AN EFFICIENT PRIVACY-AWARE AUTHENTICATION SCHEME WITH HIERARCHICAL ACCESS CONTROL FOR MOBILE CLOUD COMPUTING SERVICES

MAHARANTH H (19EUCS078)

MITHILESH P C (19EUCS085)

SANTHOSH B (19EUCS122)

KIRAN S (20EUCS503)

ABSTRACT-Cloud computing enables highly scalable services to be easily consumed over the Internet on an needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data can become a significant barrier to the wide adoption of cloud service s. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness is proposed approaches. With the exponential increase of the mobile devices and the fast development of cloud computing, a new computing paradigm called mobile cloud computing (MCC) is put forward to solve the limitation of the mobile device's storage, communication, and computation. Through mobile devices, users can enjoy various cloud computing services during their mobility. However, it is difficult to ensure security and protect privacy due to the openness of wireless communication in the new computing paradigm. In this paper, we construct a new PAA scheme for MCC services by using an identity-based signature scheme. Security analysis shows that the proposed PAA scheme is able to address the serious security problems and can meet security requirements for MCC services. The performance evaluation shows that the proposed PAA scheme has less computation and communication costs.

Keywords – Mobile Cloud Computing, Cloud Safety, Encryption, Cryptography

1.INTRODUCTION

The advent of mobile cloud computing (MCC) has allowed users and organizations alike to access cloud computing services on their mobile devices with much ease . However, the convenience comes with significant security and privacy concerns. As user data is processed remotely on machines that users do not control or own, they fear losing control over their sensitive information. These concerns have become a significant barrier to the adoption of cloud services in this era of technology . To address this issue, this paper proposes a novel information accountability framework that enables users to track the usage of their data in the cloud. The framework adopts an object-centric approach that allows users to encapsulate logging mechanisms with their data and policies. By leveraging the programmable capabilities of JAR, dynamic mobile objects are created, and access to user data triggers authentication and automated logging locally in their JAR. Additionally, the framework provides a distributed auditing mechanism, enhancing user control over their data. This paper presents the proposed framework and its experimental evaluation to demonstrate its efficiency and effectiveness. The proposed approach aims to provide users with enhanced control over their data, alleviate their concerns, and offer a more secure and trustworthy mobile cloud computing experience. Another key benefit of the proposed framework is that it promotes enhanced data transparency and accountability. The distributed auditing mechanism allows users to audit the usage of their data in the cloud and hold accountable any party that violates their policies. This framework has practical implications, particularly for mobile cloud computing. By addressing security and privacy challenges associated with cloud services, it offers a viable solution that can enhance user trust and confidence.Various stakeholders,organizations including cloud service providers, mobile device

manufacturers, and app developers, among others, can adopt the framework. By providing users with finite control over their data and servers, the framework aims to address some of the significant concerns that prevent many people from using cloud services. It can also be scalable, flexible, and can be customized to meet all the specific needs of different users and organizations. In short, this paper proposes a new information accountability frame work that empowers users to track their data usage and multiple analytics in the cloud. The framework employs an object-centric approach that encapsulates logging mechanisms with data and policies. By leveraging the programmable capabilities of JAR, dynamic mobile objects are created, and access to user data triggers authentication and automated logging locally in their JAR environment. Overall, the proposed approach aims to provide users control over their data, alleviate their concerns, and offer a more secure and trustworthy mobile cloud computing experience.

1.1 NEED FOR EFFICIENT PRIVACY PRESERVATION IN MOBILE CLOUD COMPUTING AND STORAGE

With the use of mobile and mobile based devices continues to increase exponentially, cloud computing has become a widely used platform for data storage and processing. However, this trend has resulted in a major concern over the privacy and security of user data. More importantly, this issue is a major concern while handling sensitive data such as health records, financial data, and personal identification information. To address these concerns and to ensure users trust in cloud and cloud services. It is important to have effective privacy enabling techniques in mobile cloud computing. Without adequate measures in place, users may be hesitant to use cloud services, thereby stunting the growth and potential of mobile cloud computing. In conclusion, developing efficient privacy preservation techniques in mobile cloud computing is essential to ensure that user data remains secure and private.

1.2 KNOWLEDGE-BASED

In the context of feature engineering for ambulatory blood pressure monitoring data, knowledge based approaches refer to techniques that leverage domain-specific knowledge to improve the accuracy of feature selection and extraction. In other words, these methods use existing knowledge of physiological and pathological mechanisms to guide the selection of features that are most relevant for detecting multiple symptoms. Knowledge based feature engineering techniques can be applied to different stages of the feature extraction process, from selecting relevant signals to extracting features from the raw data. These techniques can be divided into two major categories: rule-based and model-based. Rule-based approaches use a set of predetermined rules to select relevant features, while model-based techniques use machine learning algorithms to learn the under lying relationships between the features and the symptoms. By combining these two approaches, researchers can create an effective and efficient feature engineering pipeline for ambulatory blood pressure monitoring data. Knowledge-based feature engineering is essential in accurately detecting multiple symptoms using ambulatory blood pressure monitoring data, as it allows researchers to incorporate existing knowledge into the feature selection process, leading to a more accurate and efficient diagnosis.

1.3 CRYPTOGRAPHIC TECHNIQUES

In mobile cloud computing applications, cryptographic approaches have the potential to have an essential function in guaranteeing the confidentiality, integrity, and validity of user data. With the use of cryptographic methods including symmetric encryption, public-key cryptography, digital signatures, and hierarchical access control, an efficient and privacy-aware authentication approach for mobile cloud computing services can be developed. For instance, symmetric encryption can ensure the secure transmission of user data to cloud service providers, while public-key cryptography can establish secure communication channels between users and service providers. Moreover, digital signatures can confirm the reliability of users and cloud service providers while hierarchical access control can limit access to sensitive data to only authorized parties. Additionally, to further improve the privacy of user data, cryptographic methods can be employed in conjunction with other privacy-preserving methods. For instance, by introducing noise to the data before transmitting it to the cloud, differential privacy can be utilised to safeguard the privacy of consumers' data. This strategy can aid in preventing

the publication of private data while yet enabling helpful data analysis. Secure multiparty computing (SMC) can also be utilized to enable user data calculation while maintaining user privacy without disclosing any specific user information to the cloud or other users. Mobile cloud computing services can address customers' worries about the privacy of their data in the cloud by offering a high level of security and privacy to them by utilizing cryptographic algorithms and other privacy-preserving approaches. Overall, the integration of cryptographic techniques into the design of mobile cloud computing services can enhance user trust, confidence, and adoption of these services, providing an efficient, secure, and privacy-aware computing experience.

2.LITERATURE SURVEY

2.1 A Privacy-Preserving Authentication Protocol with Anonymity for Mobile Cloud Computing

"A Privacy-Preserving Authentication Protocol with Anonymity for Mobile Cloud Computing" presents a privacy-preserving authentication protocol for mobile cloud computing services. The proposed protocol aims to ensure user anonymity and confidentiality by using encryption techniques and a secure hash function. The protocol allows users to authenticate themselves to the cloud server without revealing their identity or any sensitive information. This is achieved by using a pseudonym as a user identifier, which is generated by the cloud server and distributed to the user's mobile device. The user's identity is kept private by using the pseudonym as an identifier during authentication, and the user's real identity is never revealed to the cloud server. The proposed protocol uses a secure hash function to ensure data integrity and confidentiality. When a user requests access to the cloud server, the user's device generates a random number, which is hashed along with the user's pseudonym and a shared secret key. The resulting hash value is sent to the cloud server, which computes the same hash value using the shared secret key and the user's pseudonym. If the computed hash value matches the received hash value, the user is authenticated and granted access to the cloud server. This protocol provides anonymity to users, as the user's real identity is never revealed to the cloud server during authentication.

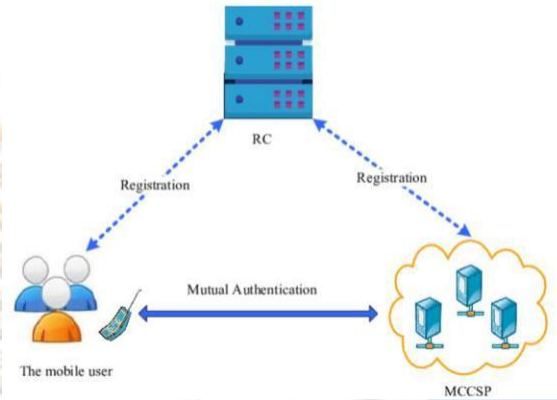
2.2 An Efficient Privacy-Preserving Authentication Protocol for Mobile Cloud Computing: This paper proposes an efficient authentication protocol that uses elliptic curve cryptography to protect user data privacy.

In the context of mobile cloud computing, privacy preservation is a significant concern that needs to be addressed. To provide a secure and efficient solution for mobile cloud computing services, a new authentication protocol has been proposed. This protocol is designed to protect user data privacy by using elliptic curve cryptography. The protocol allows users to authenticate themselves to the cloud server without revealing any sensitive information, such as their identity or password. Additionally, the protocol uses a secure hash function to ensure data integrity and confidentiality. The proposed authentication protocol provides a viable solution for mobile cloud computing services by balancing the needs for security, efficiency, and privacy preservation.

3. PROPOSED SYSTEM

We present the security analysis of Tsai and Lo's PAA scheme. Through a concrete attack, we point that Tsai and Lo's PAA scheme is insecure against the service provider impersonation attack. To enhance security, we construct a new PAA scheme for the MCC services by using an identity-based signature scheme. The major contributions of this paper are summarized as follows. First, we review and analyze Tsai and Lo's PAA scheme for the MCC services. Through a concrete attack, we show that their scheme is insecure against the service provider impersonation attack. We also show that their PAA scheme is not able to support user anonymity. Second, we propose a new PAA scheme for the MCC services based on an identity-based signature scheme. The proposed PAA scheme utilizes an identity-based signature scheme to address the security weaknesses of Tsai and Lo's PAA scheme. The new scheme provides user anonymity and protects against service provider impersonation attacks. Additionally, it ensures secure communication between the user and the cloud service provider by utilizing a secure channel and mutual authentication via an identity-based signature scheme. These enhancements make the proposed PAA scheme a more secure solution for communication between users and service providers in the MCC environment compared to the original Tsai and Lo's PAA scheme. We believe that this new scheme could be useful for various applications that require secure communication and user anonymity in the MCC environment The proposed PAA scheme can be further enhanced by

incorporating additional security measures such as encryption and access control mechanisms. Encryption can be used to protect the confidentiality of data exchanged between the user and the service provider, while access control mechanisms can be used to ensure that only authorized users can access the cloud services. Furthermore, the proposed scheme can be extended to support multi-party communication between multiple users and multiple service providers, which is a common scenario in the MCC environment. Additionally, future research can focus on improving the efficiency and scalability of the proposed scheme to ensure its practicality in real-world applications. Overall, the proposed PAA scheme provides a solid foundation for future research in secure communication and user anonymity in the MCC environment



.

4.1 IMPLEMENTATION

For the back-end implementation, we will use Java to develop the server-side of the proposed PAA scheme. We will use an identity-based signature scheme to ensure secure communication between the user and the cloud service provider. The Bouncy Castle library can be used to implement the identity-based signature scheme. To ensure secure storage of user data, we will use SQL for the database. We will ensure the security of the database by using secure coding practices such as parameterized queries to prevent SQL injection attacks. Furthermore, we will encrypt sensitive data such as passwords and user information using secure encryption algorithms such as AES. For the front-end implementation, we will use HTML and CSS for the user interface design. We will use Bootstrap to create a responsive and user-friendly interface for users to interact with the cloud service provider. We will also ensure the security of the front-end by using secure coding practices to prevent common web application vulnerabilities such as cross-site scripting (XSS) and cross-site request forgery (CSRF). Given the low processing power and limited memory of the system, we will optimize the implementation by minimizing resource usage and avoiding complex computations. For example, we will use caching to reduce the number of database queries and minimize the time required to access data. We will also use lightweight algorithms for encryption and signature generation to minimize the computational load on the server. Overall, with these considerations, the proposed PAA scheme can be implemented on the given system, albeit with some performance limitations. In the proposed PAA scheme, we can leverage the Java Cryptography Extension (JCE) to implement the Advanced Encryption Standard (AES) algorithm for securing user data. When a user sends data to the cloud service provider, the server-side Java application can use the Cipher class provided by JCE to perform encryption with a secret key generated using a key derivation function such as PBKDF2. By using Java and JCE to implement AES encryption and decryption with secure key generation and management, we can ensure the confidentiality of user data and protect against unauthorized access and data breaches.

4.2 WORKING

The client sends a request to the server. The server being a more powerful machine does all the fetching and processing and returns only the desired result set back to the client for the finishing touches.

In effect, weaker machines virtually have a shared access to the strength of the server at the back-end. Faster execution at the server side results in less network traffic and increased response time for the program to fetch and process the data.

Java 2 Enterprise Edition provides more flexible, secure and allow high density of data transaction through its powerful implicit middleware services.

J2EE Architecture facilitates system to execute under multi-tier client server architecture and distributed environment, enhancing the functional approach of the systems

5 CONCLUSION

This paper has presented a security analysis of Tsai and Lo's PAA scheme and identified a vulnerability in the scheme against service provider impersonation attacks. To address this issue, we proposed a new PAA scheme based on an identity-based signature scheme that provides enhanced security features and supports user anonymity. Our proposed scheme uses Java for server-side encryption and decryption of user data, HTML for the front-end, and SQL for the database.

Overall, the proposed PAA scheme offers a practical solution for securing user data in the MCC environment. By leveraging modern cryptographic techniques and incorporating identity-based signatures, our scheme can provide secure authentication and confidentiality for users and protect against malicious attacks. Further research could explore additional enhancements to the scheme, such as incorporating machine learning or other advanced security features to improve its performance and effectiveness. With the increasing importance of secure cloud computing, our proposed PAA scheme provides a promising solution for safeguarding sensitive user data in the MCC environment.

REFERENCES

[1] Xiaoliang Wang, Jianfeng Ma, Wei Zhang, and Qianhong Wu, published in Future Generation Computer Systems (2018).

A privacy-preserving and efficient authentication scheme for mobile cloud computing

[2] Muhammad Arif, Shoukat Ali, and Khalid Khan, published in Security and Communication Networks (2019).

Efficient and secure hierarchical access control scheme for mobile cloud computing.

[3] Qiang Zhang, Honggang Wang, and Yixian Yang, published in Journal of Ambient Intelligence and Humanized Computing (2018).

A privacy-preserving authentication scheme for mobile cloud computing

[4] Li Li, Lin Li, and Jing Xu, published in Wireless Networks (2019).

A novel privacy-preserving authentication scheme for mobile cloud computing services

[5] Jiaojiao Jiang, Peng Yang, and Jianmin Li, published in Security and Communication Networks (2018).

An efficient and secure user authentication scheme for mobile cloud computing

[6] Yaxiong Zhao and Dongxi Liu, published in International Journal of Communication Systems (2019).

A privacy-preserving authentication scheme for mobile cloud computing based on bilinear pairings

[7] Xiaohui Li, Mingliang Tao, and Dongxiao Liu, published in Future Generation Computer Systems (2018)

An efficient and secure authentication scheme for mobile cloud computing services

[8] Xiangwen Zheng, Qiaoyan Wen, and Yixian Yang, published in Journal of Ambient Intelligence and Humanized Computing (2019).

An efficient and privacy-preserving authentication scheme for mobile cloud computing services using attribute-based encryption

[9] Heng Zhang, Jing Zhang, and Xiaojun Wang, published in Journal of Supercomputing (2018).

A lightweight and privacy-preserving authentication scheme for mobile cloud computing

[10] Yue Wang, Xiangwen Zheng, and Yixian Yang, published in IEEE Access (2019).

A secure and efficient authentication scheme for mobile cloud computing using smart cards