iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 10 Issue: VII Month of publication: July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45249

A Substantiation and Key Agreement Based on Unidentified Identity for Peer-to-Peer Cloud

Dr. V. Anantha Krishna[1], K. Poornima[2], J. Vidhya[3], A. Navitha[4]
[1]*Professor, Dept of CSE, Sridevi Women's Engineering College, Hyderabad, Telangana, India*
[2, 3, 4]*B.Tech(CSE) IVth year, Sridevi Women's Engineering College, Hyderabad, Telangana, India*

Abstract: Real-time data collected by smart sensors deployed in factories is shared over open channels as the Industrial Internet of Things (IIoT) expands, posing a risk of unauthorised access to transmitted messages by adversaries, resulting in a privacy leakage problem. However, users frequently find it difficult to backup all data from the original cloud servers to their mobile phones in order to upload the downloaded data to the new cloud provider due to insufficient local storage and computational capabilities. To address this issue, it is proposed to gather information on the available solutions for the application of security issues in peer-to-peer networks, with a focus on authentication mechanisms.

Keywords: Cloud migration, Elliptic curve cryptography, Authentication, key exchange.

I. INTRODUCTION

People are increasingly reliant on devices such as smartphones and tablets. Every person can own and use multiple smart devices. It is also common for people to change their smart phones on a regular basis due to the fact that More inherent features from a variety of manufacturers are characterised by the new one. When people choose to use a different manufacturer's new smart device, the Data stored on the previous smart device provider's cloud server should be retrieved. transferred to the new smart device provider's cloud server This internet architecture does not require a centralised server. enables the ability to connect all participating nodes (peers) directly to communicate and disseminate data This research will look at the architecture of Peer-to-peer networks in general

II. EXISTING WORK

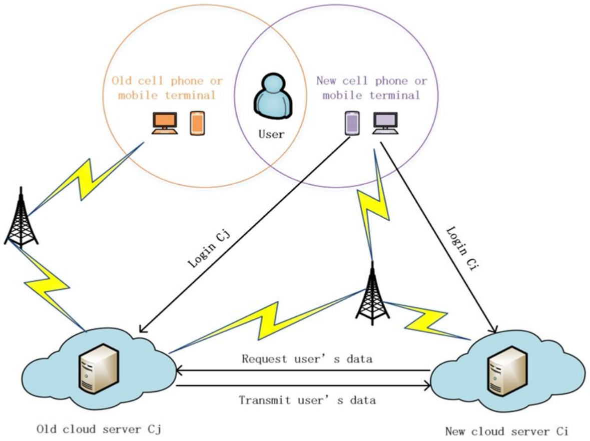
1) To assist users to gain authorization in access control contexts, property-based proxy re-encryption system. However, according to Liang and Au , this method lacks adaptive security and CCA security properties. A new proxy broadcast repeat encryption (PBRE) technique is proposed and demonstrated its security in a random oracle model under the choice n-BDHE hypothesis against the selective cypher text attack (CCA).
2) To overcome the key revocation problem, a broadcast agent encryption (RIBBPRE) security concept based on revocable identification is proposed. The agent can reverse a set of delegates provided by the principal from the re-encryption key in this RIB BPRE scheme. They also mentioned that the identity-based broadcast agent re-encryption (RIB-BPRE) techniques do not take use of cloud computing, which leads cloud users to be inconvenienced.

III. PROPOSED WORK

An anonymous three-factor authentication mechanism is presented, and biometric impression user authentication is improved. The following could be a list of contributions.

1) To begin, we present a three-factor user authenticated key-agreement system with ECC support.
2) Second, if an attacker falsifies a sensible card, the user's environment is jeopardised. In our protocol, both the client and the server verify users' biometric impressions; in some specific applications, this can provide security protection for specific requirements. Because RC is involved in the authentication process, the RC and server roles are distinct.
3) Although the proposed protocol requires more processing from the server, servers are typically expected to have sufficient resources. As a result, the server is easily accessible

Although the suggested protocol adds more processing to the server, servers are typically expected to have adequate resources. As a result, the server can easily handle these additional computations, lowering the user's computation cost. The system is built on a multi-server architecture that includes user (Uu), server (Sj), and registration centre (RC). RC facilitates user registration and also assists with the delivery of server services. To register all users, RC chooses its master secret key x. The suggested approach, like previous schemes, comprises three stages: authentication, registration, and password changing.



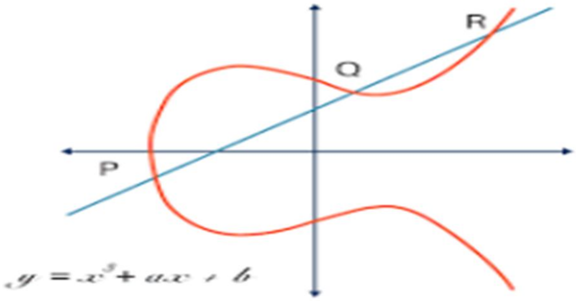
To preserve the privacy of service providers and customers, the suggested approach employs server anonymity. It's worth noting that for mutual authentication and key agreement, both of the cloud servers engaged in the migration process employ anonymous identities. This technique not only protects cloud service providers' identity privacy, but also prevents them from gaining superfluous information such as the brand of the users' old and new mobile phones. As a result, our methodology protects consumers' privacy by not disclosing their specific preferences.

IV. PREFATORY

A. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) The Elliptical Curve Cryptography (ECC) was introduced by Victor S. Miller and Neal Koblitz within the 80s, but it had been only within the late 90's that it began its application. ECC is predicated on the usage of finite field elliptic curves.

Moreover, a sum operation is defined 6 over an elliptical curve and a special item O is additionally defined because the identity element. Then, some extent G of the elliptical curve is defined as a base point and an elliptical curve is utilized for the sum operation of a number of elements (points).



Elliptical curve cryptosystems are predicated on the intractability of certain mathematical issues, even as the other public key system. Specifically, ECC is predicated on the ECDLP problem that asserts that it's inoperative to compute the discrete logarithm of a random elliptical curve in respect to a base point of an elliptical curve. Elliptic curve cryptography could be a key-based technique for encrypting data. ECC focuses on pairs of public and personal keys for decryption and encryption of web traffic

V. IMPLEMENTATION

A. Authentication and Key Exchange

Two aspects contribute to the commonly expected level of security for authenticated key-exchange (AKE) protocols. Authentication ensures the identities of the parties involved in protocol execution. Secrecy ensures that active adversaries are unaware of the key.

B. Server Registration Page

To become legitimate server Sj, the server needs to register with RC by following these steps.

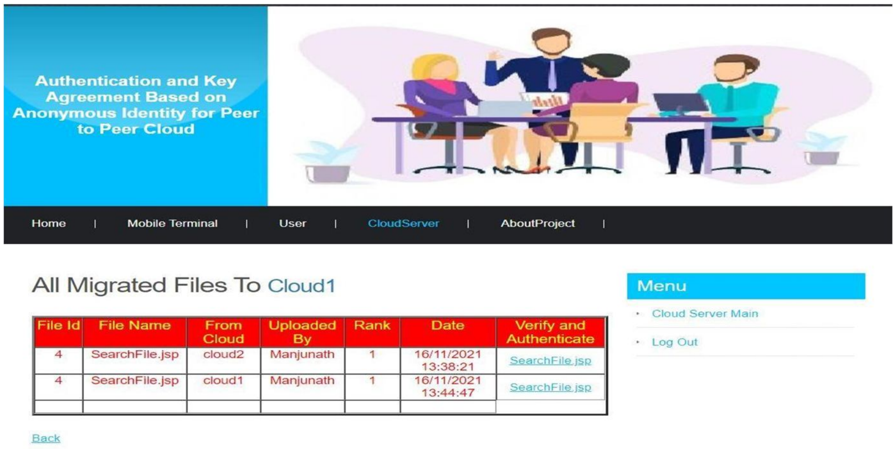
1) *SR Step1:* Sj selects his identity IDj and sends to RC through secure channel.
2) *SR Step2:* After receiving IDj, RC calculates s = h(IDj||x), pkSj = sP and pkRC = xP where x is secret key maintained by RC.
3) *SR Step3:* After that, RC sends s, pkSj , pkRC to server Sj and aborts the registration.

C. Mutual Authentication

The enhanced scheme provides mutual authentication because legitimate participants verify each other, ensuring strong mutual authentication. This property secures our protocol and allows for the early detection of potential attacks such as replay attacks.

VI. RESULTS

A. Migrated Files


Authentication and Key Agreement Based on Anonymous Identity for Peer to Peer Cloud
Home | Mobile Terminal | User | CloudServer | AboutProject |

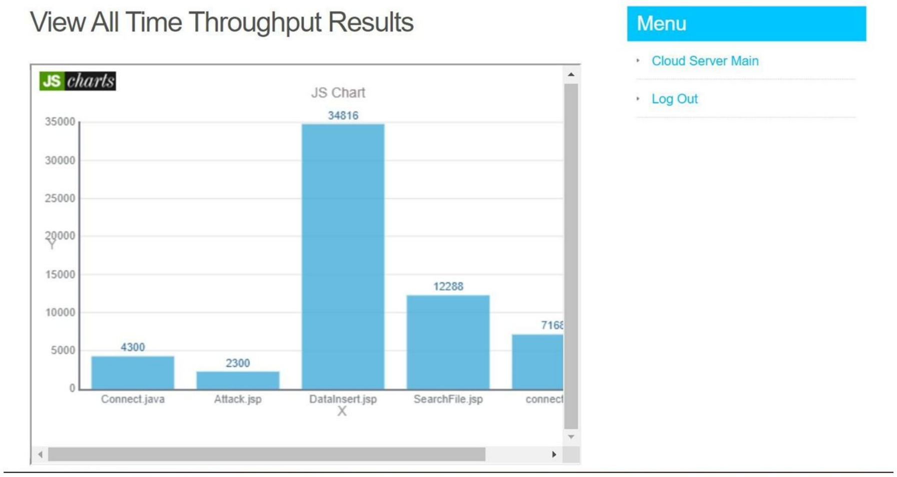
All Migrated Files To Cloud1

File Id	File Name	From Cloud	Uploaded By	Rank	Date	Verify and Authenticate
4	SearchFile.jsp	cloud2	Manjunath	1	16/11/2021 13:38:21	SearchFile.jsp
4	SearchFile.jsp	cloud1	Manjunath	1	16/11/2021 13:44:47	SearchFile.jsp

Back

Menu
- Cloud Server Main
- Log Out

B. Throughput Results



View All Time Throughput Results

Menu
- Cloud Server Main
- Log Out

VII. CONCLUSION

The study recommended employing a core contract protocol to communicate user data between multiple cloud servers. Three factors highlight the advantages of our system: security and value performance, cost projections, and communication costs. Our solution can address a fundamental trust issue while transiting data between cloud servers as well as cloud server anonymity. Our proposed technology protects users' privacy indirectly so as to safeguard cloud service providers' privacy.

REFERENCES

[1] C. I. network information center, “The 44th china statistical report on internet development,” http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/P020190830356787490958.pdf, 2019.

[2] B. Li, J. Li, and L. Liu, “Cloudmon: a resource-efficient iaas cloud monitoring system based on networked intrusion detection system virtual appliances,” Concurrency and Computation: Practice and Experience, vol. 27, no. 8, pp.a.1861–1885, 2015.

[3] J. Cui, H. Zhou, H. Zhong, and Y. Xu, “Akser: attribute-based keyword search with efficient revocation in cloud computing,” Information Sciences, vol. 423, pp. 343–352, 2018.

[4] J. Cui, H. Zhong, W. Luo, and J. Zhang, “Area-based mobile multicast group key management scheme for secure mobile cooperative sensing,” Science China Information Sciences, vol. 60, no. 9, p. 098104, 2017.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, “Ooabks: Online/offline attribute based encryption for keyword search in mobile cloud,” Information Sciences, vol. 489, pp. 63–77, 2019.

[6] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy reencryption with delegating capabilities,” in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009, pp. 276–286.

[7] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, “A secure and efficient ciphertext-policy attributebased proxy reencryption for cloud data sharing,” Future Generation Computer Systems, vol. a.52, pp. 95–108, 2015.