International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Novel Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage SystemsFor Better Security

Mrs.Vidyaswarupa S [1] ,Mr. P.Kartheek[2]

#1Student,Department of CSE, MalineniLakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India

#2Assistant Professor, Department of CSE, MalineniLakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India

Abstract__Data integrity, a core safety problem in dependable cloud storage, has obtained tons attention. Data auditing protocols allow a verifier to efficaciously take a look at the integrity of the outsourced statistics besides downloading the data. A key lookup undertaking related with present designs of statistics auditing protocols is the complexity in key management. In this paper, we are seeking for to tackle the complicated key administration project in cloud records integrity checking with the aid of introducing fuzzy identity-based auditing, the first in such an approach, to the satisfactory of our knowledge. More specifically, we existing the primitive of fuzzy identity-based statistics auditing, the place a user's identification can be considered as a set of descriptive attributes. We formalize the device mannequin and the safety mannequin for this new primitive. We then current a concrete development of fuzzy identity-based auditing protocol by using utilising biometrics as the fuzzy identity. The new protocol provides the property of error-tolerance, namely, it binds with non-public key to one identification which can be used to confirm the correctness of a response generated with some other identity, if and solely if each identities are sufficiently close. We show the safety of our protocol based totally on the computational Diffie-Hellman assumption and the discrete logarithm assumption in the selective-ID protection model. Finally, we enhance a prototype implementation of the protocol which demonstrates the practicality of the proposal.

1.INTRODUCTION

Big data is eliciting attention from the academia as well as the industry. Over 2.5 quintillion bytes of data are reportedly created every day in the world, so much that 90% of the data has been created in the last two years alone. The explosive growth in the volume of data captured by the machines, sensors, IoT and other means, has changed our lifestyle gradually. According to a prediction by IDC (International Data Corporation), data set will grow 10-fold by the year of 2020 and there will be 5,200 GB of data for every person on earth 1 . Traditional storage model cannot meet the people's requirements due to the increasing large amount of data, which leads to the emergence of cloud storage. As a basic service of IaaS (Infrastructure as a service) model in cloud computing [1], cloud storage enables data owners to store their files to the cloud and deletes the local copy

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

of the data, which dramatically reduces the burden of maintenance and management of the data. Cloud storage has a number of eye-catching features [2], say global data access, independent geographical locations, on demand selfservice, resource elasticity and so on. Currently, both the individuals and big companies are enjoying the benefits due to cloud storage services

2.LITERATURE SURVEY

1) DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party

AUTHORS: Ali, M., Malik, S. and Khan, S.,

Off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud. Wholesale of data by cloud service provider is yet another problem that is faced in the cloud environment. Consequently, high-level of security measures is required. In this paper, we propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a data security system that provides (a) key management (b) access control, and (c) file assured deletion. The DaSCE utilizes Shamir's (k, n) threshold scheme to manage the keys, where k out of n shares are required to generate the key. We use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of failure for the cryptographic keys. We (a) implement a working prototype of DaSCE and evaluate its performance based on the time consumed during various operations, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) verify the working of DaSCE using Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The results reveal that DaSCE can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion.

2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the Attribute-Based Encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy but

also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi-anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControlF which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the DBDH assumption, and our performance evaluation exhibits the feasibility of our schemes.

3) Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

AUTHORS: Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J

In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

4) Jobber: Automating inter-tenant trust in the cloud

AUTHORS: Sayler, A., Keller, E. and Grunwald, D

Today, a growing number of users are opting to move their systems and services from self-hosted data centers to cloud-hosted IaaS offerings. These users wish to both benefit from the efficiencies that shared multitenant hosting can offer while still retaining or improving the kinds of security and control afforded by self-hosted solutions. In this paper, we present Jobber: a highly autonomous multi-tenant network security framework designed to handle both the dynamic nature of cloud datacenters and the desire for optimized inter-tenant communication. Our Jobber prototype leverages principals from Software Defined Networking and Introduction Based Routing to build an inter-tenant network policy solution capable of automatically allowing optimized communication between trusted tenants while also blocking or rerouting traffic from untrusted tenants. Jobber is capable of automatically responding to the frequent changes in virtualized data center topologies and, unlike traditional security solutions, requires

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

minimal manual configuration, cutting down on configuration errors.

4.PROPOSED SYSTEM

The proposed protocol revolutionizes key management in traditional remote data integrity checking protocols. We also presented the the system and security models for this primitive, and a concrete fuzzy identity based data integrity auditing protocol using the biometric based identity as an input. We then demonstrated the security of the protocol in the selective-ID model. The prototype implementation of the protocol demonstrates the practicality of the proposal. Future work includes implementing and evaluating the proposed protocol in a real-world environment.

Proposed the concept of remote data integrity checking (RDIC, is also known as data integrity auditing), which comprises three parties, namely: cloud server, data owner and third party auditor (TPA). A publicly verifiable RDIC protocol allows the TPA or anyone to check the integrity of the stored data on the cloud without the need to retrieve the entire dataset.

The concept of proof of retrievability (POR), as well as providing a construction based on short signature algorithm and proving its security in the random oracle model. A number of remote data integrity checking protocols have been proposed catering to different real world requirements, such as dynamic operation privacy-preserving and publicly auditing .

The secret key to the user's identity, without the need for a digital certificate. Since then, a number of ID-based schemes (including remote data auditing protocols) have been proposed. example, several ID-based remote data auditing protocols were proposed and in these protocols, identity information is an arbitrary text string. The latter comprises user's name, IP address and E-mail address, which allows a user to register for a private key corresponding to his identity from the private key generation center.

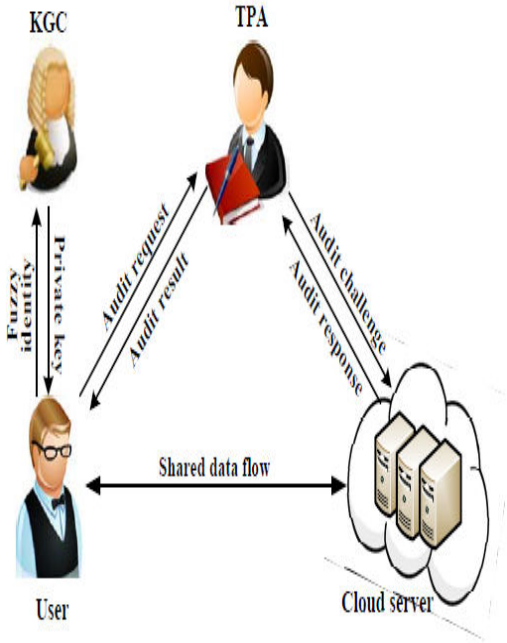

Fig 1:Architecture

Data Owner:

The client wants to upload new files to the cloud, it needs to verify the validity of the encrypted secret key

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

from the cloud and recover the real secret key. We show the time for these two processes happened in different time periods. They only happen in the time periods when the client needs to upload new files to the cloud. Furthermore, the work for verifying the correctness of the encrypted secret key can fully be done by the cloud

TPA Auditing:

TPA to check the integrity of the stored data on the cloud without the need to retrieve the entire dataset.A HVT aggregates response of the challenged blocks into a single value, which significantly reduces the communication costs between the server.TPA is the trusted entity designated to verify the cloud data's integrity on behalf of the cloud user upon request.

TPA and cloud server run a challenge response protocol for data integrity auditing to determine if the stored data are intact. Homomorphism and allows the TPA to detect the corruption of the file F in cloud without heavy communication overhead.TPA samples on the blocks of the file M to generate a challenge chal and sends chal to the cloud server. According to the challenge, the server generates proof resp by aggregating the challenged blocks and the corresponding authenticators in the Response algorithm. Finally, the TPA verifies the response resp to determine whether the file F is intact on the cloud.

Server:

That is to say, it is the cloud servers who control the fate of the data after the data owners uploading their files to the cloud. While most cloud service providers are honest (e.g. due to their vested interest in ensuring a good reputation and avoiding civil litigations), data loss incidents are inevitable. As a consequence, data owners require a strong integrity guarantee of their outsourced data and they want to make sure that the cloud servers store their data correctly. Therefore, cloud data integrity is of particular importance in secure and reliable cloud storage.

A HVT aggregates response of the challenged blocks into a single value, which significantly reduces the communication costs between the server and the TPA.In the schemes discussed above, the data owner has a pair of public/private keys (pk and sk respectively), where sk is used to generate authenticators of blocks and pk is used to verify a proof generated by the cloud server.

Finally, both TPA and cloud server run a challenge response protocol for data integrity auditing to determine if the stored data are intact.

Data Sharing:

The shared data are signed by a group of users. Therefore, disputes between the two parties are unavoidable to a certain degree. So an arbitrator for dispute settlement is

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

indispensable for a fair auditing scheme. We extend the threat model in existing public schemes by differentiating between the auditor (TPAU) and the arbitrator (TPAR) and putting different trust assumptions on them. Because the TPAU is mainly a delegated party to check client's data integrity and the potential dispute may occur between the TPAU and the CSP, so the arbitrator should be an unbiased third party who is different to the TPAU.

As for the TPAR, we consider it honest-but-curious. It will behave honestly most of the time but it is also curious about the content of the auditing data, thus the privacy protection of the auditing data should be considered. Note that, while privacy protection is beyond the scope of this paper, our scheme can adopt the random mask technique proposed for privacy preservation of auditing data, or the ring signatures in to protect the identityprivacy of signers for data shared among a group of users.

Auditing:

Public auditing schemes mainly focus on the delegation of auditing tasks to a third party auditor (TPA) so that the overhead on clients can be offloaded as much as possible. However, such models have not seriously considered the fairness problem as they usually assume an honest owner against an untrusted CSP. Since the TPA acts on behalf of the owner, then to what extent could the CSP trust the auditing result? What if the owner and TPA collude together against an honest CSP for a financial. In this sense, such models reduce the practicality and applicability of auditing schemes.

Secret Key Update:

The key update workload is outsourced to the TPA. In contrast, the client has to update the secret key by itself in each time period in scheme. We compare the key update time on client side between the both schemes the key update time on the client is related to the depth of the node corresponding to the current time period.Outsource key updates for cloud storage auditing with key-exposure resilience.

Cloud storage auditing protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the TPA and are transparent for the client. In addition, the TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. We give the formal security proof and the performance simulation of the proposed scheme.

User:-

Identity can be viewed as a set of descriptive attributes. We formalize the system model and the security model for this new primitive. We then present a concrete construction of fuzzy

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

identity-based auditing protocol by utilizing biometrics as the fuzzy identity. The new protocol offers the property of error-tolerance, namely, it binds with private key to one identity which can be used to verify the correctness of a response generated with another identity, if and only if both identities are sufficiently close.

User data may be lost due to deliberate deletion by cloud servers in order to make the available storage space for other files to get more profit. A survey reported that 43% of the respondents had lost their outsourced data and had to resort to recovering the data from backups. Data loss incident happens frequently in reality and has been regarded as one of the key security concerns in cloud storage.

A registration authority that validates the identity of users requesting information from the CA, a central directory, and a certificate management system.The secret key to the user's identity, without the need for a digital certificate. Since then, a number of ID-based schemes (including remote data auditing protocols) have been proposed.

The user's identity may not be truly unique if the identity information is not chosen properly (e.g. using a common name such as "John Smith"). Secondly, a user needs to "prove" to the private key generator centre that he is indeed entitled to a claimed identity, such as presenting a legal document supporting the claim.

4.CONCLUSION

Cloud storage offerings have end up an more and more necessary phase of the statistics science enterprise in current years. Thus, making sure the integrity of records outsourced to the cloud is of paramount importance. In this paper, we introduced the first fuzzy identity-based records integrity auditing protocol. The proposed protocol revolutionizes key administration in regular far off facts integrity checking protocols. We additionally introduced the the machine and safety fashions for this primitive, and a concrete fuzzy identitybased information integrity auditing protocol the usage of the biometricbased identification as an input. We then established the protection of the protocol in the selective-ID model. The prototype implementation of the protocol demonstrates the practicality of the proposal. Future work consists of imposing and evaluating the proposed protocol in a real-world environment.

REFERENCES

[1] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Roadmap Working Group, SP 500-291-v1.0, NIST, Jul, 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech. Rep.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

[3] Y. Deswarte, J. J. Quisquater and A. Saidane."Remote integrity checking".Integrity and Internal Control in Information Systems VI.Springer US, pp.1-11, 2004.

[4] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson and D. X. Song, "Provable data possession at untrusted stores," in Proc. of ACM Conference on Computer and Communications Security, pp.598-609, 2007.

[5] G. Ateniese, S. Kamara and J. Katz."Proofs of storage from homomorphic identification protocols".Proc. of ASIACRYPT, pp.319-333, 2009.

[6] R. L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems".Communications of the ACM, 21(2), pp.120-126, 1978.

[7] H. Shacham and B. Waters, "Compact proofs of retrievability," Proc. of Cryptology-ASIACRYPT, 5350, pp.90-107, 2008.

[8] D. Boneh , B. Lynn, and H. Shacham, "Short signatures from the weil pairing", In Proc. of Asiacrypt 2001, pp.514-532, 2001.

[9] C. C. Erway, A. Kupcu and C. Papamanthou."Dynamic provable data possession".ACM Transactions on Information and System Security (TISSEC), 17(4), 15, 2015.

[10] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing".Proc. of ESORICS2009, LNCS 5789, pp.355-370, 2009.

Author's Profile

Mrs.Vidyaswarupa S, as M.Tech student in the department of CSE at MalineniLakshmaiah Engineering College, Kanumalla. She has completed B.Tech from JNTUK. Her areas of interests are Cloud Computing,Object Oriented Language, web technologies and AWS.

P.Kartheek Currently working as Assistant Professor in Computer Science and Engineering department in MALINENI LAKSHMAIAH ENGINEERING COLLEGE, singarayakonda