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 3, March 2016

A Review on Data Storage in Cloud Computing

Harpreet Kaur[1], Sheenam Malhotra[2]

M. Tech Student, Dept. of C.S, SGGS, World University, Fatehgarh Sahib, Punjab, India[1]

Asst. Professor, Dept. of C.S, SGGS, World University, Fatehgarh Sahib, Punjab, India[2]

ABSTRACT: Today, a large number of organizations are moving towards cloud for storing a large amount of data. Security is the most important concern in cloud. There are many security issues of cloud computing which are related to trust, data confidentiality, authentication, access control etc. These issues breach the CIA triad of cloud. The impact of data security and the extent of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling. Many encryption techniques are available in cloud computing but some are efficient in terms of time and some are attack resistant. But the need is to propose a technique that is the combination of both.

KEYWORDS: Cloud computing, data storage, encryption, AES, Randomness, attack resistant

I. INTRODUCTION

1.1Cloud Computing**:** In recent years, cloud computing becomes a very important part of the computing world. Usage and popularity of cloud computing is increasing day by day. Nowadays users are totally dependent on its application for their work. Basically, it is technology which offers various services over the web. Several services are provided by cloud computing and those customers who are utilizing their services are charged accordingly. Generally, three types of service models which are provided by cloud are platform as service, software as service, and infrastructure as service. Hence, it can be said that cloud computing provided services according to users demand.NIST definition of Cloud Computing the National Institute of Standards and Technology (NIST) provided the formal definition of Cloud Computing ”Cloud Computing is a model for enabling pervasive, convenient on demand network access is a shared pool of configurable computing resources, applications, services etc. that can be quickly delivered and release with least management effort. “Cloud computing consist of 5 characteristics, three service models and four deployment models.

1.2 Threats in Cloud Computing

- Account or Service Hijacking:Account or service hijacking is a process through which end user account for cloud computing service is hijacked by hacker. Attacker gain access to credentials, privileges, personal information etc. They can eavesdrop onuser’s activities and transactions and can manipulate user’s sensitive data. Attacker may also have access on types of resources or services customer is using and can use the same resources services for his own interest.
- Denial of Service Attack:Denial of service attack (DOS) also known as Distributed Denial of Service Attack (DDOS) through this attack attacker aims to make resources, services, machine or network unavailable for its legitimate users. Making resources unavailable includes temporary or permanent interrupt or suspension of services for the end user.
- Data Scavenging Attack:Data scavenging attack attacker searches, collects bits and bits of data may or may not from data residue from a system to gain knowledge of sensitive information. These are further of two types:-
    i. Keyboard Attack:In this data scavenging is done by attacker through resources of systems e.g. keyboard. Any key paused is noted and results can be used to search and gain access to important data.
    ii. Laboratory Attack**:**In this type of data scavenging attack attacker searches and collects information from electronics equipment attached to a system.

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 3, March 2016

- Data Leakage**:**Data leakage is defined as the illegitimate transmission of data from a distributed system; enterprise to external location, sensitive information is leaked to provide gain to others. All types of data that is data in motion, data in use or data at rest can be attacked by the attacker.
- Virtual Machine Escapeand Hopping Attack**:** Virtual machine escape and hopping attack is the process of interaction with host operating system by breaking virtual machine. A virtual machine is isolated guest operating system installation within a normal host operating system.InHopping attack attacker searches for virtual machine working on same hardware. For accessing information from one virtual machine the attacker use other virtual machine to enter to the virtual machine of interested information.
- Customer Data Manipulation**:**In a Cloud Computing system customer register themselves for accessing resources, applications. Customer stores their data in cloud storage and accesses them from anywhere anytime. All these information from personal information, login information, or the data which is stored by customer on cloud storage is of keen interest to attacker. If attacker gain access to any of these data and manipulate it the attack is known as Customer Data Manipulation.
- Sniffing and Spoofing**:**Sniffing attack means an attacker with the help of an application or device can read, monitor and capture data interaction between Cloud service Provider and end user. Spoofing means pretending to be someone else's IP address. In this attack attacker sends packets and pretend its IP address to be of legitimate user of the network. After gaining network access attacker can modify, reroute or erase the data.
- Man-in-the-Middle Attack:Man-in-the-middle attack literally means attacker is in between Cloud Service Provider (CSPs) and end user who is monitoring, capturing and controlling all end users communication silently. The captured information may be later used by attacker for legitimate and personal purposes or to gain interest.
- Simple Power AnalysisAttack (SPA):In cryptography attacker uses power analysis attack which is a form of side channel attack. By this attack attacker studies cryptographic hardware device and its power consumption. Attacker searches for cryptographic keys and other secret data from cryptographic hardware device.
- Differential Power Analysis Attack (DPA):Differential Power Analysis Attack is a type of power analysis attack which is a side channel attack. It is more advanced form of attack than Simple Power analysis attack (SPA). In this attack attacker computes intermediate values, analyze data from different cryptographic operation.
- Higher Order Differential Power Analysis Attack (HODPA):In Higher Order differential Power Analysis attack, attacker monitor, capture and analyze related information between different cryptographic operations.

II. **RELATED WORK**

Cao et.al (2014) [1]presented research work of multi-keyword ranked search over encrypted data (MRSE) in cloud computing had defined it and solved the issue of privacy preserving. For enhancing privacy protection of the user and the data, data to be sent to the cloud server must be encrypted; search request allows multiple keywords as there are a large number of data users and data files in cloud server. In this paper, architecture of search over encrypted data is proposed. In this architecture three roles or entities are defined: cloud server, data owner and data user. Data owner is the owner of the data which encrypts and uploads data on cloud server. Cloud server is cloud storage where encrypted data resides; search and ranking of results for end users take place. End users are the authorized users who can access data from cloud server. Three goals were achieved by this architecture: multi-keyword ranked search, preservation of data privacy and efficiency.

Prajapati and Rathod (2015) [2] in this research paper had developed a data security technique known as Bi-directional DNA encryption algorithm (BDEA) to overcome data security issues in cloud computing environment. Bi-directional DNA encryption algorithm can encrypt and decrypt Unicode characters along with ASCII characters. The proposed algorithm provides two levels of security. At first a table is maintained of DNA digital coding A, G, T, C and its corresponding binary value, then the encryption and decryption of the DNA coding. Encryption starts with plaintext Unicode message. Unicode message is converted to ASCII code, which is again converted to hexadecimal code. Hexadecimal code is then converted to binary code using binary convertor. Binary code is divided into different parts for which corresponding DNA digital loading is doneAs Bi-directional DNA encryption algorithm (BDEA) algorithm

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 3, March 2016

is used for Unicode character set hence wider community of cloud services users can be easily reached up to. In future, possible attack on Bi-directional DNA encryption algorithm (BDEA) is studied and analyzed.

Li et.al (2012) [3] proposed a framework which addresses issues and challenges regarding multiple Personal Health Records (PHR) owners and users. Key management complexity is greatly reduced when compared with other related works; this proposed method offers enhanced privacy with sealable and secure sharing of records. The proposed scheme enables break glass access under emergency situations, supports user revocation and attributes revocation. Proposed system divides the user into two types of domains- public domain and personal domain. Public domain includes health care domain and insurance domain. Personal domain defines the personal health records key have all access to data can grant access privileges to public domain. In the proposed framework system attribute based encryption is used to encrypt patients personal health record, this allows personal health record to be accessed by personal health record owners, public domain users having different professions.

Mishra et.al (2015) [4] studied various security issues related to cloud computing environment and compared different cryptographic algorithms on various factors. He presented introduction to cloud computing and its model. He studied and monitored cloud model into five essential characteristics, four deployment models and three service models. Security issues of cloud computing system is taken into consideration and studied such as availability, data integrity, storage, authentication, access control, privacy confidentially etc. Different threats like hijacking, sniffing, data leakage, scavenging, spoofing, data manipulation etc. in his research paper cryptology basics were also discussed. Cryptography is used for encryption and decryption of data that resides in cloud. There are two types of cryptography: - (1) Symmetric Key Cryptography (2) Asymmetric Key Cryptography. RSA is best among Asymmetric Algorithm. In cloud computing environment RSA is used for encryption key generation for Symmetric Key Cryptography.

MT Nurpeti et.al (2014) [5] presented in this paper a reliable, secure and fast security technique for information containing digital images. To improve security from attacks like brute force, plain text attack etc. he developed a chaos based encryption algorithm. For encrypting digital images logistic map is used as Chaos function which produces key stream for encryption and thereby producing encrypted image. For decryption again logistic map is used for key stream for converting encrypted image to original image. From the performance analysis of this Chaos based encryption algorithm shows that (1) Time of encryption and decryption of color images is longer than grayscale images (2) Value distribution of pixels is uniform in encrypted image and the key stream generated were fully random hence this encryption is difficult to crack by attacks like plain text attack. (3) Key space of 1030 and key availability of 10-16 is there in encryption algorithm. Hence this proposed Chaos based encryption algorithm provides much high level of security.

Saparudinet.al (2014) [6] proposed a new encryption algorithm by using Henon Chaotic Map for encryption of images. Images were partially or selective encrypted by the proposed algorithm. The proposed algorithm perform its operation in three steps (1) Fact Detection (2) Encryption (3) Decryption. Henon Map is 2- dimensional chaotic map' Chaotic based image encryption techniques are more secured, efficient and premising. These techniques are very fast in encryption and decryption process. The proposed techniques use improved Henon Map by replacing Henon Map's two equations with one single equation. Improved Henon Map performs encryption and decryption by using nine function along X-axis and tangent function along Y-axis. Encrypted data is obtained by doing bit XOR operation of original data and the key. To decrypt encrypted data and to get original data back the encrypted data and the key undergoes bit XOR operation. Security analysis of this technique is done using Histogram analysis, sensitivity, entropy and correlation co-efficient. This brings out the conclusion that proposed technique can resist all possible attacks including brute force attack. This technique is highly effective and efficient.

Kumar et.al (2014) [7] presented a paper to provide compendious introduction of cryptography. Cryptography is a technique to encrypting and decrypting data and images to make it unable to read for illegitimate users. Cryptography of images is equally important as of simple text data. Cryptography technique is used in developing image encryption algorithm. This research work presents the survey and analysis of various image encryption techniques. These image encryption techniques are compared on the factors such as key size, key sensitivity, entropy (both original and cipher), histogram analysis, Correlation (both original and cipher) and their NPCR percentage by the work. It was concluded

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 3, March 2016

that chaotic algorithm provides utmost uncertainty and provides improbable security. It was also concluded that to achieve high level of security not only scrambling but substitution and snuffing is required. Images require more space hence require more bandwidth to be transferred over the network. Therefore image encryption algorithm needs compression of data continuous effective and efficient enhancement.

Sachdeva and Mahajan (2013) [8] in their research work focused on cryptography as a basis of security of data when the data is transmitted over the network its security is the major issue. In this paper cryptography is chosen technique to protect the data. Cryptography consists of encryption and decryption. When sender sends data to receiver over the network it must be unreadable for any other person. For making it unreadable encryption is done using a cryptographic encryption algorithm. Similarly if receiver wants to read data sent by the senders it must be decrypted using cryptographic decryption algorithm. Decryption is done to make encrypted form readable for legitimate users. In this work AES, DES, RSA cryptographic algorithm are implemented analyzed and compared. On the basis of analysis their performance was compared on the basis certain factors. It is concluded that RSA algorithm had taken much longer time as compared to AES and Des. AES used least encryption time for all of the packet size. Also the decryption of AES algorithm was better than other algorithms.

Singh and Supriya (2013) [9] surveyed various encryption algorithms in their research work. Encryption algorithm converts plain message to cipher text. Only the legitimate authorized user can read the message. Large number of information is stored on computers and transferred over network. Security of this data is an important issue against different attacks. Cryptography has also become complex for making information more secure. Different encryption algorithms are used for security purposes. All the algorithms have same positive factors and negative factors. The encryption algorithms RSA, AES, DES, 3DES are compared based on several such factors like key length, Rounds, Cipher Text, Speed and Security. Amongst the encryption algorithms RSA has smallest speed of encryption and decryption and AES has the highest speed. Results showed that RSA provides least security and AES provides highest excellent security. In the paper it was concluded that, AES is the best cryptographic encryption algorithm in terms of security, performance, flexibility, and throughput and avalanche effect.

Hovath [10] in his research work, attribute based encryption (ABE) more appropriate for data access control of cloud database by the clients. This proposed method enabled operational, effective and efficient user revocation which is essential factor of cloud computing framework execution. The experimental result of the proposed was the extension of the decentralized CP-ABE scheme, with addition of user based revocation. Proposed revocation system was made practical effective by decreasing computational overhead of revocation event occurs from the service provider of cloud. In future, comparison between different revocations schemes are needed for attribute based encryption.

III. CONCLUSION

Cloud Computing is technology which offers various services over the web. Several services are provided by cloud computing and those customers who are utilizing their services are charged accordingly. In cloud computing, Security is utmost significant issue. There are other safety problems of cloud computing which are related to trust, data confidentiality, authentication, access control etc. The effect of data security and the extent of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling , etc.

REFERENCES

1. Cao, Ning, et al. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." *Parallel and Distributed Systems, IEEE Transactions on*25.1,pp 222-233, 2014.
2. Prajapati, Ashish, and AmitRathod. "Enhancing Security in Cloud Computing Using Bi-directional DNA Encryption Algorithm." *Intelligent Computing, Communication and Devices*.Springer India,pp-349-356, 2015.
3. Li, Ming, et al. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." *Parallel and Distributed Systems, IEEE Transactions on* pp-131-143, 2013.
4. Mishra, Neha. "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues." *RIET-IJSET: International Journal of Science, Engineering and Technology*,pp-59-6, 2015.

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 3, March 2016

5. . Sordid, M. T., and Eva Nurpeti. "Performance of Chaos-Based Encryption Algorithm for Digital Image." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 12.3,pp-675-682, 2013.
6. Saparudin, Saparudin, GhazaliSulong, and Muhammed Ahmed Saleh. "Multi Facial Blurring using Improved Henon Map." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 12.4 ,2014.
7. . Kumar, Mohit, AkshatAggarwal, and AnkitGarg. "A Review on Various Digital Image Encryption Techniques and Security Criteria." *International Journal of Computer Applications* 96.1,19-26, 2014.
8. Mahajan, Prerna, and AbhishekSachdeva. "A study of Encryption Algorithms AES, DES and RSA for Security." *Global Journal of Computer Science and Technology* 13.15 ,2013.
9. . Singh, Gurpreet, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." *IJCA* 67.19,pp-33-38, 2013.
10. Horváth, Máté. "Attribute-Based Encryption Optimized for Cloud Computing."*SOFSEM 2015: Theory and Practice of Computer Science*. pringer Berlin Heidelberg,pp-566-57, 2015.