JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-5 (May-2019)
ISSN (O) :- 2581-6934

Enabling Efficient User Revocation and Unblocking of Authorized User

Ms. M. Sukumari ME [1] , R.M.SaravanaPriya ME [2]

[1] Assistant professor, [2] Student

[1 2] Department of Computer Science and Engineering, Rajas International Institute of Technology for women

Abstract— Cloud storage auditing schemes for shared data refer to checking the integrity of cloud data shared by a group of users. User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for user revocation in such schemes is linear with the total number of file blocks possessed by a revoked user. The overhead, however, may become a heavy burden because of the sheer amount of the shared cloud data. Thus, how to reduce the computational overhead caused by user revocations becomes a key research challenge for achieving practical cloud data auditing. A novel storage auditing scheme that achieve highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud was proposed. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, user revocation by just updating the non-revoked group users' private keys rather than authenticators of the revoked user was realized. The integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated. Meanwhile, the proposed scheme is based on identity-base cryptography, which eliminates the complicated certificate management in traditional Public Key Infra structure (PKI) systems. The security and efficiency of the proposed scheme are validated via both analysis and experimental results.

Index Terms—Cloud computing; cloud storage auditing; user revocation; big data; identity-based cryptography

INTRODUCTION

1.1 COMPUTER SECURITY

Computer security, cybersecurity or IT security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. The field is of growing importance due to increasing reliance on computer systems, the Internet and wireless networks such as Bluetoothand Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions and the various tiny devices that constitute the Internet of Things. Due to its complexity, both in terms of politics and technology, it is also one of the major challenges of the contemporary world.

1.2 CLOUD COMPUTING

Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance. Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. *Cloud computing* is shared pools of configurable *computer* system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. *Cloud computing* relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT

teams to more rapidly adjust resources to meet fluctuating and unpredictable demand. The field is of growing importance due to increasing reliance on computer systems. Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.

SECURITY IN CLOUD COMPUTING

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

SECURITY AND PRIVACY

Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud ID, for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

Privacy

Providers ensure that all critical data are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

LITERATURE SURVEY

2.1 Privacy-Preserving Public Auditing for Shared Data in The Cloud

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. A novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud was proposed. In particular, exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With the mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, this mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. The experimental results demonstrate the effectiveness and efficiency of this mechanism when auditing shared data integrity.

2.2Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability

Cloud storage service has been widely adopted by diverse organizations, through which users can conveniently share data with others. For security consideration, previous public auditing schemes for shared cloud data concealed the identities of group members. However, the unconstrained identity anonymity will lead to a new problem, that is, a group

ISSN:-2581-6934|www.jidps.com

member can maliciously modify shared data without being identified. Since uncontrolled malicious modifications may wreck the usability of the shared data, the identity traceability should also be retained in data sharing. An efficient public auditing solution that can preserve the identity privacy and the identity traceability for group members simultaneously was proposed. Specifically, first design a new framework for data sharing in cloud, and formalize the definition of the public auditing scheme for shared cloud data supporting identity privacy and traceability. And then construct such a scheme, in which a group manager is introduced to help members generate authenticators to protect the identity privacy and two lists are employed to record the members who perform the latest modification on each block to achieve the identity traceability. Besides, the scheme also achieves data privacy during authenticator generation by utilizing blind signature technique. Based on the proposed scheme, further design an auditing system for practical scenarios. Finally, the proposed scheme is secure based on several security requirements, and justify its performance by concrete implementations.

2.3PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN THE CLOUD

With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud.

A novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind was proposed. By utilizing the idea of proxy re-signatures, allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that this mechanism can significantly improve the efficiency of user revocation.

2.4 PUBLIC INTEGRITY AUDITING FOR DYNAMIC DATA SHARING WITH MULTIUSER MODIFICATION

The rapid development of cloud storage services makes it easier than ever for cloud users to share data with each other. To ensure user's confidence of the integrity of their shared data on cloud, a number of techniques have been proposed for data integrity auditing with focuses on various practical features, e.g., the support of dynamic data, public integrity auditing, low communication/computational audit cost, and low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read-only applications. Recently, a few attempts started considering more realistic scenarios by allowing multiple cloud users to modify data with integrity assurance. Nevertheless, these attempts are still far from practical due to the tremendous computational cost on cloud users, especially when high error detection probability is required by the system. A novel integrity auditing scheme for cloud data sharing services characterized by multiuser modification, public auditing, high error detection probability, efficient user revocation as well as practical computational/communication auditing performance was proposed.

This scheme can resist user impersonation attack, which is not considered in existing techniques that support multiuser modification. Batch auditing of multiple tasks is also efficiently supported in this scheme. Extensive experiments on Amazon EC2 cloud and different client devices (contemporary and mobile devices) show that this design allows the client to audit the integrity of a shared file with a constant computational cost of 340 ms on PC (4.6s on mobile device)

ISSN:-2581-6934|www.jidps.com

and a bounded communication cost of 77 kB for 99% error detection probability with data corruption rate of 1%.

2.5 Efficient Integrity Auditing for Shared Data in The Cloud with Secure User Revocation

With the cloud storage services, users can easily form a group and share data with each other. Given the fact that the cloud is not trustable, users need to compute signatures for blocks of the shared data to allow public integrity auditing. Once a user is revoked from the group, the blocks that were previously signed by this revoked user must be re-signed by an existing user, which may result in heavy communication and computation cost for the user. Proxy re-signatures can be used here to allow the cloud to do the re-signing work on behalf of the group. However, a malicious cloud is able to use the re-signing keys to arbitrarily convert signatures from one user to another deliberately. Moreover, collusions between revoked users and a malicious cloud will disclose the secret values of the existing users. A novel public auditing scheme for the integrity of shared data with efficient and collusion-resistant user revocation utilizing the concept of Shamir secret sharing was proposed. Besides, this scheme also supports secure and efficient public auditing due to this improved polynomial-based authentication tags. The numerical analysis and experimental results demonstrate that proposed scheme is provably secure and highly efficient.

2.6 IRIBE: INTRUSION-RESILIENT IDENTITY-BASED ENCRYPTION

In order to limit the damage of key exposure for identity-based encryption, a new paradigm called intrusion-resilient identity-based encryption (IRIBE) was. Compared with key-insulated identity-based encryption and forward-secure identity-based encryption, IRIBE can achieve a stronger level of security. In the proposed scheme, the cipher texts in any other time periods are secure even after arbitrarily many compromises of the base and the user, as long as compromises do not happen simultaneously. Furthermore, the intruder cannot decrypt the cipher texts pertaining to previous time periods, even if it compromises the base and the user simultaneously. Therefore, the proposed IRIBE scheme can greatly enhance the security of identity-based encryption. Formalize the definition and the security notions of this paradigm. The proposed scheme is proven secure in the standard model.

3. System Analysis

3.1 Existing System

In cloud storage auditing schemes, the data owner needs to use his/her private key to generate authenticators (signatures) for file blocks. These authenticators are used to prove that the cloud truly possesses these file blocks. When a user is revoked, the user's private key should also be revoked. For traditional cloud storage auditing schemes for share data all of authenticators generated by the revoked user should be transformed into the authenticators of one designated non revoked group user. This non-revoked group user needs to download all of revoked user's blocks, re-sign these blocks, and upload new authenticators to the cloud.

3.1.1 Disadvantages

- Unblocked users cannot upload the data.
- Need authenticators for uploading data.
- Costs of computation resource is high.

3.2 Proposed System

In this proposed system, a novel cloud storage auditing scheme was constructed for shared data supporting real efficient user revocation. In order to realize efficient user revocation, strategy for key generation is used. In this design, the group's public key is replaced by the group's identity information, which remains unchanged in the whole lifetime. The group's private key derives from two components. One component remains fixed since being issued, and the other component alters with user revocation.

A novel private key is used to support user revocation. When users are revoked from the group, all of the non-revoked users can update their private keys by this technique to make the cloud storage auditing still work, while the identity information of the group does not need to change. In addition, the revoked users are not able to upload data and authenticators to the cloud any more. In this way, all of the authenticators generated before user revocation do not need to be recomputed. Therefore, the overhead of user revocation is

ISSN:-2581-6934|www.jidps.com

fully independent of the total number of the revoked user's blocks. Even when the amount of data is immense, the group can still complete user revocation very efficiently. Besides, this scheme is based on identity-based cryptography, which eliminates the complicated certificate management in traditional PKI systems, including certificate generation, certificate revocation, certificate renewal, etc. The correctness and the security of the proposed scheme is proved by concrete analysis.

3.2.1 Advantages

- It supports real efficient user revocation.
- Independent in number of revoked user blocks.
- High security

System Design

System design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. System design could be seen as the application of system theory to product development. There is some overlap with the disciplines of system analysis, system architecture and system engineering. System design provide the following designs,

Architectural design

The architectural design of a system emphasizes the design of the system architecture that describes the structure, behavior and more views of that system and analysis.

Logical design

The logical design of a system pertains to an abstract representation of the data flows, inputs and outputs of the system. This is often conducted via modelling, using an over-abstract model of the actual system. Logical design includes entity-relationship diagrams.

Physical design

The physical design relates to the actual input and output processes of the system. This is explained in terms of how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed.

4 SYSTEM IMPLEMENTATION

4.1 MODULES

Private Key Generation

The PKG generates the master secret key, the master partial key and the system public parameters. The PKG randomly chooses the master secret key which is used to generate the identity key for group users. The PKG holds the master secret key itself. The PKG randomly chooses the master partial key which is sent to the group manager for generating the partial key. After receiving the group ID, the PKG sets the identity key and send it to the group user. Group user can verify the correctness of the identity key. The group manager generates the partial key and provided to the user. Then finally user verify the correctness of the partial key and then the private key was generated.

Authenticator Generation

The group user computes an authenticator for each block mi of file F, and generates a file tag to ensure the integrity of the file identifier name, verification values R_{ID} and R_{RN}, and the number of user revocations RN. The group user uploads the file F and the set of authenticators along with the file tag to the cloud. Finally, the cloud verifies the correctness of authenticators as follows, the group user computes the authenticators by using the name of the file, index of the block, number of user revocation. Then the authenticators are computed. The group users compute the file tag and upload the file along with the file tag in the cloud and delete the file from the local storage. The cloud verifies the validity of the file tag and authenticators. The cloud checks whether RN in the file tag is the newest RN. If it is, the cloud does the following two steps otherwise, the cloud regards the user as a revoked user or an illegal user and refuses this user's request. The cloud verifies the validity of the file tag by checking whether the signature is a valid signature via ID. The cloud verifies the authenticator is valid otherwise they are from the revoked users.

ISSN:-2581-6934|www.jidps.com

Auditing

TPA generates an auditing challenge for the cloud. The cloud generates a corresponding proof to demonstrate that possesses the intact cloud data. Sends the auditing challenge chal = $\{i,V_i\}$ $i\epsilon I$ to the cloud. After receiving the auditing challenge chal from the TPA, the cloud generates a proof of data possession as follows: It sends P along with TPA as a file tag to the cloud. The TPA verifies the correctness of the proof from the cloud. The TPA first retrieves the file tag, and verifies the validity of the file tag by checking whether it is a valid signature via ID. If it is, the TPA parses name, RN, R_{ID} and R_{RN}. Then the TPA verifies the correctness of proof by providing the success or failure output.

User Revocation

When group users are revoked, the group manager and non-revoked group users will execute this algorithm. The number of user revocations RN increases by one. The group manager generates a new partial key according to the new RN, and each non-revoked group user updates his/her private key according to the new partial key. The revoked group users cannot upload the new data to the cloud any more. The process of user revocation is, when group users are revoked, the group manager sets the number of user revocations and sends this message to non-revoked group users and the cloud. The group manager set the partial key and send to the non-revoked users in the group. After receiving the new partial key the non-revoked users compute the new private kay and upload the data in the cloud. The revoked users do not have the new private key, so they cannot generate valid authenticators of blocks corresponding to the newest RN. When a revoked user uploads new data to the cloud, he/she will not be able to pass the verification of step in Authenticator Generation algorithm. Therefore, the revoked user is not able to upload new data to the cloud any more.

Conclusion and Future Enhancement

8.1 CONCLUSION

In this project, an identity-based cloud storage auditing scheme was proposed for shared data, which supports real efficient user revocation. In this scheme, the cloud or the non-revoked user does not need to re-sign any file blocks of the revoked user. The overhead of user revocation scheme is fully independent of the number of the revoked user's blocks. Security proof and experimental results show that the proposed scheme is secure and efficient.

8.2 FUTURE ENHANCEMENT

In the proposed system, it need to generate the new partial key for the new non revoked users, if the key was missed then the user cannot upload the file so the One Time Password(OTP) was generated to the authorized user to avoid the missing of key.

REFERENCES

[1]. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng (2015), "Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation," IEEE Trustcom/BigDataSE/ISPA, pp. 434-442.

[2]. B. Wang, B. Li, and H. Li (2012), "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," In Proc. of IEEE Cloud 2012, pp. 295-302.

[3]. B. Wang, B. Li, and H. Li (2015), "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106.

[4]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao (2016). "Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability," Journal of Systems and Software, vol. 113, pp. 130-139.

[5]. J. Yu, R. Hao, H. Zhao, M. Shu, and J. Fan (2016), "IRIBE: Intrusion-resilient identity-based encryption," Information Sciences, vol. 329, pp. 90-104.

[6]. Y. Yu, M. Au, G. Ateniese, X. Huang, W. Susilo, Y.Dai, and G. Min (2016), "Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage," IEEE Transactions on Information Forensics and Security, vol.12, no.4, pp. 767-778.

[7]. J. Yuan and S. Yu (2015), "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726.