ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Survey on Privacy Preserving and Data Security Solution on Cloud Computing

Sonali B Patil

M.E Student, Dept. of Computer Engineering, SES'SFOEGOI College of Engineering, Diksal, Raigad, Maharashtra, India.

ABSTRACT: Cloud computing is a rapidly growing model of computation in which resources of the computing infrastructure are provided as services over the Internet. It provides the computing services such as shared resources, software and information over the internet. The user can store his data at any time and from any part of world through network in cloud storage. Cloud computing is network based technology therefore some security issues occurred like privacy, data security, confidentiality etc. In cloud computing, number of user use cloud services at a time which increases the data load in cloud storage, also increases the risk of data vulnerability. Hence, the data security and privacy must be provided in cloud computing models. The paper mainly focuses on encryption techniques to resolve the problem of data security and privacy. This paper makes a survey on different solutions to provide data security and privacy in existing cloud computing scenario.

KEYWORDS: authentication, cloud computing, encryption techniques, cloud security, privacy.

I. INTRODUCTION

By enjoying data storage and sharing services in the cloud. The cloud computing becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The users can access your applications and data from anywhere. Resources in cloud systems can be shared among a large number of users. The cloud system could improve its capacity through adding more hardware to deal with the increased load effectively when the work load is growing.

Emerging cloud services are becoming indisputable parts of modern information and communication systems and step into our daily lives. User store the sensitive information on cloud is there any cloud service secure and provide privacy preserving authentication of users. There are few cryptographic tools that can both hide user identity and provide secure communication. There are few cryptographic tools and scheme like anonymous authentication scheme, group signature, zero knowledge protocols that can both hide user identity and provide authentication. The cloud service providers control the process of authentication by giving the permission to valid users only.

II. ENCRYPTION USED IN CLOUD

Encryption provides authenticity, confidentiality and data privacy in cloud environment by using number of keys. Where datais encrypted by using encryption key and data is decrypted with the decryption key. This process is easily performed when it applies on small data or information, but if the data is very large, it will take long time. When encryption is used in cloud environment, it may affect its end to end performance and it is hard to implement and deployment in cloud environment so far. In this section, we studied some well known standard encryption algorithm like DES, AES, RSA, ECDSA and customized encryption techniques like Identity & Attribute Based, which are using widely in cloud architecture currently.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

III. SECURITY ISSUES

Cloud computing provides flexibility, reliability, availability, performance and much more in our computing experience but, behind of it, there are various security issues found on this modern computing model. Data security issue comes in light, when cloud model became famous and found large number of users/clients. Due to wide accessibility of cloud model, it is also used to store massive volume of data but available data security and privacy mechanism are still not enough to protect it. Trust, confidentiality, privacy, integrity and availability these types of security issues found in cloud environment.

A. Trust

Trust is most critical part in cloud cloud computing system. In cloud computing environments, the customer is dependent on provider for various services. In many services, the customer has to store his confidential data on the provider's side. Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements [9]. In cloud deployment model trust is conceal so far. Trusted Third Party is introduced by some private organizations for maintaining trust on present cloud computing scenario. This party also has their data policy and encryption mechanism to provide authorization of data and communication [8].

B. Confidentiality and Privacy

Confidentiality means secrecy; it means the Information is secret and not disclose to others. In cloud computing model, users are uploading the information or data or files in cloud storage. This information may be personal then, it needs privacy from unauthorized persons [10].

Privacy is related to the personal information, must be hide and protected from unauthorized persons. It controls the discloser of private data and make it confidential, which allows either authorized users or systems those have privilege to acquire secured data. In cloud based model the storage server are not in single locations, instead of this they are distributed in different locations. In each location the data uses policy is changed, hence it increases the risk of privacy breach [10].

C. Integrity and Availability

Integrity means that assets can be modified only by authorized parties or in authorized ways. Integrity may be associated with data, software and hardware. In cloud environment, user's data or files is replicated in various storage servers over different locations, hence it may increase the risk of breach in their integrity and accuracy [11]. In cloud computing, solution integrity refers to the ability of the cloud provider to ensure the reliable and correct operation of the cloud system in support of meeting its legalObligations [9] Availability allows the property of a system is accessed and used by an authorized entity. It also provides the capability to serve even though possibility of a security infringement or system failure. When the data is in remote location owned by cloud service provider, consumer would have to deal with system failure. Availability always refers to data, software must be available to authorized users upon demand. Data will not be available if there is an operational issue in cloud [12].

IV. RELATED WORK

Privacy-preserving cloud computing solutions have been developed from theoretical recommendations to concrete cryptographic proposals. There are many works which deal with general security issues in cloud computing but only few works deal also with user privacy.

The authors [1] estimate the cost of common cryptographic primitives (AES, MD5, SHA-1, RSA, DSA, and ECDSA) and secure outsourced data. The authors deal with the encryption of cloud storage but do not mention privacy preserving access to cloud storage.

In paper [2], proposed a system for information storage security. There were 4 algorithms "Keygen, SigGen, GenProof, VerifyProof" [2]. Keygen is for key generation, used by user, SigGen is used for verification Meta data by user, GenProof is for a proof of correctness of data storage, run by the cloud server, and VerifyProof is used to audit the proof from the cloud server by "Third Party Auditor (TPA)" [2]. There are two phases in this Public Auditing System, one is Setup and second is Audit. Setup includes KeyGen and SigGen algorithm. Audit includes GenProof and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

VerifyProof algorithm. In this paper, concept of "homomorphic authenticator and random masking"[2] utilize by authors, which affirm that TPA would not have any information of the stored data [2].
In paper [3], provides fine grained access control and authenticate users without knowing their identities before storing information. Only validate user can write on the cloud and invalid user does not get access to the cloud and the author does not provide any cryptographic solution.
In paper [4], it uses AES encrypted algorithm to encrypt user data before upload on cloud. The author proposes cryptographic solution for privacy and also reduces the risk of the leakage of user private information.
The authors[5] proposes security solution for privacy preserving cloud services, which provides anonymous access to users with the help of authorization proof sign and authorization proof verify. Verification process of user Access must be efficient and the computational cryptographic overhead must be minimal. Revocation manager has capability to revoke malicious client and reveal their identities. Data confidentiality and integrity are secured by a symmetric cipher but it is not completely safe.
In paper [6], NasrinKhanezaei proposed a secure cloud storage services scheme. This scheme has combination of asymmetric and symmetric encryption techniques (i.e. RSA and AES encryption methods) to achieve the security of cloud data, which provides secure communication between cloud service providers to user.
In paper [7], PrashantRewagad proposed cloud data security architecture. The proposed architecture has three way protection schemes. First protection scheme is Diffie Hellman algorithm for key exchange securely. Second scheme includes digital signature for authentication purpose and third scheme includes AES encryption algorithm for encrypt/decrypt the user's data file. The above schemes are implemented separately from storage servers.

V. PROPOSED SYSTEM

The number of techniques for providing privacy and security we analysed. We will implement the system, different combination of mechanism which provides privacy and security. Mechanisms are authentication, anonymous authentication for registered users. For the method used for security in cloud for affixstorage and access of data in cloud which is ECCseems more suitable and efficient algorithm for thefurther work to be proceeded. The proposed work also provides the confidentiality and integrity of transmitted data between users and cloud service providers by storing data of data owners to the data servers.

VI. CONCLUSION AND FUTURE WORK

Cloud computing is a fastest growing technology. But it still has many disadvantages among which a major problem is privacy preserving of cloud data and cloud security. User wants a secure gateway to access its private information securely. The above discussed methods provide various solutions to preserve privacy and provide security on data. but User to cloud provider (and vice versa) security has been difficult to achieve so far due to the complexness of the cloud and hence user wants the advanced security techniques to be developed.
Our future work will focus on implement efficient encryption solution that should be adjusted in each part of the cloud and provide complete solution of data privacy & security , provides the most security between cloud service provider and user(by providing some authorities to data owner also). We also focus on security issues such as confidentiality, integrity, availability, privacy..

REFERENCES

1. Y. Chen and R. Sion, 'On securing untrusted clouds with cryptography', in Proceedings of the 9th annual ACMworkshop on Privacy in the electronic society. ACM, 2010, pp. 109– 114.
2. Cong Wang, QianWang, and KuiRenWenjing Lou, 'PrivacyPreserving Public Auditing for Data Storage Security in Cloud Computing',IEEE INFOCOM 2010, pp. 1-9.
3. SushmitaRuj, Milos Stojmenovic and AmiyaNayak, 'Privacy Preserving Access Control with Authentication for Securing Data in Clouds',in proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp. 556-563.
4. DebajyotiMukhopadhyay, GiteshSonawane, ParthSarthi Gupta, SagarBhavsar, Vibha Mittal." Enhanced Security for Cloud Storage using File Encryption" Department of Information Technology Maharashtra Institute of Technology,2013
5. L.Malina and J.Hejny" Efficient Security Solution for Privacy-Preserving Cloud Services" 6th international conference on telecommunications signal processing year 2013, pp. 23-27.
6. NasrinKhanezaei, ZurinaMohdHanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services," IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 -14 December2014, pp. 58-62.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

7. Mr. PrashantRewagad, Ms.YogitaPawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication Systems and Network Technologies 2013, pp. 437-439.
8. DimitriosZissis, DimitriosLekkas, "Addressing cloud computing security issues," Future Generation Computer Systems 28 2012, pp.583-592.
9. HuagloryTianfield, "Security Issues In Cloud Computing"IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012,pp. 1082-1089.
10. Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology Special Publication 800-144 80 pages December 2011.
11. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thorn "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences,2012, pp. 5490-5499.
12. Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", lRACSTInternational Journal of Computer Science and Information Technology & Security (lJCSITS) Vol. 1, No. 2, December 2011,pp. 136-146.

BIOGRAPHY

Sonali Bapu Patil is a student of ,SES'SFOE College of Engineering, Diksal, Raigad, Maharashtra, India. She pursuing Master of Engineering (M.E) degree in Computer Engineering branch from Mumbai University .Here the survey paper on cloud security.