IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

Client Side Cryptography Based Security for Cloud Computing System

Ashok Kumar K, Sree Ram J, Andrew Pravin A, Prabakaran S, Syed Asrar Shah
Department of Computer Science and Engineering
Dhanalakshmi College of Engineering, Chennai

Abstract: The untrustworthiness of pall garçon and the data sequestration of druggies it's necessary to translated the data before outsource the pall Aiming to realize secure keyword hunt over translated data against vicious druggies and vicious pall service providers we find a compromised system by into the block chain into SSE the pall storehouse used in searchable symmetric encryption schemes(SSE) is handed in a private way, which can not be seen as a true pall. also, the pall garçon is allowed to be believable WE begin by pointing out the significance of storing the data in a public chain We introduce a system that leverages blockchain technology to give a secure distributed data storehouse with keyword hunt service The System allows the customer to upload their in translated form distributes the data content to pall bumps and insure data vacuity using cryptographic ways we introduce a system that leverages blockchain technology to give a secure distributed data storehouse with keyword hunt service. TKSE realizes garçon- side verifiability which protects honest pall waiters from being framed by vicious data possessors in the data storehouse phase. likewise, blockchain technologies and hash functions are used to enable payment fairness of hunt freights without introducing any third party indeed if the stoner or the pall is vicious. Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it's suitable for pall computing..

Keywords: Security for cloud computing systems based on client-side cryptography

I. INTRODUCTION

Cloud computing technology has evolved rapidly in recent years, and many studies have been conducted on cloud computing security issues such as: B. Access Control and Privacy. Cloud storage, a typical service of cloud computing, requires both data security and search capabilities. In fact, user-side verifiability takes into account the possibility that cloud servers are malicious. This means that the cloud server may return only partial search results or maliciously return incorrect results. User-side verifiability issues are first addressed in . However, these two schemes cannot support server-side verifiability and fair payments without a trusted third party. Additionally, server-side verifiability takes into account that data owners may be malicious. This means that data owners can maliciously offload invalid data during the data storage stage and fraudulently claim compensation later. This concern has not been addressed and receives little attention in the literature. Last but not least, most of the previous systems depended on banks. In particular, payment issues are not taken into account or default traditional payment mechanisms are abused, requiring the introduction of trusted third parties (TTPs) such as trusted banks for payment fairness. Paying fairly encourages honest behavior for users and cloud her servers[7]

II. LITERATURE SURVEY

[1] X. Chen, C. Jia, W. Lou, J. Li, J. Li, and X. Chen We deploy a hybrid private key for each user to accomplish this goal using a unique collusion-resistant method that uses an AND gate to connect and bind the identity component and the time component. In order to show the effectiveness of our suggested construction, we conclude by presenting extensive experimental findings. Their efforts were directed towards improving security, however they share the same drawback as Boldyreva's original building..

Raditional encryption methods, according to X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, can only partially address this issue because it is exceedingly challenging to do significant calculations over encrypted data. The building is safe from an attack by the FAU and is also publicly verifiable. Additionally, we demonstrate that our construction can achieve the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

desired security properties. The algorithm's clear drawback is that the outsourcer must perform additional costly operations like scalar multiplications and exponentiations.

H. Tian, J. He, F. Zhang, and H. Li One of the technological advancements that can be leveraged to reconcile the needs for both privacy and national security in information aggregation systems is the field of searchable encryption, according to DARPA. The issue of searchable symmetric encryption, which enables a client to store data on a remote server in a form that allows for private data searches, has been explored in this article. New security definitions and new developments are just two of the contributions we make. By establishing tighter definitions that ensure security even when users conduct more realistic searches, we alleviate this problem.

HG Do and W K Ng.The system enables clients to upload their data in encrypted form, distributes the data content across cloud nodes, and guarantees data availability using cryptographic methods. In the present work, we provide a system that uses blockchain technology to deliver a secure distributed data storage with keyword search function. The system enables clients to upload their data in encrypted form, distributes the data content across cloud nodes, and guarantees data availability using cryptographic methods. Additionally, it gives the data owner the option of allowing others to search through her data. The solution also allows for private keyword searches over the encrypted dataset. Hacks and manipulation are still a possibility.all transactions are final.

Q. Zhao, D. Zheng, H. Shi, and R. Guo. We formally establish the security of this attribute-based signature scheme in the random oracle model under the assumption of the computational bilinear Diffie-Hellman, including the attribute-signer's perfect privacy and invulnerability. In the random oracle model, this attribute-based signature scheme is secure. The comparison between the suggested approach and methods suggested in other studies demonstrates the effectiveness and attributes of each method. Revocation of users is not supported.

III. EXISTING SYSTEM

In addition, by using blockchain technology and hash functions, it is possible to fairly pay the search fee without going through a third party, even if the user or the cloud has malicious intent. With TKSE, an encrypted data index based on digital signatures allows users to search offloaded encrypted data and ensure that the search results returned from the cloud meet the prescribed search requirements. Security analysis and performance evaluation showed TKSE to be secure, efficient, and suitable for cloud His computing: First, His SSE scheme with user-side verifiability based on proposed. User verifiability also he implemented in SSE. It also realizes fair payments based on blockchain technology and hash functions without introducing TTP. Data confidentiality and privacy have been achieved, but identity privacy has been neglected. Low security. no data content .

IV. PROPOSED SYSTEM

To preserve searchability, we have developed encryption technologies that are searchable in two representative environments, including symmetric key settings. Also, this idea cannot be directly combined with blockchain technology, as the terms of redemption of search fees by the user and her CSP must be set. As a basic building block of information security, MAC private key cryptographic hash function servers are required and used in many applications. Security applications and - protocols used in all sorts of ways

- these are used for computer vision and storing passwords in databases. Here, SHA stands for Secure Hashing Algorithm to reduce data blocks and improve data security. Save data management costs. To protect user privacy and data security. message authentication code. integrity protection.

V. SYSTEM ARCHITECTURE

Client-side encryption-based security for cloud computing systems is an approach aimed at improving the security of cloud computing by encrypting data on the client side before uploading it to the cloud. This architecture can be described as follows. Client-side encryption: In this approach, client- side software or applications perform encryption before uploading data to the cloud. Encryption keys are generated and managed by the client, so your data remains safe even if your cloud provider is compromised. Cloud storage: Encrypted data is stored in the cloud by a cloud provider. Cloud providers cannot decrypt data without an encryption key that only the client can use. Secure communication: Use secure communication protocols such as SSL/TLS to ensure data remains secure during transit between the client and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

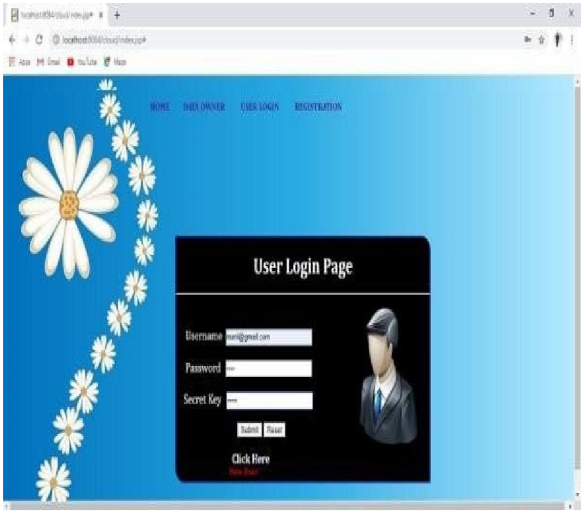
the cloud. Client-side decryption: A client-side software or application decrypts the data as it is retrieved from the cloud. This keeps your data safe even if it is intercepted in transit. Authentication and Authorization: To prevent unauthorized access, authentication and authorization mechanisms are implemented to ensure that only authorized users can access data. Overall, client-side encryption-based security provides an additional layer of security to cloud computing system architectures by encrypting data on the client side before uploading it to the cloud. This ensures data is safe even if the cloud provider is compromised and gives customers more control over their data.

VI. METHODOLOGY

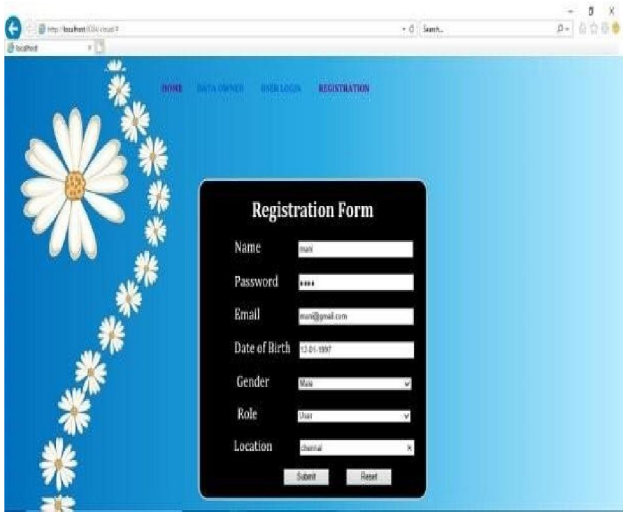
Methodologies for implementing client-side encryption-based security in cloud computing systems include selecting appropriate cryptographic algorithms, generating and managing cryptographic keys, implementing client-side encryption and decryption, and communicating , implementing authentication and authorization mechanisms, and testing and validating systems.

A. LOGIN

Websites, computer programmes, and mobile applications all need logins. They serve as a security mechanism to guard against unauthorised access to sensitive information. The user is denied access when a login attempt fails (i.e., the username and password entered do not correspond to an existing user account). After several unsuccessful attempts at logging in, many systems prevent users from even attempting to do so.



B. REGISTRATION



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

A person who has previously registered on a website, programme, or other system is referred to as a registered user. Logging in is the process by which registered users present the system with credentials (such as a username, email address, and password) to verify their identity. The majority of systems designed for public use enable any user to sign up by simply choosing a register or sign up function and entering these credentials for the first time. Additional rights may be granted to registered users over those given to unregistered users.

C. CREATE SECRETE KEY

Secure communication in the presence of third parties is practised and studied through the use of cryptography. In the past, encryption was the main focus of cryptography. Information that is plain text is transformed into cypher text through the process of encryption. Decryption is done in reverse. Information can be made secret from everyone but the intended receivers by using encryption. The pair of algorithms known as cyphers are used to create encryption and decryption. Operation of the cypher depends on the algorithm and the key. The secret that communicants are aware of is the key.

D. AUTHENTICATION SCHEME

It is used to address the issue of verifying the keys of the person (let's say "person B") that someone else ("person A") is conversing with or attempting to converse with. To put it another way, it is the procedure used to ensure that the key held by "person B" belongs to "person A" and vice versa. Although other algorithms disclose the keys at the time of authentication as well, this is often done after the keys have been transferred between the two sides over some secure channel. The easiest way to solve this issue is for the two users to meet in person and exchange keys. This is not practicable, though, for systems with lots of users or if the users don't know one another personally (like online buying). To address this issue, several algorithms are available for both symmetric keys and asymmetric public key cryptography.

E. TWO SIDE VERFICATION

In this module, two authentication methods are used sequentially to verify that the person or item requesting access is indeed who or what they claim to be. This procedure is known as two-side verification

VII. FUTURE SCOPE

Achieve high levels of security to deliver reliable computing and storage services. It provides data integrity, data confidentiality, authentication and authorization. Eliminate internal and external security threats. Avoid both active and passive attacks in cloud network environments. Achieve different levels of security in your cloud framework.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

VIII. CONCLUSION

In order to provide a safe distributed data storage with keyword search service, we introduce a system that makes use of blockchain technology. The system enables the client to upload their data in encrypted form, distributes the data content to cloud nodes, and ensures data availability using cryptographic techniques. With the help of TKSE, server-side verifiability is realised, preventing trustworthy cloud servers from being used as pawns by bad actors throughout the data storage phase. Additionally, even when a user or cloud is evil, payment fairness of search fees can be enabled without the introduction of a third party using block chain technologies and hash functions. Our security research and performance assessment show that TKSE is both secure and effective, making it appropriate for cloud computing.

REFERENCES

[1] J. Li,J. Li,X. Chen,C. Jia,W. Lou," Identity- Grounded Encryption with unloaded cancellation in Cloud Computing," IEEE Deals on Computers,vol. 64,No. 2,pp.425- 437, 2015

[2] X. Chen,J. Li,X. Huang,J. Ma, andW. Lou, " New intimately empirical databases with efficient updates, " IEEE Deals on reliable and Secure Computing,vol. 12,no. 5,pp. 546 – 556, 2015

[3] H. Tian, " A searchable symmetric encryption schemeusingblockchain, " arXivpreprint, 2017 H. Li,F. Zhang,J. .

[4] H.G.DoandW.K.Ng, " Blockchain grounded system forsecure datastorage with private keyword hunt, " in Services(SERVICES), 2017IEEEWorld Congress on. IEEE, 2017,pp. 90 – 93.

[5] R. Guo,H. Shi,Q. Zhao, andD. Zheng, " Secure trait- grounded hand scheme with multiple authorities for blockchain in electronic health records systems, " IEEE Access,vol. 776,no. 99,pp. 1 – 12, 2018.

[6] Securing Cloud Data with customer- Side Cryptography" by Min Xu and Kwok- Yan Lam(2013 IEEE 14th International Conference on High Performance Computing and Dispatches & 2013 IEEE 9th transnational Conference on Bedded Software and Systems)

[7] Client-Side Encryption for Cloud Storage: An Empirical Study" by Mohammed AlZain and Simon Foley (2018)

[8] Privacy-Preserving Data Sharing in Cloud Computing using Client-Side Cryptography" by Lila Boukhatem, et al.2017

[9] Client-Side Encryption for Secure Cloud Storage" by Martin Mulazzani, et al. (2012 IEEE)

[10] "Client-Side Encryption for Cloud Storage Services" by Hassan Takabi and James B. D. Joshi (2014 IEEE)