INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 4 - V8I4-1165)
Available online at: https://www.ijariit.com

Confidential data protection using a multi-level security approach in the cloud

Sagar Bagale
sagarsbagale@gmail.com
Nagesh Karajagi Orchid College of Engineering and Technology, Solapur, Maharashtra

Sudhir Shinde
sudhirs.shinde@gmail.com
Nagesh Karajagi Orchid College of Engineering and Technology, Solapur, Maharashtra

ABSTRACT

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. This exciting computing model depends on data traffic and controlled by a third party. Despite the expected savings in infrastructure and the development cost for business flexibility, security is still the biggest challenge for the implementation of computing for many service-based companies. Security in cloud computing is mainly focused on the protection and to guarantee data security. This paper discusses challenges related to data security and privacy implementation in cloud computing environment. A multiple level approach is proposed to accommodate the protection of confidential data in cloud computing environment. This framework consists of different levels application security level, keyword-based file search, public key and fingerprint verification level. The main objective of this paper is to discuss the framework implementation and its architecture verification. It is expected from the research a verified framework to protect private and confidential data in cloud environment.

Keywords: *Cloud Computing, Security, Privacy, Confidential Data*

1. INTRODUCTION

The cloud computing offers different types of service models Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). The information technology for cloud computing infrastructure consists of networks based on IP software, services, and virtual interface. Cloud uses different models of service such as hybrid, community, private or public cloud model. Cloud creates a new understanding between companies, organizations, and their information. This requires the existence of a third party to manage relationships. It is named service provider in the cloud computing. This type of relationship creates many security stabs. Security in cloud computing is mainly focused on the protection and to guarantee data security. In order to understand the risks and threats to data put in storage of the cloud, it is important to know who users are, and what the services that equips by the cloud. These definitions are provided by [1]. Users (also Clients or Customers) are individuals, companies, or governments seeking the use of infrastructure and services in the cloud. Service Providers are individuals, companies, or governments with the ability to offer infrastructure and services for general consumption. The main objective of this paper is to improve and develop the performance of security and privacy for storing sensitive information in the public cloud. This work permits verification of using the appropriate way to protect sensitive information in the cloud computing environment.

2. CLOUD COMPUTING SECURITY CHALLENGE AND ISSUES

It is clear that security plays an important role in the acceptance of dealing with cloud computing where to put the data and run the software away from the user's location are a big challenge from the security aspect for many companies and users, also there are many possible problems resulting [2]. These problems will be explained from three aspects: data, privacy and security, and persons or companies are discussed below:

2.1 First aspect relates to data consists of:

1. Data integrity: Data integrity includes the following cases: mistakes may occur when data is transmitted from one place to another or from one computer to another. Other possible mistake occurs as result of exposure to the problems of hardware and functional such as viruses or crash the disk. There are many services consumers and providers access and modify data in cloud computing. Therefore, there is need to have some methods of safety data in cloud computing [3].
2. Data access control: Sometimes private data can be accessed illegally due to a lack of access control to confidential data. Sensitive data in a cloud computing environment is one of the key issues in terms of security in the cloud-based system [3].

3. Data theft and loss: Cloud computing is used for processing and storing data external servers for cost efficiency and flexibility of operation. For this, there is opportunity to steal data from external servers. And data loss is a serious problem in cloud computing. If banking and commercial transactions and the ideas of research and development, all occur on the Internet, and unauthorized persons will be able to access shared information. Even if everything is secured what happens if the server goes down or crash or attacked by a virus, the entire system goes down and data loss can occur as a result [3].

2.2 Second aspect relates to privacy and security consists of:

1. Protection and privacy issues: Personal customer information security is very important in cloud computing. Most of servers are external, so the vendor must ensure the security of the information from the other operators [3].
2. Infected and malicious application: The provider of service must have full right to use the server for the purpose of observing and preservation of the server [3]. So, this will prevent any intruders from sending any infected application on the cloud, which will strongly affect cloud computing and client service [3].

2.3 Third aspect relates to persons or companies consists of:

1. User level security issues: The user must ensure that its own work, there is no loss of data or manipulate the data for other customers who are using the self-same cloud [3].
2. Provider level security issues: The cloud is perfect only when there is ideal security by the vendor offers to customers. Provider should provide a good layer of security for customers and users. And should make sure that server is good secured from all outer menaces may come through it [3]. The main objective of this research is to improve and developthe performance of security and privacy for accessing confidential information in the public cloud.

3. RELATED WORK

In this paper, focused the challenges of security, privacy and design a good policy in cloud computing security. Many papers discussed the technology and growth of the cloud computing security. This section reviews papers mentioning cloud computing in different aspects.

In paper [4] the author applied deductive method for verification and validation of security systems. In this method security components designed in form of common security items, each of those items- data item or functional item is itself encrypted. The author proposes to use encryption to protect all applications resources. Based on this principle, in this system the data in files and database tables are encrypted, messages and control parameters are encrypted, and software models also encrypted. This method leads to protect software models from penetration or exposure to viruses. The data is not exposed to theft or breach, and messages exchanged in the system environment will be protected. Some authors suggested using a trusted third party [5], take care to ensure the security features specified within the cloud [5]. This proposed solution relies on encryption and authentication to ensure the integrity and confidentiality of data and communications.

Some other authors suggested a security framework for cloud computing platform in this context where the processes the request submitted by the customer and building link security model supports the safe transport of the data model [6]. Transmits the user's request to the front of podium in the server through a secure connection and is delivering the application to the desired application server. Also, there are problem of protecting the privacy of information, and knowledge of the characteristics of cloud computing, and how variation in the legal protection of privacy of information within the internet [7]. Many solutions have been proposed to the problem of privacy protection, including data encryption method. Some authors focus on problems related to the confidentiality of the data and privacy in cloud computing and proposing a new model- called multi cloud databases (MCDB) [8]. The purpose of the proposed model is to identify security risks and privacy in the cloud computing environment.

There is also a related work that aims to highlight the lack of a legal framework for the transmit of personal data across the borders through cloud computing services and explore the benefits that might be achieved through the adoption of the regulatory framework [9]. They examined a variety of alternative models. According to the study of these models and cloud computing, this study tries to find regulatory framework for the preservation of personal information in relation to cloud computing.

The problems of security and integrity of the data include key management, control of access, searchable encryption techniques, distant integrity checks, and prove the owner of the information in the cloud are common area of study. Because of the problem of expose data in the cloud, the authors used homomorphic encryption mechanism, and suggested a plan for the security of data and cloud computing [10, 11]. This plan included the transfer of data between the cloud and user safety and security. New method to ensure security and data breaches that provide confidential cloud computing. To avoid the occurrence of any change or loss of data on a server, the authors used two servers, one for the encryption process known as (trusted computing platform) and the other known as (storage server), storage server for storing consumer data file [12]. Likewise, a group of researchers proposed a new architecture based on data encryption and using another party in addition to CSP this make only authorized user can send and retrieve data to cloud computing [13].

Other research focused on the improvement of cloud computing in terms of security issues associated with reliability and privacy. And explain the main reasons that affect the security risks. As well gave suggestions and recommendations in certain areas and suggested different anonymization techniques and approaches to preserve sensitive information in cloud. They analysed the advantages and disadvantages of these techniques and the security and privacy of sensitive information in the cloud computing environment [14, 15, 16]. Many of the questions relating to the protection of sensitive information privacy in the cloud computing environment are still without solutions [17], and most of the existing solutions using limited methods such as data encryption by third party, and this technique need to be used exchange of encryption keys, which may expose the keys to detection and penetration, and this leads to the possibility of data breaches. In addition, the encryption process takes high computation and need more time and space this leads to slower in store and retrieval the data [11, 18].

4. THE PROPOSED FRAMEWORK

The proposed project adds three or more layers of protections to access files on server. When all the verifications are successful then only access to the files is provided. This project will contain two main modules: Merchant (data owner) and Buyer (Data user). Merchant (data owner) uploads the files to the server and buyer (data user) has to register first by adding fingerprint details and later useit while accessing the files. Buyer needs to search files and request for access to concerned merchant. If merchant accepts the access request buyer will receive a key through registeredmail id. If the secret key and the fingerprint mismatches file will not be downloaded. Below are the three levels which arerequired to access data from cloud:

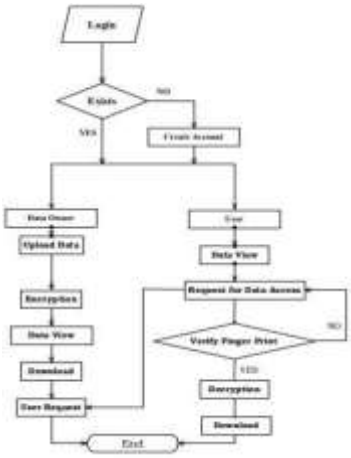

Figure 4.1: Data Flow Diagram

4.1 Application Security Level

This level of security uses application user credentials, username, and password for authenticating the user. Steps in this level are:

a. Data user registers username and password to system through graphical user interface.
b. Using MD5 algorithm, password is encrypted and saved into database.
c. To access data, user logs in to application using the username and password used during registration.
d. System uses MD5 algorithm to convert entered password. If credentials match, then system allows user to proceed with application, else user request is rejected.

Algorithm 1 for Application Security Level

1. Register to system: User/Owner provides own details
2. Authentication:

A= {a1, a2...an}

Where, A= No. of user attributes. (e.g., username,password, email etc.)

3. Use MD5 algorithm to encrypt and save password in database
4. Auth={Active/Inactive}
5. Login to system. To perform functionality User/Owner Login to system
6. Upload Data (File)

4.2 Private Key Authentication

This level of authentication uses public key generated bydata owner for file access by data user to provide access for that file. Data owner generates key and send it to data user through the registered email address.

Steps in this level are:

a. Data user searches for file by entering the keyword from specific file name.
b. System uses keyword-based file search techniques to search files and displays list of files.
c. Data user sends request to data owner for access to that file by selecting specific file.
d. Data Owner uses AES (advanced encryption Standard) to generate key.
e. Generated key is encrypted using SHA256(Secure Hashing Algorithm) and stores in database.
f. Data user receives that key through email and uses the same key while downloading the file.

Algorithm 2 for public key generation

1. Get instance AES (Advanced Encryption Standard Algorithm) using gey generator.
2. Generate secret key
3. Get MessageDigest instance for hashing using SHA256(Secure Hashing Algorithm)
4. calculate message digest of an input and return array of byte
5. Convert byte array of hash into digest
6. Convert the digest into hex value
7. Pad with leading zeros
8. Return public key

4.3 Fingerprint Authentication

This level of security uses fingerprint of data user to authenticate and provide access to specific file. Fingerprint of user is obtained during registration process and saved into database. Below are the steps involved inthis level:

a. Data User registers the fingerprint during registration process.
b. Raw fingerprint is then converted into ISO text template and stored into database.
c. While downloading the file, once the public key verification is successful, user scans the fingerprintwhich he used during registration.
d. Scanned print then converted to iso text template and system compares it with database template.
e. If both fingerprint and public key verification is successful, then user is allowed to download the file, otherwise user access to file is rejected.

Algorithm 3 for accessing and downloading the data

1. Scan the fingerprint using fingerprint device scanner
2. Read scanned image as BitMapData anddisplay the image
3. scanneduserFingerPrint=convert fingerprint image to iso text template.
4. savedUserFingerPrint=Retrieve user iso text template of user from database.
5. Compare scanneduserFingerPrint and savedUserFingerPrint using iso templatematching method.
6. If scanneduserFingerPrint and savedUserFingerPrint matches, then
7. savedEncryptedKey=retrieve key fromdatabase
8. Compare savedEncryptedKey with user key
9. If savedEncryptedKey matches
10. Then allow access to data
11. Else reject user access.

5. RESULT AND DISCUSSION

Implementation of this paper carried out to compare it with existing system to evaluate the security. The implementation platform used is built with Java framework (jdk 7 version) on the Windows platform. The system it does not require any specific hardware to perform; any standard machine is able to run the application. In existing system, if password is known by the second person, then there are chances of getting access to all data at once. In this system, even if password is comprised, the other person must have file details, public key, and fingerprint. Implementation of this paper shown that security of each data or file increased by three times the existing system.

Figure 5.1: Fingerprint and Key Verification Page

6. CONCLUSION

Many new challenges have developed with the rapid advancement of adaptive services in the cloud. One of the most critical problems is to protect data when it is stored in the cloud. To provide more security, for each file, different public key is generated and encrypted and used along with iso text template of the fingerprint to verify authorized user of data. In addition to this project's three-layered security, it can also increase two more levels of security if data user's email two factor authentication is enabled. In future we can add more security by adding fingerprint authentication and key authentication in application security at the time of login.

7. ACKNOWLEDGMENT

We take opportunity to express my gratitude to all those who have rendered cooperation and guidance that supported for this research. We are profoundly grateful and express our deepest gratitude to teachers, guides and mentorswho helped me to make this research happen.

8. REFERENCES

[1] L. Youseff, M. Butrico, and D. Da Silva., "Toward a Unified Ontology of Cloud Computing," In 2008 Grid Computing Environments workshop, pages 1-10. IEEE, Nov. 2008.

[2] Loganayagi.B, S. Sujatha, "Enhanced cloud security by combining Virtualization and Policy Monitoring Techniques," International Conference on Communication Technology and System Design 2011.

[3] Anitha Y, "Security issues in cloud computing- A Review," International Journal of Thesis Projects and Dissertations (IJTPD), 2013.

[4] A. G. Abbasi, "Generic Security Framework for Cloud Computing Environments," Doctoral Dissertation in Communication Systems, School of Information and Communication Technologies (ICT), Stockholm, Sweden, 2011.

[5] D. Zissis, D. Lekkas, "Addressing cloud computing Security issues," Future Generation Computer Systems 28 (2012) 583–592.

[6] X. Xiaoping, Y. Junhu, "Research on Cloud Computing Security Platform," Fourth International Conference on Computational and Information Sciences (2012).

[7] F. Chang Chenga, W. Hsing Lai, "The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the protection of Information Privacy," Procedia Engineering 29 (2012) 241-251.

[8] M. A. AlZain, B. Soh, E. Pardede, "A New Model to ensure Security in Cloud Computing Services," Journal of Service Science Research (2012) 4:49-70.

[9] A. Abu Oliem, "Cloud Computing Regulation: An attempt to protect Personal Data transmission to Cross- Border Cloud Computing Storage Services," International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.

[10] M. Zhou, "Data security and integrity in cloud computing," Doctor of philosophy Thesis, School of Computer Science and Software Engineering University of Wollongong, (2013).

[11] F. Zhao, C. Li, C. Feng Liu, "A cloud computing security solution based on fully homomorphic encryption," ICACT 2014, February 16- 19, 2014.

[12] A. Gupta, Mrs.V.Chourey , "Cloud Computing: Security Threats & Control Strategy using Tri-Mechanism," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) 2014.

[13] S. K. Gupta, S. Rawat, P. Kumar, "A novel based security architecture of cloud computing," Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International conference on8-10 Oct. 2014.

[14] D.W.K. TSE, "Challenges on Privacy and Reliability in Cloud Computing Security," Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on (Volume:2) 26-28 April 2014 Page(s):1181 – 1187.

[15] S.Chintawar, Ismail, "A brief survey on privacy preserving data Anonymization Techniques on Cloud," International Journal of Computer Engineering and Applications, Volume VIII, Issue II, Part I, November 2014.

[16] A. Gholami, and Erwin Laure, "Security and Privacy of sensitive data in cloud computing: A Survey of recent developments," David C. Wyld et al. (Eds): NET COM, NCS, WiMoNe, CSEIT, SPM-2015, PP. 131-150, 2015.

[17] F. Kelbert, "Data Usage Control for the Cloud," 13th IEEE/ACM International Symposium on Cluster, Cloud andGrid Computing 05/2013.

[18] M. Tebaa, S. EL HAJJI, "From Single to Multi-Clouds Computing Privacy and Fault Tolerance," IERI Procedia10(2014) 112-118

