International Innovative Research Journal of Engineering and Technology
ISSN NO:2456-1983

International Conference on Emerging Innovation in Engineering and Technology
ICEIET-2017

Multilayaered Security Framework For Cloud Data Based On Privacy

V.Geetha[1], D.Indhumathi[2]
[1]Associate Professor, Pondicherry Engineering College, Puducherry-605014, India
[2]PG student, Pondicherry Engineering College, Puducherry-605014, India

[1]vgeetha@pec.edu
[2]mathi01993@gmail.com

ABSTRACT

Cloud computing is one of the prominent technology and it is a rapid growth with minimum investment over the internet. Providing the data in cloud both consumer level and provider level follow the common encryption method but there are techniques to access the encryption data .Tackle the problem of security, data security is one of the major issues in cloud. The continuous increase of computational power has produced an overwhelming flow of data framework is a conceptual structure mainly focuses on serve as support. So multi-layered data security is provided. Several framework and layers are implemented based on the type of data. Our paper mainly target on data security in cloud by multi-layered approach which results in reduce in computation time, speed of processing be increased, Efficiency be increased .Types of framework are: private cloud framework, public cloud framework, hybrid cloud framework. Cloud environment has large of data to transfer and storage. Security issues in cloud are data breaches, hijacking of accounts, insiders threat, malware injection, abuse of cloud service, insecure API's,deniel of service attacks, insufficient due to diligence, shared vulnerabilities ,data loss.

Keywords: data security, multi-layered approach, framework, types of framework, layers of framework.

I. INTRODUCTION

Cloud computing is a technology can retrieve the data form anywhere over the internet .Main advantage is pay per use, low infrastructure cost. In pay per use it is a market dependent here the customer is played based on market condition it a pay per use model in which the consumer has to pay based on pricing among the consume of the product .consumer's interest trying to purchase the product at the lowest price. Cloud computing is a pay-as-a-go model. organization motive is to maximize the profit with minimize the risk when moving to a cloud.it has advantageous of deliver lower IT cost by initially lower because every equipment is rented not bought, it has longer lifespan than on-promise because the software is easily updated and managed in the cloud .system resources is low because of provider will manage the contour, upgrade and maintenance.

It has disadvantages of downtime, unplanned downtime will cause the bad outcome in cloud and will affect in unproductiveness of business. In SME environment different level of group in enterprises based on the level of groups the information be provided .These issues fall into two broad categories: security issues faced by cloud providers and security issues faced by the customers.The issues faced by the providers is organizations providing software-, platform-, or infrastructure-as-a-service via the cloud and issues faced by their customers companies or organizations who host applications or store data on the cloud.the responsibility to provide the data security in cloud and also provide reduce time consumption ,reduce the data loss.in order to safeguard the resources and maintain efficiency .user stored the data in cloud .there is chance to hack that data .so provided with strong security ,data integrity ,privacy, data encryption method and policies to maintain the data in cloud. Data security provided with data confidentiality, data access controllability and data integrity.data confidentiality be provided with only licensed users only access the data. Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to cloud.Legal users can be authorized by the owner to access the data, while others cannot access it without permissions. Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that his data in a cloud can be stored trustworthily.In public cloud the security are provided by the another party cloud service provider. Private cloud offers more control over the security parameterto very accurate and precise inference, as uncorrelated errors are removed because of multiple base classifiers.

II. EXISTING DATA SECURITY TECHNIQUES

A. Authentication
B. Authorization
C. Intrusion detection
D. transparency
E. Trust management
F. Identity management
G. Encryption
H.

I. A. *Authentication*

J. It is a computer to know its identity to the server. Generally authentication deals with identity to server by means of username and password then it improve with the retina scans ,cards, fingerprint and voice recognization. Authentication does not determines what the individual task has done, it deals with the identify and verify who the person.

A. Authorization

Authorization is a process of server determines the authorization to access the resources and access a file.Auhtorization linked with authentication who client the seek the resources to access it.The type of authentication vary for authority, the password required for some cases but not in all cases.

B. Intrusion detection

IDS can play a vital role in cloud computing for detection of false alarm, attacks .a better IDS will able to detect the origin and abnormal activities .Provider will deploy ID in certain location and feed into your intrusion detection system.

C. Trust management

Provide the trust management in cloud by means of various cryptographic techniques.

D. Transparency

Transparency deals with consider the potential risk and threats as well as create and develop the right countermeasures for the enterprises. Transparency lead to leak the personal information related to credit card details it leads to several disadvantages in case of cybercriminal activities.

E. Encryption

It is a process of encrypt the plain text .in cloud the security is one of the major issues in cloud. If the cloud is breached, the information is available to the hackers.so client could encrypt the data before upload the data in cloud.

- Elliptic curve cryptography
- Chaotic cryptography
- Quantum cryptography
- Homomorphic encryption.

III. SURVEY ON ENCRYPTION

Nidal Hassan Hussein et al,[12] it surveyed about the cloud storage for cryptography, in cloud storage architecture it has three components are data processor, data verifier, token generator.it has various algorithm and cryptography techniques.benifits and drawbacks are cryptography storage.benifits are confidential assurance, geographic restriction, reducing risk of security breaches, data retention and destruction, electronic discovery and subpoenas. Drawbacks of cryptographic storage are security and privacy.

Jianjun Zhanga et al,[15] discussed about privacy preserving searchable encryption scheme goals to achieve the privacy for the cloud server. These paper it gives the privacy requirement features like keyword privacy, index confidentiality, query confidentiality and trapdoor unlinkability.Advantages and disadvantages of semantic searchable encryption scheme, and it introduce the smart semantic searchable encryption scheme, and its advantages is security word net is used to expand the query.

Junggab Son et al,[16] it proposed about group sharing in cloud environment. Proposed method is conditional proxy Re-encryption (CPRE) its deals about whenever the group changes the data needs to download all of the existing data on the cloud, encrypt them again with a new condition value, and uploads them to the cloud. Then (O-CPRE) outsourcing for secure for big data sharing in cloud environment. Advantages is cost of expensive is reduced the conditional value is significantly reduced and burden of client is reduce.

Punam V. Maitri et al,[17] it discussed about .Cryptography and steganography techniques are more popular now a day's for data security.Surveyed about AES, blowfish, RC6 and BRA algorithms are used to provide block wise security to data. All algorithm key size is 128 bit.LSB steganography technique is introduced for key information security.comparsion with all the algorithm with proposed system. The advantages is Data integrity is accomplished using SHA1 hash algorithm. Low delay parameter is achieved using multithreading technique .the future work discuss with high level security using hybridization of public key cryptography algorithms.

Zhenxing Qi an et al,[18] it proposed a reversible data hiding in encrypted images(RDH-EI) by recovery progressive method.it has the content owner, data hider, data recipient.in content owner encrypt the original image and send to server. The duty of data hider has divides the encrypted image. Finally the data recipient extract message using extraction key. Finally the original image be lose less image recovered by progressive recovery. Embed message into three LSB-layers of the encrypted image. Table shown the maximum embedding message and figure shown with rate distortion comparison. These paper increase the embedding rate.

NEED FOR SECURITY FRAMEWORK

Framework defines the security based on customer perspective, provider perspective. A customer expects on demand service, security and reliable service. Provider expects a framework protecting the business details .cloud framework is an open source. Evaluate the component of framework by the level (infrastructure, software or both) it

has the complete structure to develop the security, privacy to cloud and gives the set of rules and policies.

IV. SURVEY ON FRAMEWORK

There are several security framework proposed for cloud data in the literature.

Mohamed Almorsy et al .[2] proposed a security framework based on FISMA standard to fit the cloud provider and consumer to be secured .It has various security service related to security are security service categrorization,security service implementation, security control assessment ,security control assessment, security control assessment, security authorization for stakeholders to maintain the security needs.it has three layers first is management layer and it is for security for consumer ,service provider next enforcement layer for identified risks and feedback layer for monitoring the security service.

Daniel.moritz et al, [3] suggested a framework for tele lab for flexibility and resistance. Tele lab consists of front end and backend, front end consists of web application and backend service for virtual management.The Tele-Lab architecture supports this approach by using XML-RPC as the standard communication channel.The usage of a private cloud framework leads to a much more stable and scalable Tele-Lab.

Devi T et al, [4] surveyed on the data security framework in cloud. A new framework namely hybrid model, and these paper provide the hyper elliptic curve cryptography (HECC) and hashing algorithm for security to cloud..SHA 3 for data integrity and make computation easier for longer message size. Main objective of these paper is to provide data integrity, data security and user authentication.

Glen ford Map and Mahdi Aiash et al, [7] has presented about the new security framework for cyber security and provide the cloud storage security .these paper modify the IP V6 to capability ID system for user, application and cloud infrastructure .capability unit (CU) for in which the computation be performed only the right capability loaded in CU.The new capability format is type, property field, object ID, random bit field, hash field. Current work going on secure transportation on LAN /cloud environment. These paper mainly focus on E-health system for patient monitoring the system at their homes and storing the data in public cloud environment.

FatmaMasmoudi et al, [5] interested to solve the security issues in cloud .in these paper it follow a three level approach 1.modelling 2.specification 3.verification.complexity of cloud be solved by modelling step (cloud consumer, cloud broker, cloud provider) it follows NIST concept with layers in Interface layer for display and interaction with consumers, middle layer that offers both control and execution services, and physical layer for physical equipment. It treated the property of isolation where security rules must guarantee virtual and physical isolation of an SEE.We used the proof tool/EVES to check whether the specified system respects isolation. Advantage is reduce the complexity of cloud system.

Rui Zhang et al, [8] it gives the solution to public verifiability and information security for searchable encryption scheme.it generate the PVSAE for encryption ,IND CKA for security and search pattern privacy. Another technique is 3 PVSAE for strong encryption.it also describe about relevant work of encryption scheme. These paper show the efficiency of PVSAE in terms of search and verification. The total search complexity for whole search process is equal to the values in the table multiplied by n, where n is the total number of keywords. We observe that our 3PVSAE scheme is much more efficient than VAVKS.

Dharmendra S. Raghuwanshi et al,[9] has deals with achieving data security with various encryption approach at file level and block level. In file level the data be encrypted before upload to the cloud.in block level the EBS level to achieve the security with additional storage level .then hybrid approach for encryption at both file level and block level and another encryption is disk encryption method has illusion accessing encrypted data not original data.it describe the pros and cons of various encryption methodology and best one is homomorphic for data privacy in cloud. Illustrating the performance overhead in terms of additional time taken in uploading and downloading with encryption over Normal uploads and downloads for same size of objects. Performance chart clearly shows that performance overhead is reasonable and can be ignored on the account of security. For both cloud provider and consumer perspective the proposed integrated data encryption approach for data security and privacy.

M.V. Shalala et al,[10] discussed about the security to cloud private cloud framework .in these framework it has access right delegator, preference setting, alert and information events and access log analyser. Mainly the information events and access log analyser it retrieve the specific logs using some filters. Checked with privacy monitoring tool main motto of these paper to privacy for transparency. Finally the graph shown the when the number of users increased and response time also increased. The main advantages is security, Forensic investigation. Future issues are more control over personal information.

Vijayanand K.S et al,[11] it proposed a framework for security for multiple cloud service provide for hybrid cloud environment .in these paper the data be split into multiple chunks and each chunks be stored in multiple cloud service provider.it discussed about security issues and cahallenges.it has advantages of trusted cloud service provider for reduce risk and data loss. LI Yan et al, [14] has discussed about security framework for web crawler .SSL and simhash is used in these framework.SSL for security.simhash for reduce the duplicate file. Experimental result shown for simhash algorithm for removal of duplicate. Advantages is security and reduce the storage.

Deepak Singh et al,[13] has proposed a framework for security .in these paper it AES, SHA-1,station-to-key agreement protocol for confidentiality, integrity and authenticity. Mainly discuss about authentication for authenticated.it for ring structure server for fault tolerant. Results shown that computational power and time be reduced and it mainly focus on PDA and mobile apps.

V. CONCLUSION

In this paper , a survey of various existing data security techniques of cloud computing and survey about encryption techniques and survey on framework for cloud to give the structure for security for data in cloud and list the table layers and pros and cons of that layer.

REFERENCES

[1] Chakrawarti, Rajesh Kumar, and KajalSinghai. "The architechtural framework for public cloud security." Soft Computing Techniques for Engineering and Technology (ICSCTET), 2014 International Conference on. IEEE, 2014.

[2] Almorsy, Mohemed, John Grundy, and Amani S. Ibrahim. "Collaboration-based cloud computing security management framework." Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011.

[3] Devi, T., and R. Gane San. "Data security frameworks in cloud." Science Engineering and Management Research (ICSEMR), 2014 International Conference on. IEEE, 2014.

[4] Sirohi, Preeti, and Amit Agarwal. "Cloud computing dat a storage security framework relating to data integrity, privacy and trust." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.

[5] Li, Jun, et al. "GEODAC: A data assurance policy specification and enforcement framework for outsourced services." IEEE Transactions on Services Computing 4.4 (2011): 340-354.

[6] Masmoudi, Fatma, MoniaLoulou, and Ahmed HadjKacem. "Formal Security Framework For Agent Based Cloud Systems." Advanced Information Systems for Enterprises (IWAISE), 2014 International Workshop on. IEEE, 2014.

[7] Mapp, Glenford, et al. "Exploring a New Security Framework for Cloud Storage Using Capabilities." Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on. IEEE, 2014.

[8] Humphrey, Marty, Robert Emerson, and Norm Beekwilder. "Unified, Multi-level Intrusion Detection in Private Cloud Infrastructures." Smart Cloud (SmartCloud), IEEE International Conference on. IEEE, 2016.

[9] Raghuwanshi, Dharmendra S., and M. R. Rajagopalan. "MS2: Practical data privacy and security framework for data at rest in cloud." Computer Applications and Information Systems (WCCAIS), 2014 World Congress on. IEEE, 2014.

[10] Saadat, Sara, and Hamid Reza Shahriari. "Towards a process-oriented framework for improving trust and security in migration to cloud." Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on. IEEE, 2014.

[11] Zhong, Hongye, and Jitian Xiao. "Design for a cloud-based hybrid Android application security assessment framework." Reliability, Maintainability and Safety (ICRMS), 2014 International Conference on. IEEE, 2014.

[12] Hussein, Nidal Hassan, Ahmed Khalid, and Khalid Khanfar. "A Survey of Cryptography Cloud Storage Techniques." International Journal of Computer Science and Mobile Computing, pg (2016): 186-191.

[13] "Smicloud: A framework for comparing and ranking cloud services." Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on. IEEE, 2011.

[14] Zhang, Jianjun. "Semantic-Based Searchable Encryption in Cloud: Issues and Challenges." Computational Intelligence Theory, Systems and Applications (CCITSA), 2015 First International Conference on. IEEE, 2015.

[15] Devi, T., and R. Gane San. "Data security frameworks in cloud." *Science Engineering and Management Research (ICSEMR), 2014 International Conference on*. IEEE, 2014.

[16] Raghuwanshi, Dharmendra S., and M. R. Rajagopalan. "MS2: Practical data privacy and security framework for data at rest in cloud, 2014.

[17] Zhang, Rui, et al. "PVSAE: A Public Verifiable Searchable Encryption Service Framework for Outsourced Encrypted Data." *Web Services (ICWS), 2016 IEEE International Conference on*. IEEE, 2016

.

[18] Moritz, Daniel, et al. "Enhancing a virtual security lab with a private cloud framework." *Teaching, Assessment and Learning for Engineering (TALE), 2013 IEEE International Conference on*. IEEE, 2013.

Author Biography

V.Geetha

She is currently working as Associate Professor in the Department of Information Technology in Pondicherry Engineering College, Puducherry , India. She has completed her B.Tech (CSE) in 1990 M.Tech (CSE) in 1999 and Ph.D (CSE) in 2013. She has published around 35 papers in various International Conferences and Journals including Elsevier and Inderscience. Her areas of research include Distributed Objects, Cloud Computing and Data Security

D.Indhumathi

She is pursuing her Master of Technology in the department of Information Technology from Pondicherry Engineering College. She has completed her Bachelor of Technology in department of Information Technology from IFET college of Engineering. Her areas of interest are cloud computing.