An Analysis for Security Issues and their Solutions in Cloud Computing

K. Selvakumar[1], Dr. M. Prabakaran[2]

[1]Research Scholar of Bharathidasan University, Department of Computer Science,
Government Arts College, Ariyalur, Tamil Nadu, India.
[2]Research Supervisor, Asst. Professor, Department of Computer Science,
Government Arts College, Ariyalur, Tamil Nadu, India.

---***---

Abstract- *Cloud computing is attracting great attention nowadays. The major challenge faced by cloud users and providers are security concerns towards cloud services. These security issues acts as a barrier in the growth of cloud computing. The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information. This paper addresses main security issues of cloud computing such as reliability, correctness of data, sharing of personal and sensitive information, unauthorized access of data, misbehavior or insider attacks and storage security. It also presents the analysis of some of the existing solutions for these issues in the literature*.

Key words- Cloud Computing, Cloud Security, privacy preservation, storage security, unauthorized access and reliability.

1. INTRODUCTION

Cloud Computing has become a scalable services consumption and delivery platform in the field of Services Computing. The technical foundations of Cloud Computing include Service-Oriented Architecture (SOA) and Virtualizations of hardware and software. The goal of Cloud Computing is to share resources among the cloud service consumers, cloud partners, and cloud vendors in the cloud value chain with secure manner. Cloud Computing is a type of computing infrastructure that consists of a collection of inter-connected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. Services are delivered over the Internet or private networks, or their combination. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements. The focus is to deliver reliable, secure, fault-tolerant, sustainable and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Thus cloud computing is a new way of delivering services.

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts [1] [2]. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [3]. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [4] [5]. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities [6].

1.1 Cloud Security

Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud.

1.2 Challenges of Cloud Security

The main issues of cloud security involve:

Correctness of data: The data stored in the external servers may be tampered by unauthorized or the cloud service providers. Correctness of data involves checking the integrity of the outsourced data periodically without making any local copy of files. The commonly used methodologies for ensuring correctness of data are verifier based signature schemes, private and public auditability, recovery techniques etc [21].

Sharing of personal and sensitive information: Privacy is a crucial requirement in cloud storage as revealing the personal information of users is against their confidentiality agreements. Sharing of personal and sensitive information in cloud has the risk of leaking such information to third party users.Hence the cloud environment should be trusted. In order to protect the personal information of users, privacy preservation techniques such as privacy preserving auditing, anonymous authentication and trusted computing are applied

Unauthorized Access: Unauthorized access to sensitive data is one of the most critical concerns from cloud computing customers. As prevention of unauthorized access can be generally achieved by encrypting sensitive contents before uploading them to cloud servers, there are still many challenges existing for its implementation in practical systems.

Misbehaviors or Insider attacks: Cloud computing suffers from conventional distributed systems' security attacks such as Man-in-the Middle attack, Distributed Denial-Of-Service (DOS) attack, insecure application programming interface and malicious insiders. Cloud services could be inaccessible due to these attacks and generate negative impact. [11].

Storage Security Issues: For the general cloud storage case, due to the security and control reasons, some data cannot be stored in the public cloud. Therefore, a solution needs to be proposed to reduce the cost of mobile cloud computing and communications, but also to ensure safety and to apply for hybrid cloud environments. [1].

Reliability Issues: In cloud storage, there are chances of accidental deletion of some data due to a server crash or software faults. Hence efficient solutions should be developed to recover the data in case of a loss [17].

The next section presents some of the security solutions proposed for the above listed security issues of cloud computing.

2. CLOUD SECURITY SOLUTIONS

2.1 Privacy Preservation

In order to solve the issues of sharing of personal and sensitive information, some privacy preservation techniques are proposed. There are few cryptographic tools and schemes like anonymous authentication schemes, group signatures, zero knowledge protocols that can both hide user identity and provide authentication [8].

Some of works dealing privacy preservation are discussed below:

Haralambos Mouratidis et al [7] have presented a novel framework which has a modelling language and a structured process to satisfy the security and privacy constraints. It selects the service provider based on the requirements of the cloud provider. A tool has been designed using OMI platform to implement the presented framework.

L. Malina et al [8] have proposed a privacy preserving scheme based on non-bilinear group signatures. It provides anonymous access to various services and servers of the cloud environment. It also ensures confidentiality and integrity of transmitted data using AES symmetric cipher. If any misuse of services was detected from a user, his access was revoked by a revocation manager.

Ulrich Greveler et al [9] have formulated a cloud database architecture that prevents the cloud administrators from accessing the shared data of cloud. It consists of an encryption proxy and a user interface. The workloads of the users are distributed over different proxies. The encryption proxy is responsible for secure data storage and access. Complex access rights are granted to the users using XACML.

2.2 Data Integrity

In order to ensure the correctness of data, data integrity mechanisms are developed. Data integrity is commonly assured by using cryptographic tools like digital signature authentication (DSA), hashing and verification based auditing techniques.

In DSA, the users sign pieces of data so that any forging attack can be promptly detected via signature validations. Some of the works dealing with data integrity are discussed below:

Praveen Kumarga et al [10] have introduced Dynamic Intelligent Server (DIS), for sharing the files of CSP and accurate storage of varying data. This work supports both remote data integrity and public auditability or dynamic data operations. They have used the Merkle hash tree structure for authenticating each block.

Ali Mohammed Hameed Al-Saffar [11] has proposed an identity based approach for data integrity in the distributed multi-cloud environment. They have developed a framework based on PDP. In this framework, when the combiner receives a request for data, it obtains a challenge which is distributed among the servers. The server responses are then aggregated and sent back to the client. Apart from these works, some of the approaches address the issue of data loss recovery apart from integrity.

Fawaz S. Al-Anzi et al [12] have developed a new architecture for secure data storage. In this architecture, the encrypted cipher data are split into various blocks and distributed uniquely to multiple CSPs. This ensures the reliability and availability of user data. For data loss recovery, a distributed parity scheme is implemented. Hence data cannot be reconstructed even though some of the CSPs collude with each other.

2.3 Access Control Mechanism

In order to prevent unauthorized access to sensitive data, access control mechanisms are used. An access control system is a collection of components and methods that restrict the activities of legitimate users based on predefined access permissions and privileges mentioned in the access policy. Each access control system has its own attributes, methods and functions, which derive from either a policy or a set of policies [11]. Some of the works dealing with role based access control are discussed below:

Saravana Kumar et al [13] have proposed the new ABE based encryption algorithm with hash functions, digital signature and asymmetric encryption method13.The proposed algorithm is simplified ABE and it will be suitable for the application that needs high level security and accessed time is being reduced which indeed cost is reduced comparatively. Certain outages don't really mean cloud is insecure. The cloud is actually misunderstood thing by others. Microsoft azure is being shifted fully to the cloud nowadays. Cloud computing has lot of advantages. Thus the cloud shouldn't lose its scope in future. Thus cloud has to shift to the next level by moving it to application like healthcare.

Shulan Wang et al [14] have proposed a file hierarchy based ABE scheme for cloud computing. In this scheme, hierarchical files are encrypted using a combined access structure. The ciphertext portions of attributes are shared by the files. But it does not provide data integrity. Moreover, it depends on single TA which may be subjected to failure.

Tran Viet Xuan Phuong et al [15] have proposed ciphertext policy attribute based encryption (CP-ABE) scheme. In this scheme, AND-gates with wildcards are used to define the access policy. In this scheme, they have presented a technique which applies only one group element to denote an attribute. The access policy is protected using hidden ciphertext policy. However, the key escrow problem is not resolved.

Entao Luo et al [16] have proposed a hierarchical multi-authority and CB-ABE based friend discovery scheme. It uses character attribute subsets to avoid single point failure and performance overhead. But this work does not provide data integrity

Apurva R. Naik et al [17] have proposed a modified ABE scheme to solve the key escrow problem. It provides a data sharing service for granting access control rights to the users. A public key authority (PKA) is used for partial key generation. It meets all the security requirements and provides enhanced security.

Rushikesh Nikam and Manish Potey [18] have designed Ciphertext Policy ABE (CP-ABE) and user authentication scheme. It applies CP-ABE for providing confidentiality and Multi Factor Authentication (MFA) for user authentication. For initial authentication, the traditional way of username and password are used. For further authentication, token generator technique is applied.

Attribute Based Encryption (ABE) has provided an effective way for fine grained access control. In a CP-ABE, the user's attributes used for key generation must satisfy the access policy used for encryption in order to decrypt the ciphertext [11]. Some of the works dealing with attribute based encryption are discussed below:

2.4 Trust Management

In order to detect and defend the misbehaviors or insider attacks on cloud environments, trust based solutions are developed. Trust management is essential to evaluate the abnormal activities of users and thus a user can interact with another user with high reputation one [19]. Some of the works dealing with trust management are discussed below:

Rizwana Shaikh et al [19] have presented a measurement based trust model. The trust model estimates the trust value using a list of security parameters. The main parameters are further divided into sub-parameters and functions. The user can select the required cloud services depending on these parameters. Dynamic trust is evaluated based on the past interaction history of users.

Praveen S. Challagidad et al [20] have proposed a reputation based trust model. It determines the reputations of CSP using a trust evaluation algorithm. This model collects the opinions from cloud users based on which the most trusted CSP is selected. The total trust value is determined from the user opinions, workload of the servers and number of rejected requests by the server.

Indrajit Ray et al [21] have proposed a trust-based access control model with delegation. It is based on the Role-Based Access Control (RBAC) model which is mostly used in organizations for granting access rights to the employees. Their proposed model contains set of elements, relationships and constraints.

Muhammad Yousaf Saeed et al [22] have proposed a new model which introduced Security Aware Cloud. Initially, the trust value is determined on the cloud based on which privacy and encryption modules are developed. It consists of contract trust layer for providing Quality of Service (QoS) and internal trust layer for authentication. For confidentiality, the Homomorphic encryption is used.

3. CONCLUSION

We have presented the analysis of various security issues and their solutions in cloud computing. It addressed the main security issues of cloud computing such as reliability, correctness of data, sharing of personal and sensitive information, unauthorized access of data, misbehavior or insider attacks and storage security. It also presented the analysis of some of the existing solutions for these issues in the literature. The existing security solutions such as data Integrity, privacy preservation, role based access control and trust management are discussed. Under each category, the existing methodologies are analyzed. Hence future methodologies should ensure the correctness of stored data, apart from providing confidentiality, integrity and authorized access control. They should be adaptable to multi-cloud environment where user data is distributed across multiple clouds.

REFERENCES

[1].Kamini Bharti and Kamaljit Kaur, "A Survey of Resource Allocation Techniques in Cloud Computing", International Journal of Advanced Computer Engineering and Communication Technology (IJACECT),ISSN (Print): 2319-2526, Volume-3, Issue-2, 2014.

[2] Michael glas and paul Andres, “An Oracle white paper in enterprise architecture achieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3] Harjit Singh Lamba and Gurdev Singh, “Cloud Computing-Future Framework for e-management of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM-Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5] Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST, Germany.

[6]. Naresh vurukonda and B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016),2016.

[7].Haralambos Mouratidis, Shareeful Islam, Christos Kalloniatis and Stefanos Gritzalis, "A framework to support selection of cloud providers based on security and privacy requirements", The Journal of Systems and Software,2013

[8].L. Malina, J. Hajny, P. Dzurenda and V. Zeman, "Privacy-preserving security solution for cloud services", Journal of Applied Research and Technology,2015.

[9].Ulrich Greveler, Benjamin Justus and Dennis Loehr, "A Privacy Preserving System for Cloud Computing", IEEE,2011.

[10].N.Praveen Kumarga and D.Sireesha, "Ensuring Data Integrity in Cloud Computing", International Journal of Computer Science and Network Security, Vol.14 No.9, September 2014.

[11].Ali Mohammed Hameed Al-Saffar, "Identity Based Approach for Cloud Data Integrity in Multi-Cloud Environment", International Journal of Advanced Research in Computer and Communication Engineering,Vol. 4, Issue 8, August 2015.

[12].Fawaz S. Al-Anzi, Ayed A. Salman, Noby K. Jacob, "New Proposed Robust, Scalable and Secure Network Cloud Computing Storage Architecture", Journal of Software Engineering and Applications, Vol- 7, 347-353, 2014.

[13].Saravana Kumar N,Rajya Lakshmi G.V and Balamurugan B, "Enhanced Attribute Based Encryption for Cloud Computing.", Procedia Computer Science 46 (2015), pp. 689 – 696.

[14].Shulan Wang, Junwei Zhou,Joseph K. Liu,Jianping Yu, Jianyong Chen, and Weixin Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 11, NO. 6, June 2016.

[15].Tran Viet Xuan Phuong, Guomin Yang and Willy Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions", IEEE Transactions on Information Forensics and Security, Vol. 11, NO. 1, January 2016.

[16].Entao Luo, Qin Liu and Guojun Wang,"Hierarchical Multi-Authority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks", IEEE Communications Letters, Vol. 20, NO. 9, September 2016.

[17].Apurva R. Naik and Lalit B. Damahe, "Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism",I. J. Computer Network and Information Security, 2016, 10, 53-60.

[18].Rushikesh Nikam and Manish Potey, "Cloud Storage Security Using Multi-Factor Authentication", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India, 2016.

[19].Rizwana Shaikha and M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", Procedia Computer Science 45 (2015) pp-380 – 389.

[20].Praveen S. Challagidad, Vani S. Reshmi and Mahantesh N. Birje, "Reputation Based Trust Model in Cloud Computing", Internet of Things and Cloud Computing, 2017; 5(5-1): 5-12.

[21].Indrajit Ray, Dieudonne Mulamba, Indrakshi Ray, Keesook Han, "A Model for Trust-Based Access Control and Delegation in Mobile Clouds", Lecture Notes in Computer Science book series (LNCS, volume 7964),2013.

[22].Muhammad Yousaf Saeed and M.N.A. Khan, "Data Protection Techniques for Building Trust in Cloud Computing", International Journal of Modern Education and Computer Science, 2015, 8, 38-47.