IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Cloud Security using Biometric-Based Access Mechanism Design

K.Srinath[1], Dr.K.Venkataramana[2]

[1]PG student, Vemu institute of technology,P.Kothakota,

[2]Professor, Vemu institute of technology,P.Kothakota,

ABSTRACT

In our data-driven society, secure access to remote data storage and computation services is paramount. This paper introduces a novel biometric-based authentication protocol for secure cloud server access. Utilizing a user's biometric data as a secret credential, we derive a unique identity to generate their private key. Additionally, we propose an efficient method to establish a session key between communicating parties using biometric templates for secure message transmission. With detailed security analyses and formal verification, our approach withstands various known attacks. Extensive experiments and comparative studies underscore the efficiency and effectiveness of our proposed protocol.

Keywords: Cloud Services, Biometric

INTRODUCTION:

In today's society, cloud services have become an integral part of our daily lives. However, ensuring secure access to these services poses significant challenges, both operationally and in terms of research. Authentication, authorization, and accounting mechanisms are essential components in providing robust access control to cloud services. Various authentication protocols, such as Kerberos, OAuth, and OpenID, have been proposed to establish secure delegated access mechanisms among distributed entities [1]-[12]. These protocols typically rely on the assumption that the remote authentication server is a trusted entity within the network.

Traditionally, users register with a remote server to obtain authorization, and upon authentication, they gain access to services. However, a key limitation of existing authentication mechanisms is the storage of user credentials on the authentication server, making them vulnerable to theft and misuse for unauthorized access. Additionally, employing symmetric key cryptography for secure communication introduces overhead to authentication protocols.

To address these challenges, we propose a secure and efficient authentication protocol that eliminates the need for storing user credentials on the authentication server. Instead, we leverage biometric data, specifically fingerprint images, as secret credentials. Upon registration, a private key is generated from the fingerprint image and securely stored on the server without directly storing the biometric data.

During authentication, a new biometric fingerprint image is captured and used to generate a private key, which encrypts the biometric data for transmission to the authentication server. Once authenticated, the user gains access to desired services, facilitated by mutual authentication between the user and both the authentication and service servers.

Our approach offers several key benefits:

Effective transmission of biometric data over unsecured network channels to the authentication server.

Generation of revocable private keys directly from irrevocable fingerprint images, eliminating the need for storing sensitive data.

Mitigation of traditional limitations requiring user credentials to be stored on the authentication server.

Introduction of a novel approach for generating session keys using biometric data.

Elimination of overhead associated with preloaded secret information in traditional authentication protocols.

Introduction of a biometric-based message authentication mechanism as an alternative to existing protocols like Message Authentication Code (MAC).

Overall, our proposed authentication protocol offers enhanced security, efficiency, and usability compared to traditional mechanisms, paving the way for secure and seamless access to cloud services.

LITERATURE SURVEY:

A. K. Das, M. Wazid *et al*

With the rise of Internet-enabled devices, Industrial Internet of Things (IIoT) has gained significant traction. However, the open channel of communication, i.e., the Internet, poses security and privacy challenges for shared information. Existing solutions in the literature address these concerns but often suffer from high computation and communication overheads, limiting their applicability in IIoT environments. To bridge this gap, we propose a novel biometric-based privacy-preserving user authentication (BP2UA) scheme for cloud-based IIoT deployments. BP2UA ensures strong authentication between users and smart devices through pre-established key agreements, enhancing security. Formal and informal security analyses validate BP2UA's robustness against known attacks, while its computational and communication efficiency outperforms existing schemes. Practical validation using NS2 simulation further underscores BP2UA's effectiveness in real-world IIoT scenarios.

W. Yang *et al*

Biometric systems are increasingly favored over traditional authentication methods, prioritizing security and recognition accuracy. This paper offers a comprehensive review of recent advancements in fingerprint-based biometrics, focusing on enhancing security and accuracy. Through analysis and discussion, it highlights limitations in current research and suggests future directions. Addressing critical challenges like attacks on user interfaces and template databases remains a priority. Designing effective countermeasures to bolster security without compromising recognition accuracy is a key research area. Furthermore, ensuring reliable performance under non-ideal conditions is crucial and warrants special attention in system design. The paper also discusses emerging challenges and research trends in the field, underscoring the ongoing importance of biometric system advancements.

C.-C. Chang ***et al***

Online access is integral for delivering diverse services to users globally. Ensuring data confidentiality and integrity during exchanges is paramount. Since Lamport's pioneering work, several authentication mechanisms have emerged, aiming to enhance security and reduce computational overhead. Chuang and Chen introduced a multi-server authenticated agreement protocol, leveraging smart cards and biometric data, addressing vulnerabilities in traditional password-based systems. However, Mishra et al. identified weaknesses in this protocol, prompting the proposal of an enhanced three-factor authenticated key agreement protocol using Biohashing. Despite improvements, Mishra et al.'s scheme remains susceptible to various attacks and lacks user revocation mechanisms. In response, our novel scheme utilizes Hamming distance for biometric verification and incorporates a public-key technique for robust user revocation, ensuring both error-free authentication and resilience against known attacks.

Jingwei Li *et al*

As cloud computing advances, data outsourcing to cloud services gains popularity, offering relief from cumbersome data management. However, entrusting data to untrusted cloud storage raises security concerns, particularly regarding data integrity and deduplication. In this study, we address these issues by proposing two secure systems: SecCloud and SecCloud+. SecCloud employs an auditing entity within a MapReduce cloud, reducing user computation during data uploading and auditing. Meanwhile, SecCloud+ caters to users' encryption preferences, enabling integrity auditing and secure deduplication on encrypted data. These systems ensure both data integrity and deduplication in the cloud, enhancing security while accommodating user encryption needs. This research contributes to bolstering data security in cloud environments while streamlining user processes.

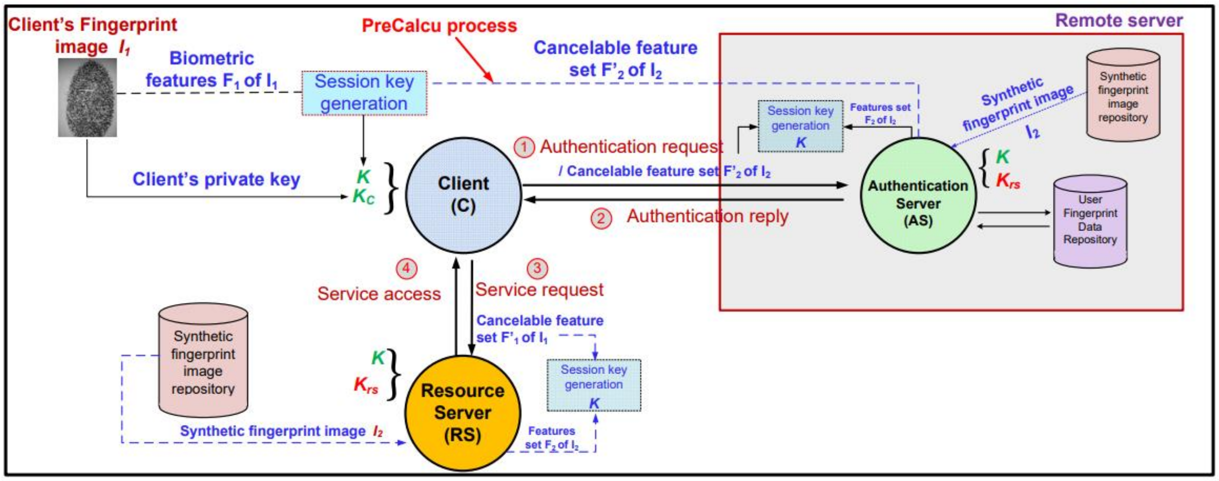
PROBLEM STATEMENT:

Various authentication mechanisms, such as Kerberos-based protocols, aim to establish secure delegated access between entities in a distributed system. Typically, these protocols rely on a trusted remote server for authentication. Users register with this server to ensure authorization. When accessing a server, both the user and server authenticate each other. However, existing mechanisms store user credentials on the authentication server, posing a security risk if compromised. Additionally, they often use symmetric key cryptography, necessitating key sharing during authentication. These limitations highlight the need for more secure and efficient authentication methods in distributed systems.

PROPOSED METHOD:

In our proposed approach, a user's fingerprint image serves as a secret credential. We derive a private key from this image, secretly enrolling it in the authentication server's database. During authentication, a new biometric fingerprint image is captured, generating a private key to encrypt the biometric data for query transmission to the server. Successful authentication grants access to the desired service server. Mutual authentication between the user and both servers is achieved using a short-term session key, generated efficiently from two fingerprint data. Additionally, a biometric-based message authenticator enhances message authenticity, ensuring secure and robust access to services.

ARCHITECTURE:


Client's Fingerprint image I_1
Biometric features F_1 of I_1
Session key generation
PreCalcu process
Cancelable feature set F'_2 of I_2
Remote server
Client's private key
K
K_C
Client (C)
① Authentication request / Cancelable feature set F'_2 of I_2
② Authentication reply
Session key generation K
Features set F_2 of I_2
Synthetic fingerprint image I_2
Synthetic fingerprint image repository
Authentication Server (AS)
K
K_{rs}
User Fingerprint Data Repository
④ Service access
③ Service request
Cancelable feature set F'_1 of I_1
Synthetic fingerprint image repository
K
K_{rs}
Resource Server (RS)
Session key generation K
Synthetic fingerprint image I_2
Features set F_2 of I_2

METHODOLOGY:

DATA OWNER:

Initially the data owner has to register to the cloud server and get authorized. After the authorization from cloud data owner will encrypt and add file to the cloud server where in after the addition of file data owner View All Uploaded Files, View All Transactions.

REMOTE SERVER

The remote server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users and performs the following operations such as View All Owners and Authorize,View All Users and Authorize ,View All Cloud Files ,View All Transactions ,View All Attackers ,View File Score Results ,View Time Delay Results ,View Throughput Results

Authenticate Server

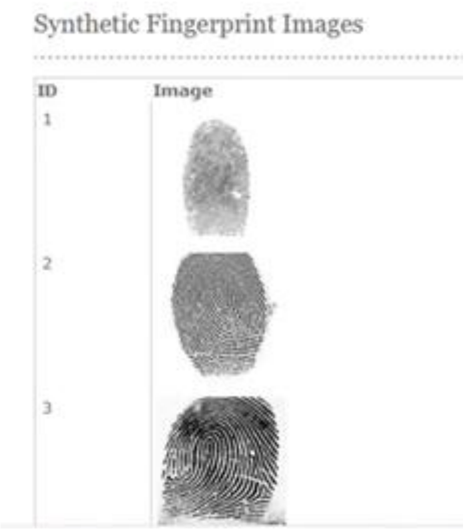
CA generates the content key and the secret key requested by the end user and also

View All Attackers.

Cleint

User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to View All Files ,Download.

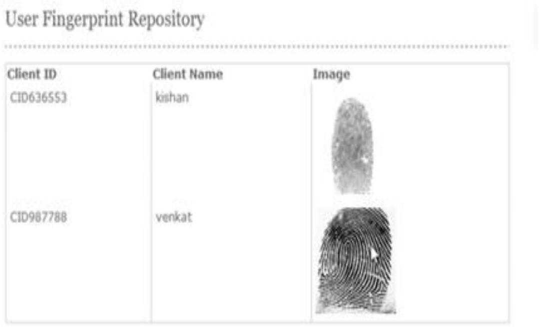
RESULTS:



Synthetic Fingerprint Images

ID	Image
1	
2	
3	

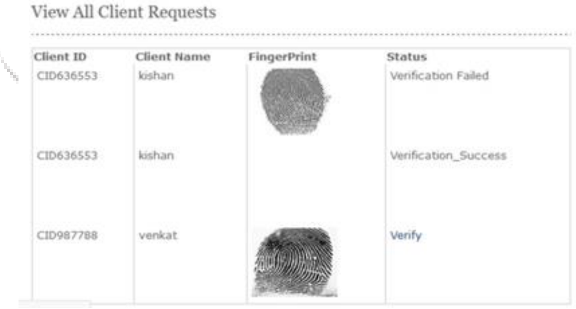
Synthetic Finger pint



User Fingerprint Repository

Client ID	Client Name	Image
CID636553	kishan	
CID987788	venkat	

User Finger Print Repository



View All Client Requests

Client ID	Client Name	FingerPrint	Status
CID636553	kishan		Verification Failed
CID636553	kishan		Verification_Success
CID987788	venkat		Verify

View All Client Requests

CONCLUSION

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks

REFERENCES:

[1] C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.

[2] “OAuth Protocol.” [Online]. Available: http://www.oauth.net/

[3] “OpenID Protocol.” [Online]. Available: http://openid.net/

[4] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.

[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : endto-end authorisation support for resource-deprived environments,” IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” Washington D.C., USA, October 2003, pp. 62–72.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.

[10] P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine, 2000.

[13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015.

[14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp.

1–13, 2013, Article ID 407971, http://dx.doi.org/10.1155/2013/407971.

[15] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.