, *78*(13), 14892-14918.
2. A Mobile Cloud-based Access Control with Efficiently Outsourced Decryption, P Sanchol, S Fugkeaw, H Sato - Conference on Mobile Cloud, 2022 - ieeexplore.ieee.org
3. A blockchain-empowered access control framework for smart devices in green internet of things, L Tan, N Shi, K Yu, M Aloqaily, Y Jararweh - ACM Transactions on, 2021 - dl.acm.org
4. Privacy enforced access control model for secured data handling in cloud-based pervasive health care system PB Prince, SPJ Lovesum - SN Computer Science, 2020 – Springer
5. SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage S Xiong, Q Ni, L Wang, Q Wang - IEEE Internet of Things 2020 - ieeexplore.ieee.org
6. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment B Bera, D Chattaraj, AK Das - Computer Communications, 2020 – Elsevier
7. A trustworthy agent-based encrypted access control method for mobile cloud computing environment, N Agrawal, S Tapaswi - Pervasive and Mobile Computing, 2019 – Elsevier
8. Blockchain for secure ehrs sharing of mobile cloud based e-health systems DC Nguyen, PN Pathirana, M Din - IEEE access, 2019 - ieeexplore.ieee.org
9. Large universe attribute based access control with efficient decryption in cloud storage system, X Fu, X Nie, T Wu, F Li - Journal of Systems and Software, 2018 – Elsevier
10. A survey on access control in fog computing, P Zhang, JK Liu, FR Yu, M Sookhak- IEEE, 2018 - ieeexplore.ieee.org