ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Security Issues of Cloud Computing- A Survey

Lal Vikram Singh[1]
Department of Computer Science
Pondicherry University, India

Amol V. Bole[2]
Department of Computer Science
Pondicherry University, India

Shailesh Kumar Yadav[3]
Department of Computer Science
Pondicherry University, India

Abstract: ***Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends information technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model.***

In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

Keywords: cloud computing, data sharing, privacy- preserving, access control, dynamic groups.

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In the cloud computing the cloud service providers (CSP) provide different types of services such as Infrastructure, data storage, software etc.

As the demand for cloud computing increases, security and privacy will become more critical. Cloud security and privacy provides broad coverage of terms and definition to help both IT and Information professionals. There have been many attempts to understand cloud computing and illustrate the security issues involved with such technologies. By utilizing the cloud, the office staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Designing an efficient and secure Data sharing scheme for group in the cloud is not easy task due to following reasons

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be will not to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.

Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company.

Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

II. LITERATURE SURVEY

In [1], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. . However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

In [2], files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated.

In their extension version, the NNL construction [3] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale.

Ateniese et al. [4] leveraged proxy reencryptions to secure distributed storage. specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

In [5], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegate's tasks of data file re-encryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Lu et al. [6] proposed a secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs

encrypted data with her group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

In Xuefeng Liu, Yuqing Zhang [7] Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud In this paper, they propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

In Cong Wang & Kui Ren [8] Privacy-Preserving Public Auditing for Secure Cloud Storage enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, a secure cloud storage system supporting privacy-preserving public auditing. They further extend result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. In C´ecile Delerabl´ee & Pascal Paillier [9] Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Cipher texts or Decryption Keys. This paper puts forward new efficient constructions for public-key broadcast encryption that simultaneously enjoy the following properties: receivers are stateless; encryption is collusion- secure for arbitrarily large collusions of users and security is tight in the standard model; new users can join dynamically i.e. without modification of user decryption keys nor cipher text size and little or no alteration of the encryption key. We also show how to permanently revoke any subgroup of users. Most importantly, our constructions achieve the optimal bound of O(1)-size either for cipher texts or decryption keys, where the hidden constant relates to a couple of elements of a pairing- friendly group.

III. PARAMETERS FOR ANALYSIS

There are certain inherent requirements that must be met by any Security protocol developed for the cloud computing. We present these parameters below:

A) Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

B) Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

C) Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

D) Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

IV. ANALYSIS

In this section we will analyses the various protocols that have been developed for Security against the parameters discussed in the previous section.

A) Access Control: In cloud computing we based on the group signature technique for achieve efficient access control. To access the cloud, a user needs to compute a group signature for his/her authentication. The employed group signature scheme can be regarded as a variant of the short group signature, which inherits the inherent unforgeability property, anonymous authentication, and tracking capability.

To Achieve Access Control we also analysis the following points:

i. Unrevoked Users are able to access the cloud.

ii. Revoked Users cannot utilize the cloud after their revocation.

iii. An Attacker is unable to access the cloud server based on the assumption of intractability.

For achieving the access control, we use the concept of Dynamic Broadcast Encryption. A basic property very much desired in broadcast encryption (and other group-based protocols) is that the group should be dynamic in the sense that the group manager can invite new members to join or permanently revoke undesired members in a very efficient way. Although long term revocation necessarily implies a modification of the keys, there is no such theoretical requirement when a new member joins the group. In this respect, we say that a broadcast system is dynamic when

I. The system setup as well as the cipher text size are fully independent from the expected number of users or an upper bound thereof,
II. A new user can join anytime without implying a modification of preexisting user decryption keys
III. The encryption key is unchanged in the private-key setting or incrementally updated in the public-key setting, meaning that this operation must be of complexity at most O (1).

A dynamic broadcast encryption scheme involves two authorities: a group manager and a broadcaster. The group manager grants new members access to the group by providing to each new member a public label labi and a decryption key dki. The generation of (labi, dki) is performed using a secret manager key mk. The broadcaster encrypts messages and transmits these to the whole group of users through the broadcast channel. In a public-key broadcast encryption scheme ,the broadcaster does not hold any private information and encryption is performed with the help of a public group encryption key ek containing, possibly among other things, all user labels. When the broadcaster encrypts a message, some group members can be revoked temporarily from decrypting the broadcast content thanks to a one-time revocation mechanism.

Algorithm:

A dynamic public-key broadcast encryption scheme DBE with security parameter λ is a tuple of probabilistic algorithms DBE = (Setup, Join, Encrypt, Decrypt) described as follows:

Step1: Setup (λ) Takes as input the security parameter λ and outputs a manager key mk and an initial group encryption key ek. The group manager is given mk, and ek is made public.

Step2: Join (mk, i). Takes as input the manager key mk and a user counter i. Join generates a user label labi and a user decryption key dki. The user label labi is added to the group encryption key ek := ek$\cup${labi} and the user decryption key dki is sent to the i-th user securely. We denote by n the total number of users (evolving over time) and by U = {1, . . . , n} the set of all users.

Step3: Encrypt (ek,R). Takes as input the group encryption key ek and a set of revoked users R ⊆ U and outputs a random pair (hdr,K).When a message M ∈ {0, 1}∗ is to be broadcast to users in U \ R, the broadcaster generates (hdr,K).Encrypt(ek,R), computes the encryption CM of M under the symmetric key K and broadcasts (hdr,R,CM). We will refer to hdr as the header or broadcast cipher text, (hdr, R) as the full header, K as the message encryption key and CM as the broadcast body.

Step4: Decrypt (dki,R, hdr). Takes as input a header hdr, a subset R ⊆ U and a user decryption key dki. If i ∈ U \R, the algorithm outputs the message encryption key K which is then used to decrypt the broadcast body CM and recover M.

B) Data Confidentiality: In cloud computing, for Data Confidentiality we go under the hardness of the WBDHE (Weak Bilinear Diffie-Hellman Exponent) problem and GDHE (general Diffie-Hellman Exponent) problem. To meet the Above problems, the problem deduced in two another methods:

i. The cloud server is unable to learn the content of the stored files
ii. Even under the collusion with revoked users, the cloud server is also incapable of learning the content of the files stored after their revocation.

C) Privacy preserving and Traceability: To achieve the privacy and traceability in cloud computing, we demonstration this issue in two fold. On one hand, the group manager has the ability to identify the real signer. On the other hand, other entities cannot reveal the signer's identity from a group signature. Otherwise, DL (Decision linear) assumption will be in contradiction.

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees:

1. Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.
2. Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.
3. Privacy preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.
4. Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.
5. Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

A public auditing scheme consists of four algorithms (Key Gen, Sig Gen, Gen Proof, Verify Proof). Key Gen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate Verification metadata, which may consist of digital signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof. Running a public auditing system consists of two phases , Setup and Audit:

Setup: The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and deletes its local copy. As part of preprocessing, the user may alter the data file F by expanding it or including additional meta data to be stored at server.

Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof.

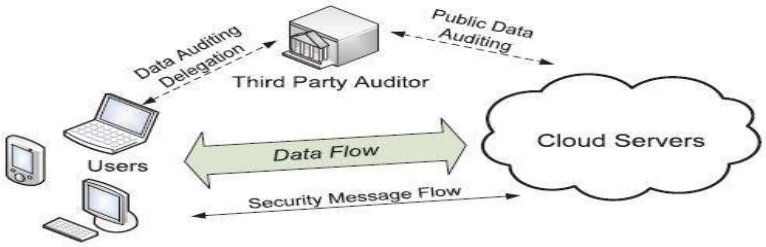

Fig. 1. The architecture of cloud data storage service.

V. TABLE I

Comparison of Parameters Provided By Different Security Research

Parameters	Access Control	Data confidentiality	Anonymity and traceability	Efficiency
Plutus [1]	Y	Y	N	N
Sirius [2]	Y	Y	Y	N
Revocation and Tracing Schemes [3]	Y	Y	Y	N
Improved Proxy Re-Encryption Schemes [4]	Y	Y	N	Y
Achieving Secure, Scalable, and Fine-Grained Data Access Control [5]	Y	Y	Y	N
Secure Provenance: Essential of Bread and Butter of Data Forensics [6]	Y	Y	Y	N
Mona[7]	Y	Y	Y	Y

VI. CONCLUSION

As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service- level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security module is not in place, potential users will not be able to leverage the advantages of this technology. This security module should cater to all the issues arising from all directions of the cloud. Every element in the cloud should be analyzed at the macro and micro level and an integrated solution must be designed and deployed in the cloud to attract and enthrall the potential consumers. Until then, cloud environment will remain cloudy .An

integrated security model targeting different levels of security of data for a typical cloud infrastructure is under research. This model is meant to be more dynamic and localized in nature. My research questions will center on application and data security over the cloud, and I intend to develop a framework by which the security methodology varies dynamically from one transaction or communication to another.

References

1. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
2. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp.131-145, 2003.
3. D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
4. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp.29-43, 2005.
5. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
6. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp.282-292,2010.
7. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" IEEE Transactions on Parallel and Distributed System,Vol.24,No.6,June 2013.
8. Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.
9. C´ecile Delerabl´ee, Pascal Paillier, and David Pointcheval. "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys" , Proceedings of the first International Conference on Pairing-based Cryptography (Pairing 2007) (2 – 3 july 2007, Tokyo, Japan) T. Takagi, t. Okamoto, E. Okamoto and T. Okamoto Eds. Springer-Verlag, LNCS 4575, pages 39–59.

AUTHOR(S) PROFILE

Lal Vikram Singh received the **B.TECH** degree in computer Science and engineering from Institution of Electronic and Telecommunication (IETE) in 2013.Currently doing **M.TECH** in computer science and engineering in Pondicherry University, Puducherry, India. His research interest includes Social Network Optimization, Cloud Computing, Big Data, Data Mining and Genetic Algorithm.

Amol V Bole received the **B.E** degree in computer Science and engineering from G.S.Moze College of Engineering Balewadi, Pune affiliated to University Of Pune**.** Currently doing **M.TECH** in computer science and engineering in Pondicherry University, Puducherry, India. His research interest includes Soft Computing and Genetic Algorithm.

Shailesh Kumar Yadav received the **MCA** degree from Gautam Buddha technical university lucknow 2011.Currently doing **M.TECH** in computer science and engineering in Pondicherry University, Puducherry, India. His research interest includes Algorithms and social network analysis.

