Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust

Preeti Sirohi[*]and Amit Agarwal[†]

[*] Institute of Management Studies, Ghaziabad Preeti.sirohi@imsgzb.com
[†]Department of Computer Science,UPES, Dehradun, India Aagrawal@ddn.upes.ac.in

***Abstract*—Cloud Computing is next generation computing technology with the dynamic capabilities of adding new resources and services as per user demand and requirement. Cloud computing is fast growing technology which facilitates more and more users and organizations shifting towards opting their services to cloud. Data security is considered as the constant issue leading towards a hitch in the adoption of cloud computing. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing. The advent of the proposed model has sufficient functionalities and capabilities which ensures the data security and integrity. The proposed framework focuses on the encryption and decryption approach facilitating the cloud user with data security assurance. The proposed solution only talks about the increased security but does not talk about the performance. The solution also includes the functioning of forensic virtual machine, malware detection and real time monitoring of the system. In this paper, a survey of different security issues and threats are also presented. A data security framework also provides the transparency to both the cloud service provider and the cloud user thereby reducing data security threats in cloud environment.**

Keywords: Data security, Privacy, Integrity, Trust, Cloud Computing.

I. Introduction

Cloud computing is considered as the future or the next generation computing paradigm for enabling convenient, on demand network access to the shared computing resources. The technologies behind the success of Cloud computing is Virtualization, Service Oriented computing , Utility Computing , Load balancing, Multi-tenant environment, the ability of pay per use of computing resources reducing large capital expenditures and operational overhead [1]. In spite of having several benefits of cloud computing data security, privacy, integrity and trust are few major hindrances for the wide acceptance of cloud computing [2]. Cloud user require the safety of their sensitive data from tampering or an unauthorized access. The cloud computing platform faces the internal and external security threats, various outages and security threats to the cloud services from time to time. The alliance cited the case of Mat Honan, a writer for wired magazine, who in summer of 2012 found an intruder had broken into his Gmail, Twitter and Apple accounts and deleted all the baby pictures of his 18-month old daughter [4]. There is a serious requirement to address the data security issues for preserving the data integrity, privacy and trust in the cloud environment.[19]. Various algorithms and protocols have been designed in the past (MD5, RSA, PDP, PoR) and are implemented in order to maintain the issues related to data privacy, integrity and trust[20], [21].

The Objective of the research is protection of data from various data security threats such as data privacy, data integrity, and data trust lying in cloud environment. The paper provides the Encryption of the sensitive data which scare the prospective consumer and the organization to use cloud computing services their sensitive data.

The paper will help and motivate the researchers for further investigation of security solutions that will help in the trustworthy cloud environment [5]. The data security model is proposed which will provide a better security to the data of the cloud user. Authentication of data at various level will lead to more data security. The real time monitoring , use of forensic virtual machine and various encryption techniques will lead to data security , data privacy, data integrity and trust.

II. RELATED WORK

This section illustrates the related work on data security. There are few approaches and models earlier proposed by various authors for ensuring the data security in a compliant ways. The author of the Paper [18] proposed an adaptive privacy management system where some of the highly sensitive was encrypted by using predefined privacy policies. In paper [17] author proposed Anonymity based algorithm for cloud computing services which process the microdata also sending the anonymous data to the cloud provider for integrating the data with additional information and can get the result. In paper [10] Temper proof cryptographic coprocessor which is configured by trusted third party are also proposed by author. Temper proof facilitates a secure execution domain in cloud computing that is physically and logically protected from unauthorized access.

In paper [7] the author talked about RACS technique which is redundant array of cloud storage technique to avoid vendor lock-in and also reduce the cost . The author of the paper [8] presented the privacy manager for protecting the data being stolen or misused and also assisting the cloud computing provider to conform the privacy law by describing the privacy architecture to protect private data. The above approaches are good for providing the security to the data but somewhere the performance is compromised.

In paper [9] the author proposes an approach for public audit and preserve data at cloud. The author talked about the

978-1-4673-6809-4/15/$31.00 ©2015 IEEE

public availability of cloud stored data for security. Third party auditor (TPA) talks about auditing the cloud data storage with no additional on-line burden to the cloud user also bringing no vulnerabilities towards user data privacy.

III. DATA SECURITY IN CLOUD

In traditional data security, various techniques were used for processing and protecting the sensitive data. To secure outsourced data, Encryption technique was commonly used technique for data security. Downloading all the data and decrypting it at local site is not very cost effective as huge bandwidth is required for decrypting at local site associated with the process. Another major security concern arises in outsourcing data is the proof of ownership which prevents the user from the exposure to his own data. The Outsourced data is handed over to the remote service provider but the owner himself is not aware about the storage of the data. Other challenging security problem is the disaster recovery. It depends on the service provider handling of the data in case of disaster which can occur in case of the remote hard drive failures due to vulnerabilities on cloud [2]. As the data to be stored is increasing day by day diminishing the security mechanism, the traditional security techniques are not that useful. The provider is handling critical and sensitive data of a customer, which does not always guarantee the data integrity, privacy and trust [16].

According to the author of the paper [4] the top threats to cloud computing are: abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile.

A. Data Privacy

The data is expanding day by day leading towards several security issues in which data privacy is one of the security challenge associated with cloud computing. The privacy threats faced by cloud computing are the complexity associated with the risk assessment, growing industry demands the emergence of timely delivery of new business models and its implications on consumer privacy , various regulatory compliance, data privacy issues in design leading towards poor data quality and also lack of transparency [13]. The Privacy Impact Assessment (PIA) to the cloud users is carried out by the Information Commissioner Office in United Kingdom (ICO) is responsible for using protocols and standards for accessing and using of the personal information in the cloud.[22]. Data privacy protocols are related to the data and software transfer protocols, data processing protocols will influence the privacy of the data on cloud [23].

B. Data Integrity

The data integrity is useful for the validity of data and also promising the reliability and uniformity of data. Lack of Integrity is a major threat in the cloud environment, there are many security risks and attacks due to the data Integrity issues. Data integrity assures the user that no modification or tampering of the data will be done without users knowledge. Data integrity is at risk when the intruder or anonymous user gains access over the stored data. The attack done on the user data can be data modification attack, data leakage attack and Tag forgery attack. Integrity monitoring of data is essential for avoiding data corruption and data crash in the data centers. In cloud computing the architectural design sometimes lead to the integrity issue [24]. Various mechanisms are adopted for preventing data integrity attacks on the cloud environment such as cooperative provable data possession (CPDP) which is the combination of hash indexing hierarchy and Homomorphic verifiable response [25, 14].

C. Data Trust

Trust is the major concern is and it breaks if two issues are not handled properly one of them is lack of transparency and other is due to breach in security and privacy. The cloud service providers offer flexibility to the use of resources which attracts consumers of cloud computing to get benefitted from the service by involving their sensitive data at risk. The consumers are unaware of the technology involved and control of the data as they are solely dependent on contracts and trust mechanism. Trust is a complex term and it is based on the positive approach or behavior of other. Trust is based on the security which the cloud service provider gives to its customers. Reputation also plays an important role in building the trust in the relation between the cloud vendor and the cloud consumer. Furthermore, trust mechanisms need to be propagated right along the chain of service provision [12].

Trust can be enhanced if the cloud provider isolates the data without violating the integrity and the privacy issues in the multi tenant environment. Transparency in storing of data and unhiding the unnecessary information from the user will built a level of trust and understanding between the cloud provider and the user [28]

IV. PROPOSED DATA SECURITY MODEL IN CLOUD

In this section a new model for data security in cloud computing environment using the information stated in the previous section is offered. This paper enhances traditional data security model for cloud computing. The proposed data security model use a three layer system structure in which these layers are used for ensuring data security. In proposed model, all the techniques and mechanism useful for implementing a highly protected environment is developed. The end user will access the cloud through internet and for that strong log in access is provided to the user. The high security login feature in the model will prevent the user with malicious intent to use the data stored on the cloud. The software encrypts and protects data at various levels by using various security techniques and security algorithms. The proposed model ensures that protection of the user confidential information by ensuring faster retrieval of the data using security intelligence and advanced security data protection

The proposed framework consist of three main layers which will interact with each other to provide data security. These are: *The first-layer :* This layer is responsible for the authentication of the user, in this layer the cloud service provider can use their authentication methods for ensuring

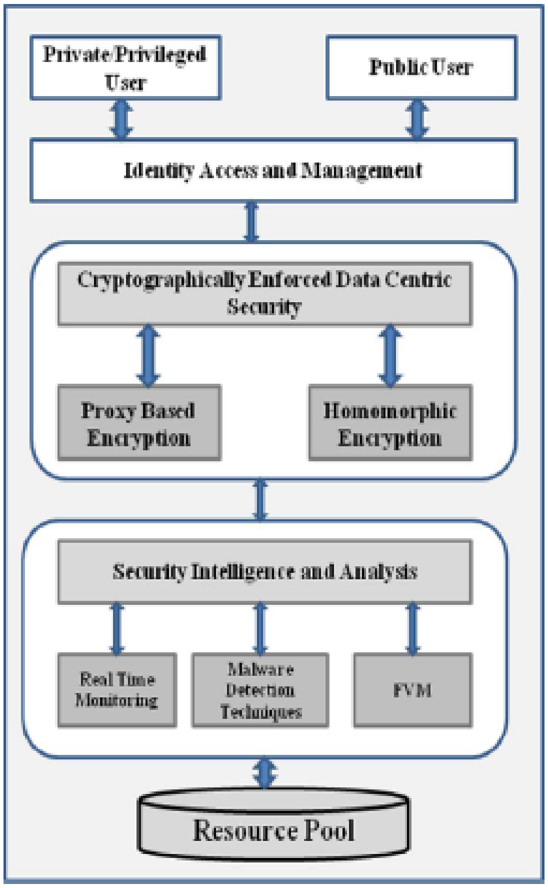
Private/Privileged User
Public User
Identity Access and Management
Cryptographically Enforced Data Centric Security
Proxy Based Encryption
Homomorphic Encryption
Security Intelligence and Analysis
Real Time Monitoring
Malware Detection Techniques
FVM
Resource Pool

Fig. 1. The proposed Data security framework in cloud environment.

the genuine user. The methods which are used for the authentication of data are one time password, two factor or multi factor authentication, short message service, fast identity online alliance [15]. The main task of the layer is to prevent the unauthorized user and processes entering in the cloud environment *The Second layer:* This layer communicates with the previous layer to make sure that only authorized user can send the receive the data. This layer has cryptographically enforced Data Centric Security. This layer follows practices of various encryption techniques which are responsible for enhancing the data privacy and data integrity in cloud computing. Proxy Based encryption and Homomorphic Based encryption methods are used in the proposed data security framework to achieve a practical preferred solution for data security in cloud computing. Proxy based encryption approach when used in cloud environment works on the principle that the data is encrypted as soon as it leaves from the cloud users organization and decrypted before the data reaches to the desired destination in the network. Homomorphic encryption allows the processing of the encrypted data without using decryption process. The secret key lies with the owner in the whole process. This approach is very much useful for ensuring data security in the cloud scenario. *The Third layer:* This layer is responsible interacting with the second layer and ensures that user requested the data for processing from storage is genuine. High level of data security is implemented in the form of security intelligence and analysis. At this layer advanced security features to protect the data before storing the data in the resource pool. This layer will enhance the security of data in the cloud architecture. This layer have the advanced features like real time monitoring, forensic virtual machine and data masking which are used for the protection of users data[16].Real time data monitoring will help in managing the consumption of resources by continuously monitoring the use of data and the functions performed on the data in the real time. Forensic virtual machines are used for monitoring other virtual machines in real time. On detection of a malware symptom FVM will exchange message with other machines about the presence about the symptom. FVM will also report to the centre that will check on the reported issue of the FVM.

Resource Pool- Resource pool is responsible for storing and managing all the user data and provides the appropriate information to the user as and when requested without delay. This layer is a resource pool from which the user can access the data. The data security models and proposals discussed above describes its own way for finding solutions to the data which is at risk and improves data security in cloud computing and deals with the data storage correctness. Dynamic detection of risk and finding their solution is still not clear and there are lots of risks which are still involved distract the users from cloud [11].

V. CONCLUSION AND FUTURE WORK

Cloud computing is common these days and more and more users are adding to the cloud environment leading towards security issues related to the data. This paper presents an overview on the data security problem associated with the cloud computing. This paper talked about various threats associated with data security in cloud computing describing briefly data integrity, data privacy and data trust associated. The model is proposed talks about three level authentication mechanisms for improving security to the data as compared to the old traditional system. Although the additional responsibilities will be added to the provider in implementation of highly secured data access network but the proposed model will minimize the issues discussed in the previous section.

In data security privacy, Integrity and Trust are some of the bench marks which helps in the evaluation of the secured system. The proposed model is helpful in building the well highly secured data security system. The proposed model is related specific to the data security in all the three layers of the cloud services which are offered to the cloud user by the cloud provider. The futuristic issue of data security in cloud computing opens new challenges such as Data locks by cloud provider, fault tolerance and disaster recovery mechanisms in cloud computing.

REFERENCES

[1] D Meng, Data security in Cloud Computing, Computer Science and Education (ICCSE), 2013 8th International conference, 2013, pp 810-813

[2] A. Shawish and M. Salama, Cloud Computing: Paradigms and Technologies, F. Xhafa and N. Bessis (eds.), Intercooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, DOI: 10.1007/978-3- 642-35016-0_2, Springer-Verlag Berlin Heidelberg 2014

[3] R. Yadav, N. Yadav, Monika and A. Seharawat, Cloud Computing: Flowing Model in IT Services,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015

[4] Babcock and Charles. ”9 Worst Cloud Security Threats Leading Cloud Security Group Lists the ”Notorious Nine” Top Threats to Cloud Computing in 2013; Most Are Already Known but Defy 100% Solution,” Information Week. UBM Tech Sites, 3 Mar. 2014. Web. 12 Mar. 2015. .

[5] Y. Sun, J. Zhang, Y. Xiong,and G. Zhu, Data Security and Privacy in Cloud Computing, International Journal of Distributed Sensor Networks, Volume 2014, Article ID 190903

[6] T.Ristenpart et.al.,Hey you, Get Off of my cloud! Exploring Information Leakage in Third-party Compute Clouds Proc. 16th ACM Conf. Computer and Communications Security (CCS ACM Press, 2009,PP 199-212.

[7] A.Libdeh, L. Princehouse, and H. Weatherspoon, RACS: A Case for Cloud Storage Diversity, SoCC 10:Proc. 1st First ACM Symposium on Cloud Computing ,2010, PP 209-240.

[8] S. Pearson, Y. Shen and M. Mowbray, A Privacy Manager for Cloud Computing, Cloudcom2009, LNCS 5931, PP 90-106, Springer 2009

[9]] D.Prasad , B. R. Singh , M. Akuthota and M. Sangeetha, An Etiquette Approach for Public Audit and Preserve Data at Cloud, International Journal of Computer Trends and Technology (IJCTT) volume 16 number 1 Oct 2014

[10] W. Itani, A. Kayssi and A. Chehab, Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009

[11] H. B Patel,D. R Patel, B. Borisaniya and A. patel, Data Storage Security Model for Cloud Computing, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012, LNICST 108, PP 37-45, 2012

[12] S. Pearson and A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science, Cloudcom-2010.66, PP 693-702

[13] D. Chen, Data security and Privacy Protection issues in Cloud Computing,Computer Science and Electronics Engineering (ICCSEE) International Conference, 2012, PP 647-651

[14] A. Jaberi , M.F Data integrity and Privacy model in cloud computing, Biometrics and Security Technologies(ISBAST)2014, PP 280-284

[15] N. Jose and C. Kanmani, Data Security Model enhancement in Cloud Environment, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 2 , PP 01-06

[16] B. Goswami, and Dr..S.N. Singh, Enhance security in cloud computing using public key cryptography with matrices, International Journal of Engineering Research and Applications,vol.2,issu.4,pp.339-344,2012

[17] D W. Chadwick and K. Fatema, A privacy preserving authorization system for the cloud, Journal of Computer and System Sciences , 2012, PP 1359-1373

[18] C. Mont, and Pearson, An Adaptive Privacy Management System for Data Repositories, Trust, Privacy and Security in digital business, Volume 3592, 2005, pp 236-245

[19] Khan, S.M. and K.W. Hamlen., Anonymous Cloud: A Data Ownership Privacy Provider Framework in Cloud Computing. in Trust, Security and Privacy, Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. 2012

[20] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 2011. 34(1): p. 1-11.

[21] C. Ning., et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data, INFOCOM, 2011 Proceedings IEEE. 2011.

[22] S. Pearson, Taking Account of Privacy when Designing CloudComputingServices,”ICSE’09 workshop,Vancouver,canada,978-1-4244-3713-9-09,IEEE,Page no 44-52 (2009)

[23] C.Saravanakumar and C.Arun, Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing, Contemporary Computing and Informatics (IC3I), 2014, pp 997- 982

[24] S. Meena, E Daniel and Dr. NA. Vasanthi, Surveyon Various Data Integrity Attacks in Cloud Environment and the Solutions, International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], pp 1076-1081

[25] Y. Zhu, H. Hu, G. Ahn, and M. Yu, ”Cooperative provable data possession for integrity verification in multi-c1oud storage,” IEEE Transactions on Parallel and Distributed Systems, no. 99, 2012

[26] BKSP, R. Kumar, G. Geethakumari, A Model for Trust Enhancement in Cloud Computing, A Model for Trust Enhancement in Cloud Computing 2014, PP 1-5