A REVIEW OF DATA PRIVACY AND SECURITY IN CLOUD COMPUTING

Sugandh Bhatia
Punjab School of Economics, Guru Nanak Dev University, Amritsar-143005, India
sugandhcs.rsh@gndu.ac.in

Rajinder Singh Virk
Department of Computer Science, Guru Nanak Dev University, Amritsar-143005, India

Jyoteesh Malhotra
Department of Electronics and Comm. Engg.,GNDU Regional Campus, Jalandhar-144009, India

Abstract - Cloud computing is a growing paradigm and is considered to be an important cost-effective solution. Cloud service providers (CSPs) offer different storage services for users in a sophisticated manner. CSPs such as IBM, Google, Oracle, Microsoft, Amazon and many more allow cloud users to store their data in cloud server. The pressure of storing and retrieving in local machine can be reduced with the help of cloud storage. The data stored on cloud can be shared by a user or a group of users which requires privacy and security of the data. In this research paper, an attempt has been made to point out different techniques to resolve the data privacy and security issues in cloud computing environment.

Keywords: Cloud Computing, Security, Privacy, Data Storage & Integrity

1. INTRODUCTION

Cloud computing is one of the most transformative computing technologies. Many companies like Google, Amazon, Microsoft, IBM, Rackspace, GoGrid, Heroku, Eccentex, Facebook, Slideshare, LinkedIn, etc. furnishes services based on cloud computing. In 2015, the cloud computing market was of $ 80 bn. The study by Forbes forecasts that worldwide public cloud revenue will increase from $ 80 bn in 2015 to $ 167 bn in 2020 [7]. This zippy expansion or growth, therefore, reflects the growing significance of cloud computing. But, unfortunately, there are some weak points in cloud computing and it is an arduous task for the client and service provider to ensure that appropriate security measures are effectively implemented. In fact, data security, privacy and cost of service are the important parameters on which cloud services are measured. Thus, security is the pivotal component for customers and service providers. In October 2016, 3.2 million debit cards belonging to major banks in India were hacked [11]. According to the report around 2.6 million cards were on Visa and MasterCard platform, while over 600 thousand were on the Rupay platform. The card network companies had received complaints from banks about unauthorized card usage from locations in China. As per reports, the breach had generated in Hitachi payment services. Hitachi is one of the largest providers for point of sale services, ATM machines and mobile transactions in India. A malware in Hitachi system had compromised user data. The Payments Council of India has ordered a forensic audit on Indian bank servers and systems to find the origin of breach. It is need of the hour to design and implement a secure framework for cloud computing environment [1]. Therefore, this paper discusses emerging issues of data privacy or security and accentuates its scope, challenges and opportunities.

2. DATA PRIVACY AND SECURITY ISSUES IN CLOUD COMPUTING

Data privacy and security risks may differ according to the nature of cloud. Although cloud computing provides various type of services such as Infrastructure-as-a- Service, Platform-as-a- Service and Software-as-a- Service. But, with all these benefits, cloud computing carries some issues about confidentiality, integrity and availability of information on the cloud [10]. The following issues are addressed in cloud computing.

- Leakage of data and unauthorized data access.
- Mishandling of important and sensitive data by cloud service provider.
- Delivery of critical data to law enforcement agencies and third party users without taking the permission of the customers.
- Dearth of measures to satisfy compliance and regulatory requirements.
- Lack of measures to ensure confidentiality and integrity.
- Cloud application programming interface (API) enforced by the CSP is not able to protect the sensitive data of the customers.

3. LITERATURE REVIEW

There has been many research on privacy and security of data in cloud computing. Various security mechanisms proposed and implemented by researchers in industry and academia. In this review paper, some of the few important works has cited.

Wei et al.[14] (2010) suggested SecCloud which provides a security protocol to cloud data. This protocol provides security to both stored data and computational data. Encryption is applied in SecCloud to store data in secure mode. Cloud customers, cloud service provider (CSP) and trusted third party (TTP) use cyclic additive pairing and multiplicative groups for key generation. Verifiable signature, encrypted data and session key is delivered to cloud data center. For generating the session key, Diffie - Hellman algorithm is used. When encrypted data is received by the cloud, the first step is to decrypt that data and afterwards digital signature is verified. The last step is to store the original data on the specified location in the cloud. The SecCloud checks whether data is stored at accurate position or not.

Feldman et al.[6] (2010) has proposed encryption/ decryption techniques combined with auditing and access control to provide privacy and security. However, security to the data stored on public cloud can be provided with this mechanism. But, by performing this, large computational burden was imposed on the owner of data for key distribution, management of data and data query.

The authors C.Wang et al.[12] (2011) presented an adaptable distributed storage auditing system to guarantee privacy and security in cloud. The integrity of stored data was checked by using the homomorphic token and distributed erasure coded data techniques. Different dynamic operations such as block modification, deletion and support third party auditing were allowed to user. The proposed scheme required less resource for computation and communication and was adequate against data modification attack and server colluding attack.

Popa et al.[9] (2011) proposed a secure storage system named as CloudProof. It ensures confidentiality, integrity and availability. Confidentiality is achieved by private keys that are available with the owner of the data, which is to be encrypted. A new method is introduced in this system which is known as attestation mechanism. This mechanism permits users to store data by putting a block identifier and the contents of the block in the cloud. Block hash is implemented by attestation structure for computing integrity checks by signature verification.

Zissis. D et al.[16] (2012) presented a system which used a trusted third party (TTP) with in a cloud environment. In this system, cryptography is used to ensure confidentiality, integrity and authenticity of data. The notion of trust against the third party reveals the faith of customer. All operational, ethical and managerial tasks are controlled by third party. The relying party has only one option and that is to trust the third party for the security support in all transactions. Trusted third party is a security facilitator in cloud environment. The presence of TTP makes the system secure and due to the involvement of TTP in the environment the overall cost of operations is increased and moreover, the system or environment is fully dependent and in the control of TTP.

The authors Chen et al.[4] (2012) explained a framework which is used to ensure that the cloud data is kept secure and private. It provides security from unauthorized user and unintentional modifications. Cloud users face two critical security threats such as data segregation and session hijacking. Major challenges in cloud computing exist at abstraction level and dynamism in scalability. Privacy and security might differ at various levels and thus, it may result a security breach in cloud services at various regions, containers and contexts. Authors classified stored data in to two groups, IaaS environment data and data in PaaS and SaaS environment. Data in case of IaaS is stored in the cloud rather than local hard drive. Amazon simple storage service is a perfect example of this case. In PaaS and SaaS, generally, data is not stored for long term, it is used primarily for application processing. Encryption and decryption can be justified on the data in case of IaaS. But, in case of PaaS and SaaS environments encryption can't be recommended, because, it is not feasible to perform encryption and decryption at each level of computing tasks.

Costache et al.[5] (2013) presented a cloud platform named as Merkat. It is based upon three main characteristics. First, it furnishes support for per-application service level objective (SLO) by executing applications in virtual environment which are autonomous. Second, in Merkat, resource utilization is achieved at maximum level. It is based on the market which provides resources to virtual machines. This way, applications of the users are executed in an efficient and impressive manner. Finally, in Merkat, two types of per-application resources scaling policies are implemented. These are horizontal and vertical scaling. But the drawback of Merkat is that all the services are interrupted in case of failure and application performance should be improved with the help of price prediction algorithms.

Yang et al.[15] (2014) proposed a mechanism DAC- MAC (Data Access Control for Multi Authority Cloud Storage). This mechanism concentrates on multi authority cloud storage system, as there might be a chance that user were provided with attributes from various authorities. This demands the requirement for efficient system to execute different attributes together with which forward and backward security is procured. The scheme DAC- MAC carries decryption efficiency with the use of token based model. A novel multi – authority Cipher text- Policy Attribute- Based Encryption (CP-ABE) scheme is presented which is useful in real time critical applications and for access control of encrypted data.

Wang et al.[13] (2015) proposed DDOS attack defense DaMask for cloud environment. Advance programmable network monitoring technique is used in DaMask that detects attack and corresponds with the help of a flexible control structure. There are three layers named as network switches, network controllers and network application along with two modules named as anomaly based network attack detection module (DaMask-D) and attack mitigation module (DaMask-M) are used in DaMask. A caution is sent when an attack is detected by DaMask-D. Afterwards, packets of information along with caution will be transferred to the DaMask-M module. Two functions are performed by DaMask-M. These functions are countermeasure selection and log generation. Major advantage of using DaMask is that the computation cost is low in this mechanism.

The authors Chang et al.[2] (2016) proposed a framework which provides privacy and security to business clouds. This framework is named as Cloud Computing Adoption Framework (CCAF). Three basic technologies of security such as firewall, encryption and identity management is implemented which provides multilayered security in CCAF. It is proved in penetration testing that it is possible to detect and block more than 99% viruses and trojans. Even, SQL injections can also be blocked with CCAF multilayered security protection. Therefore, it provides real privacy and security to cloud data if compared with another tools, frameworks and mechanisms.

4. LIMITATIONS IN EXISTING SYSTEMS/ METHODS

1) Insecure interface of APIs.
2) Data leakage or loss.
3) Possibility of service hijacking.
4) Lack of governance
5) Misuse, mismanagement and mishandling of cloud data.
6) Existence of compliance risks.
7) Traceability is not supported in existing systems.

5. PROPOSED SYSTEM

In the proposed system, a model is designed as shown in Figure 1 to provide security at three levels. The first level is when the data is not in use and in idle stage. The second and third levels are concerned only when the data is active or in motion. Data can be in motion when it is stored by the user or it is fetched by the user from data center. When a new user entered in to the system, a secret key and access structure is provided to that user. The access structure allows the user to encrypt data before uploading it on the cloud [8]. It is also ensured that only approved and certified users can access to it. When the user enter in the cloud after passing and completing successfully all the barriers of security and privacy, it is now possible to fetch the data from cloud but user should go through another security check in the form of encryption and decryption. In the process of transfer and storage of data, encryption is applied and decryption is performed while using the data. In case of Storage as a Service, one of the important components of cloud architecture is data center. The overall performance of the business is dependent on data center. The management of data should be performed very carefully. One last step of security is applied before giving the full access of data to client that involves data update and encryption. Involvement of intrusion detection mechanism enhances the cloud security and it is beneficial for cloud security team. If intrusion occurs in the system, then system will send message to cloud security team, data center and users.

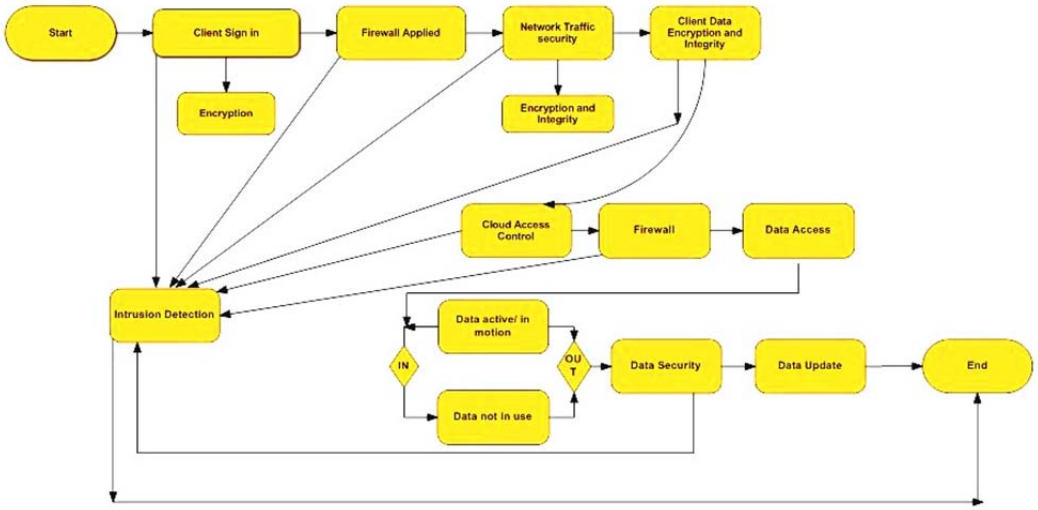

Figure1. Data Security Model of Proposed System

In this system, attack detection, denial of service, anti-spoofing, SQL injection, parameter tampering, cookie poisoning and other vulnerabilities are controlled. For authentication purpose, in the proposed system RSA can be applied. Every user is provided with numerous key pairs to initiate new instances with the help of various combinations of key pairs. Open SSL can be implemented by the user to generate public and private keys in a secure environment. Private keys are generated, managed and handled by the client, whereas, in the cloud environment keys are generated, managed and controlled by CSP [3]. In every cloud data security model there can be many entities involved such as client, cloud service provider, data center and cloud control team. Therefore, the use of this proposed system is important and apposite in achieving the cloud data security and privacy since it is required to protect the data at each level in cloud environment.

6. CONCLUSION

Despite many benefits and services offered by the cloud computing, the organizations and users are compelled to think so many times before adopting the cloud services. This research papers reveals various issues of data privacy and security in cloud computing environment. In every deployment model, the privacy and security of data, cloud resources and infrastructure should be ensured. Various cloud security models and frameworks have been reviewed in this paper. There is a lack of specific criteria on which it is concluded that which framework is good and which is bad. A framework is proposed in this paper which suggests providing encryption at different levels on data along with intrusion detection mechanism. In developing countries like India, cloud computing can play an important role to achieve sustainable development of the Nation, if implemented, organized and managed in a secure and effective manner.

References

[1] A Trusted Framework for Data Security in Cloud Environment. (2015). *International Journal of Science and Research (IJSR)*, *4*(11), 1728-1730. doi:10.21275/v4i11.sub159028

[2] Chang, V., Kuo, Y., &Ramachandran, M. (2016). Cloud computing adoption framework: A Security Framework for Business Clouds. *Future Generation Computer Systems*, *57*, 24-41. doi:10.1016/j.future.2015.09.031

[3] Chang, V., &Ramachandran, M. (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing*, *9*(1), 138-151. doi:10.1109/tsc.2015.2491281

[4] Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*. doi:10.1109/iccsee.2012.193

[5] Costache, S., Parlavantzas, N., Morin, C., &Kortas, S. (2013). Merkat: A Market-Based SLO-Driven Cloud Platform. *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*. doi:10.1109/cloudcom.2013.59

[6] Feldman, A., Zeller, W., Freedman, M., &Felten, E. (2010). Group Collaboration Using Untrusted Cloud resources. *OSDI*.

[7] www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#317b6c172187

[8] Improved Cloud Storage Security Framework Based on TTP Crypto Network. (2015). *International Journal of Science and Research (IJSR)*, *4*(11), 153-155. doi:10.21275/v4i11.sub159067

[9] Popa, R. A., Lorch, J. R., Molnar, D., Wang, H. J., &Zhuang, L. (2011). Enabling security in cloud storage slas with cloudproof. *Proceedings of the USENIX Conference on USENIX Annual Technical Conference, USENIXATC, Berkeley, CA, USA*.

[10] Selvamani, K., &Jayanthi, S. (2015). A Review on Cloud Data Security and its Mitigation Techniques. *Procedia Computer Science*, *48*, 347-352. doi:10.1016/j.procs.2015.04.192

[11] Shukla, S., &Bhakta, P. (2016, October 20). 3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit. *Economic Times* [Mumbai], p. 1.

[12] Wang, B., Zheng, Y., Lou, W., &Hou, Y. T. (2015). DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking. *Computer Networks*, *81*, 308-319. doi:10.1016/j.comnet.2015.02.026

[13] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2011). Toward Secure and Dependable Storage Services in Cloud Computing. *IEEE Transactions on Services Computing*, *5*(2), 220-232. doi:10.1109/tsc.2011.24

[14] Wei, L., Zhu, H., Cao, Z., Jia, W., &Vasilakos, A. V. (2010). SecCloud: Bridging Secure Storage and Computation in Cloud. *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*. doi:10.1109/icdcsw.2010.36

[15] Yang, K., Jia, X., Ren, K., Zhang, B., &Xie, R. (2014). DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. *IEEE Transactions on Information Forensics and Security*, *8*(11), 1790-1801. doi:10.1109/tifs.2013.2279531

[16] Zissis, D., &Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. doi:10.1016/j.future.2010.12.006

Authors

Sugandh Bhatia is currently working as Assistant Professor in Punjab School of Economics, Guru Nanak Dev University, Amritsar and pursuing his PhD in the Faculty of Engineering and Technology, Guru Nanak Dev University, Amritsar. His field of research interests includes Cloud Computing, Cloud Forensics, Data Security and Privacy.

Rajinder Singh Virk received the PhD in Computer Science and Engineering from Guru Nanak Dev University, Amritsar. He currently holds the position of Professor and Head of Department of Computer Science, Guru Nanak Dev University, Amritsar. He has more than 17 years of experience of teaching and research and has more than 27 publications. His research interests are Distributed Database, Artificial Intelligence and Soft Computing.

Jyoteesh Malhotra is Associate Dean of Academics, Student Welfare and Professor and Head in the Department of Electronics and Communication Engineering and Department of Computer Science and Engineering in the Regional Campus Jalandhar of Guru Nanak Dev University, Amritsar. He received PhD, M.Tech (Gold Medalist) and has more than 20 years of experience of teaching and research. He has more than 170 publications of International and National repute in his credit. His research interests include Wireless Networks and Optical Communication.