Enhancing Data Security in cloud using Encryption Techniques

Tannu[1]

[1]UIET, Kurukshetra University, 136119, Kurukshetra, Haryana,India
Email-id: [1]tannuchanana1990@gmail.com

Dr. Karambir [2]

[2]UIET, Kurukshetra University, 136119, Kurukshetra, Haryana, India
Email-id: [2]karambir@kuk.ac.in

Abstract

In Cloud computing the term 'cloud' that is used in discipline of science and describe the huge number of things. The security models in cloud like authentication, confidentiality, data integrity data recovery, accessibility. It involves cloud services, deployment model, security issues and challenges in cloud computing. Nowadays ,enhancing data security in cloud is a main concern and solution is to use encryption schemes or algorithms-AES (advanced encryption standard) algorithm, SHA (secure hashing function) and mainly purpose of using these algorithms is to store or secure more data in cloud.

Keywords: cloud, security models, encryption, AES, integrity, hash function.

1. INTRODUCTION

Security in Cloud

The major fear in this computing environment is the safety. Security is necessary in cloud computing whether it is Host level, Network level and Application level. At these levels numerous types of security threats can occur. Following association of threats is done on the basis of Amazon EC2 cloud [1].

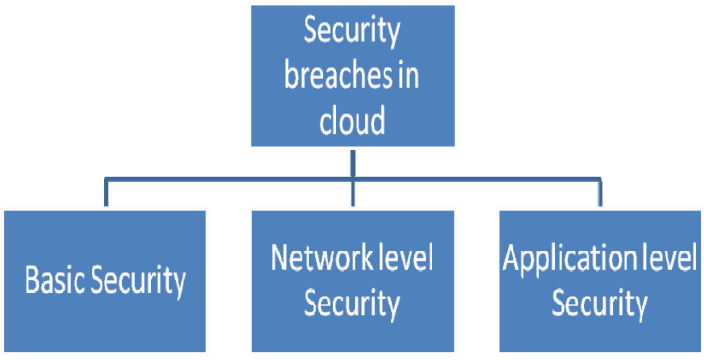

Fig. 1 Security breaches in Cloud

1.1 Cloud computing

The cloud computing term is used for delivery services (such as servers, storage and applications) and delivered to an organizations computers, devices over the internet. The word 'cloud' is to be used in discipline of science

and describe the vast number of things. Cloud computing is also a internet-based computing and in internet based computing the word 'cloud' is to be used like a metaphor for the internet.

1.2 Challenges in Cloud Computing

i. Access: The accessibility is the main challenge in cloud when there is an unauthorized access to the data, the ability of altering on the client data arise.

ii. Availability: The data must be available all the time for the clients without having problems that affect the storage and lead to the client data lose.

iii. Integrity: To correctness of data, integrity of data is a major challenge in cloud and the field of security to secure or control data on cloud and have major lay on the service provider [3].

1.3 Solution to Data security challenges

Encryption is recommended as a enhanced solution to secure information. Before storing data in cloud server it is better to encrypt data. Applying encryption on data to avoid access of data from other users .

(i) Encryption schemes

Encryption schemes are of two types that is symmetric and asymmetric encryption. In symmetric algorithm encryption as well as decryption both can be performed with the single key and types of symmetric encryption are AES (advanced encryption standard) that can use different length say 128, 192, 256 bits with a private key of same length and DES encrypts the data in a block of 64 bits and key length is 56 bits. Asymmetric encryption-the encryption key is public, as the decryption key remains private. The types of asymmetric algorithms are RSA, Dieffie- Hellman (Elliptic curve cryptography). Symmetric encryption system has faster than asymmetric and advantages over asymmetric crypto system.

(ii) Integrity Check using secure Hash Function Algorithm

Every time the client needs the way to see integrity of the information, they recover the document as of cloud and calculate hash standard of the document for a second time and compare it with the pre-computed hash values kept at local hash source.

2. LITERATURE SURVEY

Bhaskar Prasad Rimal *et.al.* [1] delivered a classification of cloud computing and expand the current and new cloud systems. The objective of this paper was to create a disciplined procedure of scattered resources with least expenditure in command to acquire great throughput with comfort in cloud computing. The cloud services involved like (Saas) software as a service, (Paas) platform as a service, (Iaas) infrastructure as a structure and hardware as a service.

Prince Jain [2] firstly discussed various models of cloud computing, security issues and research challenges in cloud computing. This paper presented the data security is a major issue for Cloud Computing. There were several other security challenges included security aspects of network and virtualization. .

Rabi Prasad Padhy [3] discussed the overview of cloud computing environment and cloud services. The use of cloud computing in industries, education, banking all sectors were moving towards cloud due to its services and the resources based on bandwidth consumed, space occupied and it described about the security issues and research challenges and purposed was to store data or to maintain data in cloud in the data center's like Microsoft, Google etc.

Prashant Rewagad and Yogita Pawar [4] proposed a work on encryption algorithms and used digital signature scheme with Dieffie Hellman algorithm and (AES) Advanced encryption standard algorithm to protect data and to authenticate data that was stored in cloud. This paper solved the security issues like authentication, confidentiality and data integrity and apply three way mechanism to secure data or to verify data.

Rajkumar Buyya [5] discussed the various opportunities and challenges of cloud computing. This paper show cloud computing deployment model and classified the model into three categories: Public cloud, Private cloud, Hybrid cloud and also described the evolution of cloud and concept of security in cloud .

Zhifeng Xiao *et.al.* [6] discussed the cloud computing environment and advanced research of cloud computing. It included some attributes of security in cloud environment such as integrity, confidentiality, availability, accountability and purpose was to provide security.

Yu-Sung Wu *et.al.* [7] discussed the concept of data storage in cloud system and purpose of this paper was to provide integrity to the cloud storage area and securely store or manage the data. It included some important security services like key generation, Encryption and Decryption in Cloud Computing system.

Cheng-Chi Lee *et.al.* [8] proposed a work on encryption scheme is AEB(attribute based encryption) scheme mainly included two schemes – Key policy based encryption, and cipher text-policy based encryption .The attributes plays important role in AEB and the access structure of key policy was based on user's private key and the access structure of cipher policy is based on cipher text.

Manjesh.K.N and and R K Karunavathi [9] discussed the cryptography technique advanced encryption algorithm and purpose was to secure data or to secure communication among data. AES advantage in software or hardware and advanced encryption standard algorithm is high speed algorithm and key length of AES encryption is 128 bit, 192 bit and 256 bit. This paper used pipelining stages to increase the area and throughput.

Monjur Ahmed and Mohammad Ashraf Hossain [10] discussed the security challenges of cloud computing and approaches used in cloud computing was rather dynamic and vast. This paper show data location was a crucial aspect in cloud computing security and cloud users' personal data security was thus a crucial concern in a cloud computing environment.

Ashwini Bangar and Swapnil Shinde [11] described the cloud computing characteristics and to secure cloud by applying different encryption techniques. This paper also discussed the hybrid systems and to implement the cryptographic algorithms such as Symmetric algorithms like AES, DES and Asymmetric algorithms like RSA and Dieffie Hellman, digital signature. And also used various attacks so that intruder not able to attack the cloud data. The author compared the various encryption algorithms which was scalable or not.

Okeke Stephen[12] discussed to secure data using encryption techniques so that attackers not to theft the data .The data security is major concern when user send the files into cloud and this paper described encryption techniques that plays important role to secure data and to protect or correct integrity of data. The encryption techniques used to encrypt the user data in cloud and algorithms used like symmetric encryption purposed was to store large data in cloud storage.

Mahesh S.Giri *et.al.* [13] described the techniques of data integrity - Proof of retrievability (POR) and POR scheme based on selection of random bits in data blocks that were suited for client and in this paper POR was not used for prevention mechanism but only used for static data.

Vinay Kumar and Sandeep Sharma [14] discussed the methods of fault tolerance and models to be used in cloud computing and important concerned was to detect failure and fault and delay fault was not accepted in cloud computing .The techniques used robust fault tolerance, virtualization technique and this paper described fault tolerance methods, algorithms and also show the fault tolerance schemes.

Nivedita Shimbre and Priya Deshpande [15] described the cloud computing model, security issues and important concerned was to used the SHA-1 techniques and hash coding techniques in which every file block contains the hash code so using hash code only authorized users could access the data. This paper also show the AES (advanced encryption standard) algorithm to securely store the data on cloud and using cloud storage system it analyzed the data security problems.

Vishal R. Pancholi and Bhadresh P. Patel [16] discussed about enhancing the concept of security in cloud or to improve data in cloud server. This paper used AES algorithm that was to be based on permutation and substitution. AES uses 128,192, 256 bit key that is highly secured. Also purpose was to improve the performance.

Harish Singh [17] gave the overview of security and show the network security was biggest concern or more challenging. To perform network security testing was important aspect of this paper and purposed was to safe more data or secure that data so attacker not able to theft the data and also checked the integrity of data.

B. M. Kore *et.al.* [18] discussed the concept cryptosystem that was used for cloud data sharing. This paper show the cryptographic techniques that was used to efficiently store the secure data in cloud storage and used those schemes that was more flexible. The purpose of this paper was to compress the keys, using cryptosystem concept.

Kadwe Yugandhara *et.al.* [19] discussed the concept of data storage or cloud storage. The cloud storage use the service- Iaas (infrastructure as a service) and it shows the security .The best method used to solve the issues of cloud was encryption techniques and this paper discussed the algorithms AES and HMAC (message authentication code) and purposed of this paper was to secure more data in cloud system and store encrypted data into the storage server so its easy for user and data was not to be lost.

Devi Thiyagarajan and R. Ganesan [20] proposed the cryptographic model and model based on multiple keyword concept and purposed of this model was to encrypt or store secured data in cloud. The techniques used to generate random bits by using Bloom filter technique. This paper used the schemes elliptic curve cryptography and bloom filter based and show indexing faster due to its scalability increases.

Mohaned Zkaria Salem *et.al*. [21] discussed the mechanism of privacy preserving public auditing and used the independent entity TPA (third party auditor) and purpose was to modify data or to improve integrity and audit the data. This paper used encryption techniques AES and SHA to compare and evaluate performance or to maintain privacy and secure data.

Renuka C. Deshpande and S. S. Ponde [22] discussed the deduplication concept used in cloud and reduced the over space in network or detected the duplicate data.. This paper described schemes AES and SHA scheme and used deduplication concept or to gave access rights to server . The main purposed was to detect duplicate data and trim down the bandwidth.

CONCLUSION

This survey concluded the concept of data security in cloud using encryption techniques- Advanced encryption standard algorithm(AES) and to check data integrity, data deduplication using secure hash function algorithms (SHA). Nowadays, Security is a major concern to secure more data in cloud or integrate data and to store secure data in cloud so we conclude some challenges in cloud like accessibility, data integrity etc. and also give the solution of data security challenges. The purpose to use the encryption techniques is to safe more data so that attacker not able to attack data .

3. REFERENCES

[1] Bhaskar Prasad Rimal; Eunmi Choi; Ian Lumb, (2009) “A taxonomy and Survey of Cloud Scheming Systems”, IEEE Fifth International Joint Conference on INC, IMS, and IDC,vol.10, No.2, pp. 44-51.

[2] Prince Jain, 2010, “Security Issues and their Solution in Cloud Computing”, International Journal of Computing & Business Research, Vol.3, No.1,pp. 1-7.

[3] Rabi Prasad Padhy , Manas Ranjan Patra and Suresh Chandra Satapathy,(2011), “ Cloud Computing: Security Issues and Research Challenges”, International Journal of Computer Science and Information Technology & Security ,Vol.1,No.2, pp. 136-146.

[4] Prashant Rewagad and Yogita Pawar, (2013) “Use of Digital Signature with Dieffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, International Conference on Communication Systems and Network Technologies , Vol.33, No.1, pp.437-439 .

[5] Rajkumar Buyya, (2013), “Introduction to the IEEE Transactions on Cloud Computing”, IEEE Transactions On Cloud Computing, Vol. 1,No.1,pp.3-5.

[6] Zhifeng Xiao and Yang Xiao, (2013) “Security and Privacy in Cloud Computing”, IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, pp.843- 859 .

[7] Yu-Sung Wu; Bingrui Foo , (2013) “Amazon Web Services: Overview of Security Processes”, International Journal of Network Security, Vo.12, No.1, pp.822-866 .

[8] Cheng-Chi Lee; Pei-Shan Chung; Min-Shiang Hwang, (2013) “A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments”, International Journal of Network Security, Vol.15, No.4, pp.231-240.

[9] Manjesh. K.N and R K Karunavathi, (2013) “Secured High throughput implementation of AES Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 5, pp.1193-1198 .

[10] Monjur Ahmed and Mohammad Ashraf Hossain, (2014)“Cloud Computing and security issues in the cloud”, International Journal of Network Security & Its Applications, Vol.6, No.1, pp.25-36 .

[11] Ashwini Bangar and Swapnil Shinde, (2014) “Study and Comparison of cryptographic Methods For Cloud Security” International Journal of Computer Science Engineering and Information Technology Research, Vol . 4, No. 2, pp.205-213 .

[12] Okeke Stephen, (2014) “The Study of the Application of Data Encryption Techniques in Cloud Storage to Ensure Stored Data Integrity and Availability” International Journal of Scientific and Research Publications, Vol. 4, No. 10, pp.1-7 .

[13] Mahesh S.Giri; Bhupesh Gaur; Deepak Tomar, (2015) “ A Survey on Data Integrity Techniques in Cloud Computing”, International Journal of Computer Applications, Vol. 122 ,No.2, pp.27-32 .

[14] Vinay Kumar; Dr. Sandeep Sharma, (2015) " A Comparative Review on Fault Tolerance methods and models in Cloud Computing", International Research Journal of Engineering and Technology,Vol. 02 No.09 , pp.18-21.
[15] Nivedita Shimbre and Prof. Priya Deshpande (2015), "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", An International Conference on Computing Communication Control and Automation, Vol. 12, No. 6 , pp. 60-67.
[16] Vishal R. Pancholi and Bhadresh P.Patel, (2016) " Enhancement of cloud computing security with secure data storage using AES", International Journal for Innovative Research in Science & Technology, Volume 2 No. 09 , pp.432-441 .
[17] Harish Singh,(2016) " Network Security, A Challenge", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, No. 3, pp.57-61 .
[18] B. M. Kore ; Archana Jadhav, Prof. V. V. Pottigar, (2016) "A Literature Survey on Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem,"International Journal of Computer Science and Information Technologies, Vol. 7,No.3 , pp.1511-1513.
[19] Kadwe Yugandhara; Jadhav Ashwini; Pagar Pooja,;Patil Suchita; Prof.J.S.Pawar, (2016) " Secure Data Storage and Forwarding in Cloud Using AES and HMAC", International Research Journal of Engineering and Technology, Vol. 03, No.02 , pp.75-79
[20] Devi Thiyagarajan; R. Ganesan, (2017) "Cryptographically Imposed Model for Efficient Multiple Keyword-based Search over Encrypted Data in Cloud by Secure Index Using Bloom Filter and False Random Bit Generator ", International Journal of Network Security, Vol.19, No.3, pp.413-420.
[21] Mohaned Zkaria Salem; Sahar F. Sabbeh and Tarek EL-Shishtawy, (2017) " An Efficient Privacy Preserving Public Auditing Mechanism for Secure Cloud Storage" , International Journal of Applied Engineering Research ,Vol. 12, No.6 , pp. 1093-1101.
[22] Renuka C. Deshpande; S. S. Ponde ,(2017) " Deduplication Using SHA-1 and IBE with Modified AES", International Journal of Science and Research (IJSR) , Vol. 6 No. 2, pp. 1966-1969.