International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A Comparative Review on Data Security Challenges in Cloud Computing

Manpreet Kaur[1], Kiranbir Kaur[2]

[1] *M.Tech Scholar, Computer Engineering and Technology Department, Guru Nanak Dev University, Punjab, India*
[2] *Asst Prof, Computer Engineering and Technology Department, Guru Nanak Dev University, Punjab, India*

Abstract - ***Cloud computing is a model which provides on-demand delivery of Information Technology (IT) related capabilities or resources through the Internet to the outside world. Despite the advantages of cloud computing, the security of the data and resources is still doubtful which affect the cloud adoption. The raising amount of personal and confidential data brings up attention on storing the data securely. Data can be composed of financial transactions, vital documents, and multimedia contents. Implementation of cloud computing services may minimize local storage trust in addition decrease operational and maintenance costs. However, the users still have major privacy and security concerns about their data stored on remote servers due to potential unauthorized access among the service providers. So, these concerns bring focus on security issues related to cloud computing which is the reason why most of the industries still not adopting cloud server for the storage of their critical data. Cloud computing does not provide transparency to users to view where their data is being stored and users have to trust the service provider for handling and maintaining their data. Also, it does not provide users to access the audit logs because many users are sharing the same cloud server so audit activity of one tenant might constitute a transparency for another tenant. In this paper, the extreme focus is given to the security challenges related with cloud's service models, deployment models, and issues related to networking capabilities are discussed and studied. In addition, the existing symmetric and asymmetric encryption algorithms utilized to render security in cloud computing environment are reviewed. Furthermore, the comparative analysis of different encryption algorithms based upon few parameters is also been performed.***

Key Words: *Cloud Computing, Cloud Security Challenges, Encryption Algorithms.*

1. INTRODUCTION

Cloud computing is a model that enables the development, deployment and delivery of products and services to the customers with a pay-as-you-go model. It is a service model that involves the idea of storing and accessing the resources over the Internet rather than storing them on-premise. Basically, cloud computing has motivated academia, industry, businesses to take over this technology to host their applications on the cloud so as to cut-off the cost of buying the on-premise local server. As per Gartner survey [14], the cloud market is anticipated to rise from $76.9B in 2010 to $210B in 2016. These revenues connote that it is a promising platform.

Types of Service models provided by cloud are described below:

Software as a service (SaaS): SaaS is a software delivery model that provides access to software and its functions operating on a remote cloud infrastructure offered by cloud providers. Salesforce.com offering in the customer relationship management (CRM) space was the innovator to provide software as a service. Other examples include online word processing and spreadsheet tools, Gmail, WhatsApp, and SAP.

Platform as a service (PaaS): PaaS provides the framework for deploying and delivering of applications and services. It allows developers to develop new applications without any pressure of buying expensive tools and managing the local servers. Examples include Hadoop, Microsoft Azure, Force.com, and Google App engine.

Infrastructure as service (IaaS): IaaS provides the infrastructure such as network, memory, storage, processor to the users on demand. Examples include Amazon EC2, Windows Live Skydrive, and Rackspace Cloud.

Deployment models identified for cloud architecture are described below:

Public Cloud – The pubic cloud refers to sharing of computing infrastructure by many customers and they have no control and visibility over the computing resources where infrastructure is hosted.

Private Cloud – The private cloud does not share infrastructure with other organizations and dedicate to the particular organization. In terms of security and cost, a private cloud exceeds public clouds.

Hybrid cloud – The hybrid cloud makes usage of both of the clouds discussed above. Organizations may host less critical data on the public cloud and confidential data on the private cloud.

Community Cloud - The community cloud is used where several organizations share the similar infrastructures. It may exist on premise or off premise.

Now the question arises, if cloud computing is so powerful, why isn't everyone adopting it?

- In the cloud, the clients don't have knowledge about what's happening inside.
- In addition to this, even if the cloud provider is honest, it can have eavesdropper who can fiddle with the VMs and defiles confidentiality and integrity.
- Clouds are still susceptible to data confidentiality, integrity, availability, privacy issues plus some internal and external attacks.

This paper primarily aims to give an insight to cloud consumers and providers about various security challenges and how they can tackle these challenges through encryption algorithms. The comparative analysis of various encryption algorithms is also presented. This paper is arranged as follows. Section II explores the security challenges in cloud computing. Section III introduces related work for further reading. In section IV, we explore the comparative analysis of existing encryption algorithms. Finally section V, concludes this paper.

2. SECURITY CHALLENGES IN CLOUD COMPUTING

Security is the important aspect for many organizations for cloud adoption. Confidentiality, authentication, integrity, non-repudiation and availability for client's systems are the general principles of security. Access control is another important factor for security. There are lots of security threats to cloud computing. A single flaw in one client application could allow a malicious hacker to acquire access to more than one client's data. This problem is known as data breaches. The data loss is another issue that happens when the unauthorized user may delete or alter the entire records in the cloud if there is the vulnerability in cloud provider side. Insecure APIs and weak interfaces are another common security challenges in cloud computing. When confidential data is stored in it, the extreme focus should be given to the security of the cloud. Figure 1 shows the hierarchy of various security challenges in cloud computing.
Generally, three types of deployment model are further classified as Public, Private and Hybrid and the security issues related to these models have been discussed. In the same way, the service model is categorized further as IaaS, PaaS, and SaaS stating its security issues in common. At last, the network related issues are discussed.

2.1 Security challenges in deployment models

To raise the facility of access in the organizations assorted users and departments across the organization allow sharing of assorted resources but alas lead to data breach problem. Cloning leads to the problem of data leakage concealing the machine's authenticity. Basically, the cloning deals with duplicating and replicating the data. Resource Pooling refers to the unauthorized access because of sharing through the same network. Furthermore, in a shared multi-tenant environment when any user consumes some unequal amount of resources then some resource contention issues might occur. Authentication and Identity Management is one of the another big issue associated with deployment models in cloud-based systems.

2.2 Security challenges in service models

Typically the web browser is used for delivering applications in SaaS to cloud consumer. Since intruders are using the web to do malicious activities. So, there is a threat to data because the issues like data leakage, malicious attacks and in the case of disaster backup and storage can lead to unauthorized access of sensitive data. PaaS inherits security issues related to third-party web services. In the case of PaaS, the developers use the platform provided by cloud providers for deployment of the secure applications that can be hosted on the cloud and these PaaS applications should be upgraded frequently. This in turns affects security. Privacy and security can also be threatened because data may be stored in different locations with different legal authorities. So, the developer must be aware of legal issues related to data to ensure that data is stored in apropos locations. Service Hijacking is also considered to be as one of the topmost threat in which an unauthorized user gains an illegal access on certain authorized service. Generally in IaaS, computer hardware is provided to the consumer which can be threatened by physical attacks and there can be a lack of data security on replaced or repaired storage devices.

2.3 Network related security challenges

Cloud computing principally depends on servers, the internet and remote computers in managing, storing and

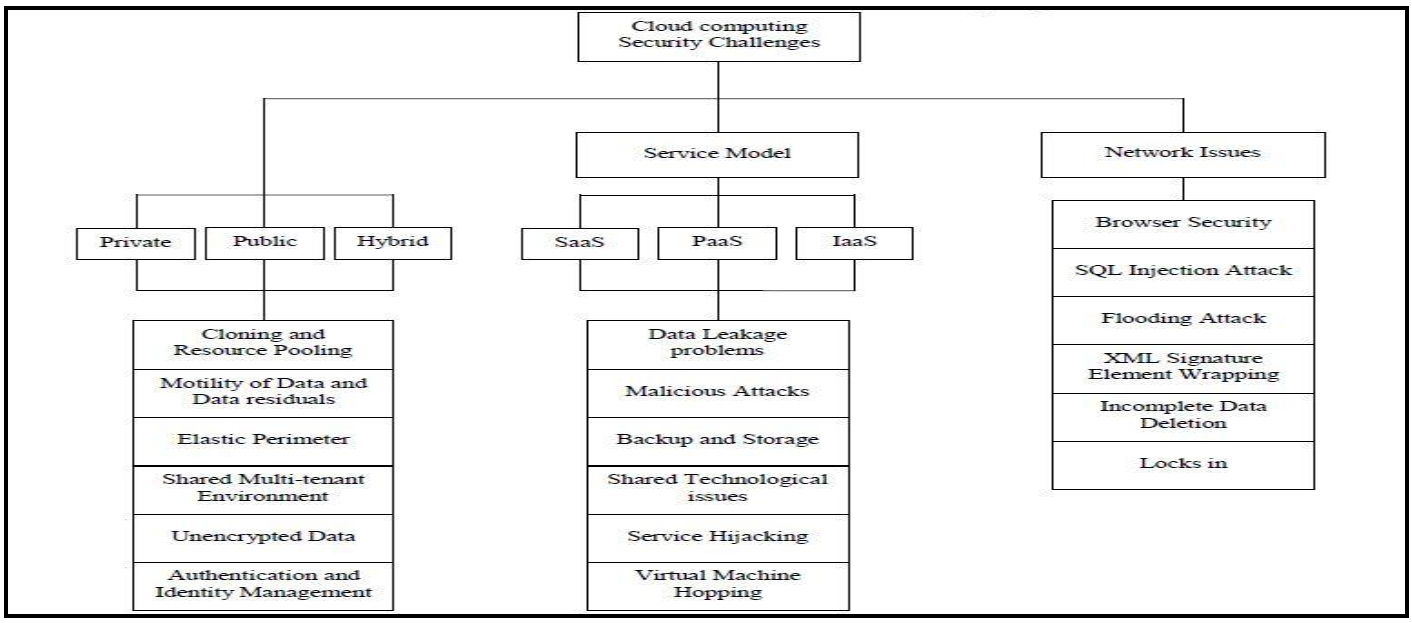

Fig -1: Classification of Security Challenges [12]

maintaining data. Therefore, the security issues associated with the network are of the prime concern. It provides on-Demand access to the high-speed data transmission rate, application, software, and resources to the users. But apart from this, the network infrastructure also faces various attacks and security challenges which are listed in the above diagram.

3. RELATED WORKS

L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari (2015) [1], proposed an efficient cloud storage model that provides confidentiality and integrity through data classification and minimizes the complexity and processing time needed to encrypt the data by applying TLS, AES and SHA security mechanism based on the type of classified data. They tested the proposed model with assorted encryption algorithms, and their simulation results showed the efficiency and reliability. This paper is established on the idea of manual classification of data and not the automatic classification and other encryption algorithms such as RSA, Elliptic curve cryptography, and asymmetric public key can be used to provide the higher level of security and confidentiality.

N. Sengupta and R. Chinnasamy (2015) [2], designed an encryption algorithm Hybrid DESCAST to provide the security to the massive amount of data sent through the internet. Through proposed algorithm, they tackled the limitations of both DES and CAST Block Cipher Algorithm and analyzed that the computation time and complexity for encryption and decryption is higher than the respective DES and CAST algorithm. In addition to this, they concluded that combining 128-bit key and 64-bit key cipher algorithms, the brute-force attack and attacks via birthday problems were averted and the algorithm is more robust.

S.K. Sood (2013) [9], proposed a security model that keeps the most confidential and critical data on the private cloud and rest of it on the public cloud and for checking the integrity of the data at the public cloud this model uses the hash codes. He proposed cloud security model that associates a role to each user and stores the role of the user in the database for user authorization process and operations can be performed by the user with respect to their roles. Also, for security purpose, this model uses dual verification scheme for key authentication on one layer and user authentication by using username and password on another layer. A cryptographic process is proposed for keeping data secure on the cloud. He analyzed the model against various types of attacks. This model is compared with various existing cloud security frameworks and the simulation results showed that this technique is much more robust, efficient and faster than other existing models. Furthermore, this model is efficient in terms of cost because it stores highly sensitive data on the private cloud and less critical data on the public cloud, where storage cost of data is relatively very less.

J.J. Hwang, Taoyuan, Taiwan, Y.C. Hsu and C.H. Wu (2011) [4], has proposed a data security model using encryption and decryption algorithms. The model used such a mechanism that the cloud service provider can perform storage and encryption/decryption tasks. The drawback of this method is that the user or data owner has no control of data.

J. Lai, R. H. Deng, C. Guan and J. Weng (2013) [5], proposed an Attribute-Based Encryption (ABE) and decryption method in the cloud-based system to provide data security. They have been designed such a decryption algorithm which is based on the user-requested attributes of the outsourced encrypted data. The limitation of this method is that it emphasis more computational and storage overhead on cloud service provider for checking the user attributes with the outsourced encrypted data. Although these overheads of the cloud server can be minimized by introducing third party auditor.

F. Moghaddam F, Karimi O and Alrashdan M T (2013) [6], reviewed the comparative analysis of six different symmetric key cryptographic algorithms in a cloud-based environment. They proposed two sorts of cloud servers; that is cloud and data servers. The limitation of this method is that it creates storage and computation overheads of maintaining two separate servers.

W. Liu (2012) [7], discussed the security problems in cloud computing, strategies to combat security problems and demonstrated various cloud perimeters. He analyzed that the service availability and data privacy in the cloud-based systems are of the primal concern in security and through comparative analysis he judged that security problem cannot be tackled through single security method and many conventional and recent technologies and strategies must be needed for protecting the cloud-based systems.

A. Behl and K. Behl (2012) [8], investigated the security challenges based on the four views such as cloud architecture view, delivery model view, characteristics view, and the stakeholder view. They investigated few solutions through which the dynamic cloud model can be secured. They discovered that how the existing issues exist in nowadays cloud model owing to confidentiality and integrity loss, SLA issues, elasticity, multi-tenancy, insecure management and cloud federation implications.

Ryan K L Ko et al. (2011) [9], presented the model known as Trust Cloud, which addressed the accountability in cloud computing through the use of five abstraction layer architecture. They also discussed issues which were encountered in accomplishing a trusted cloud. They have proposed detective instead of preventive approaches for raising accountability since later complement the former.

J.K. Wang and X. Jia (2012) [10], described several methods to secure user data such as authentication interface, single encryption, and multi-level virtualization. The other main topic of their paper is Authentication intercloud based on CA and PKI model.

G L Prakash, Dr. M. Prateek and Dr. I. Singh (2014) [11], proposed an efficient data encryption and decryption using 256 bit symmetric key with rotation for securing the highly critical remote data in cloud paradigm. They conducted an experiment on the variable size text files repository and it showed that the proposed method is superior to existing methods. Also, they introduced the mechanism for securing the cloud server from unauthorized users. In addition, they have also demonstrated the performance analysis of encryption and decryption algorithms.

4. EXISTING ENCRYPTION ALGORITHMS FOR CLOUD SECURITY

Cryptography is the one of the technique of the modern network security technologies that enables us to send secure data over an insecure channel and to protect valuable data on the internet, extranet, and the intranets. Encryption algorithms play a vital role for providing the secure transmission for sending and retrieving the data over the networks. It converts the letter to create a coded message, traditionally called as the cipher, which is used to convert a readable data called plaintext into scrambled, unreadable message called ciphertext. This conversion process makes the use of key (private key or public key) and authorized user can only decrypt the cipher text back to plain text. Basically, there are two methods for carrying out this process which are Symmetric key and asymmetric key encryption. The former make use of one key and the latter uses both keys for encrypting and decrypting the data.

DES was the primary encoding normal to be counseled by National Institute of Standards and Technology. Several attacks and ways have witnessed weaknesses of DES that created it associate unsafe block cipher. Triple DES systems are more secure and slower than single DES. AES is stronger and faster than triple-DES. Blowfish is a block cipher algorithm which uses the variable length key. Blowfish is superior in performance and processing time. RC5 is a variable length, byte-oriented stream cipher. It is widely used for web SSL/TLS, wireless WEP. RSA is slower than certain other symmetric cryptosystems. It is the secure algorithm whose security depends on the process of factoring massive integers. DSA uses exponentiation in a finite and based on the difficulty of computing discrete logarithms. Diffie-Hellman is secret key exchange method. The algorithm uses a one-way function that is easy to encrypt and hard or difficult to

decrypt. The limitation of this algorithm is the lack of authentication.

5. COMPARATIVE ANALYSIS OF VARIOUS ENCRYPTION ALGORITHMS

Table -1: Comparative Analysis of Algorithms

Algorithm	DES	3 DES	AES	Blowfish	RC5	RSA	DSA	Diffie-Hellman
Developed	IBM in 1975	IBM in 1978	Joan Daeman, Vincet Rijmen in 1998	Bruce Schneir in 1998	Ronald Rivest in 1994	Ron Rivest, Adi Shamir, Leonrd Adleman in 1977	NIST in 1991	Whitfield Diffie & Martin Hellman in 1976
Key Size	56	112	128, 192, 256	32-448	128	1024-4096	-	1024
Block Length	64	64	128	64	64	-	-	-
Rounds	16	48	10, 12, 14	16	12	1	-	-
Security	Proven Adequate	Considered Secure	Considered Secure	Considered Secure	Considered Secure	Considered Secure	-	-
Computational Speed	Fast	Moderate	Fast	Very Fast	Fast	Fast		
Cipher Type	Block	Block	Block	Block	Block	Asymmetric Block	-	-
Algorithm Structure	Balanced Feistel Network	Feistel Network	Substitution Permutation Network	Feistel Network	Feistel Network	-	-	-
Encryption	Medium	Low	High	Very High	High	High	-	-
Decryption Throughput	Medium	Low	High	Very High	-	-	-	-
Power Consumption	Low	High	Low	Very High	Low	High	-	-
Memory Usage	High	Very High	Medium	Very Low	Low	-	-	-
Security against attacks	Brute Force	Brute Force, Chosen Plaintext, Known Plaintext	Brute Force	Dictionary Attack	Brute Force	Brute Force, Timing Attack	-	Logjam Attack
Confidentiality	Low	High	High	Very High	High	High	-	-
Security / Comments	DES is the first encryption standard to be recommended by NIST. Many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher.	Triple DES systems are more secure than single DES. Slower than single DES.	Stronger and faster than 3DES	Blowfish is a variable length key, block cipher. Blowfish is the better than other algorithms in throughput, processing time and power consumption	Variable key size, byte-oriented stream cipher. Widely used (web SSL/TLS, wireless WEP).	RSA is slower than certain other symmetric cryptosystems. Security of RSA relies on the computational difficulty of factoring large integers	Uses exponentiation in a finite. Based on difficulty of computing discrete logarithms.	Widely used, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec). Limitation is lack of authentication.

6. CONCLUSIONS

Today, cloud computing is the technology being talked across industries due to its efficiency, the flexibility of resources, pay-per-use model, dynamic scalability, faster time-to-market, increased collaboration and cost efficiency. Despite its advantages, many organizations are still not adopting it because of security reasons associated with it. This paper analyzes the problem of security

associated with cloud. Encryption is the foremost option for securing the data and this paper highlights comparative analysis of symmetric as well as asymmetric encryption algorithms for providing security in cloud computing systems.

REFERENCES

[1] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas and F. AlDosari. 'A secure cloud computing model based on data classification.' Elsevier, pp 1153-1158, 2015.
[2] N. Sengupta and R. Chinnasamy. 'Contriving hybrid DESCAST algorithm for cloud security.' Elsevier, pp 47-56, 2015.
[3] S.K. Sood. 'Hybrid data security model for cloud.' International Journal of Cloud Applications and Computing, pp 50-59, 2013.
[4] J.J. Hwang, Taoyuan, Taiwan, Y.C. Hsu and C.H. Wu. 'A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service.' International Conference on Information Science and Applications (ICISA), pp 1-7, 2011.
[5] J. Lai, R H Deng, C. Guan and J. Weng. 'Attribute-Based Encryption with Verifiable Outsourced Decryption.' IEEE Trans. Inf. Forens. Security, vol 8, pp 1343-1354, 2013.
[6] F. Moghaddam F, Karimi O and Alrashdan M T. 'A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments.' Proceedings IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, pp 185-189, 2013.
[7] W. Liu. 'Research on cloud computing security problem and strategy.' IEEE, pp 1216-1219, 2012.
[8] A. Behl and K. Behl. 'An analysis of cloud computing security issues.' IEEE World Congress on Information and Communication Technologies, pp 109-114, 2012.
[9] Ryan K L Ko et al.. 'Trustcloud: a framework for accountability and trust in cloud computing.' IEEE World Congress on Services, pp 584-588, 2011.
[10] J.K. Wang and X. Jia. 'Data security and authentication in hybrid cloud computing model.' IEEE Global High Tech Congress on Electronics, pp 117- 120, 2012.
[11] Prakash G L, DR. M. Prateek and Dr. I. Singh, 'Data encryption and decryption algorithms using key rotations for data security in cloud system.' IEEE, 2014.
[12] Ms. Disha H. Parekh and Dr. R. Sridaran. 'An Analysis of Security Challenges in Cloud Computing.' International Journal of Advanced Computer Science and Applications, Vol 4, pp 38-46, 2013.
[13] R. Buyya, J. Broberg and A. Gosscinnski. 'Cloud computing.' Hoboken, N.J.: Wiley; 2011.
[14] L. Columbus, 'Forbes / Tech', Forbes.com, 2013. [Online].Available: http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.

BIOGRAPHIES

Manpreet Kaur pursuing M. Tech in Computer Science & Engineering from Department of Computer Engineering & Technology, Guru Nanak Dev University, Amritsar, Punjab, India. Her research interests include Cloud Computing.

Ms. Kiranbir Kaur is working as a professor in the Department of Computer Engineering & Technology, GNDU, Amritsar, Punjab, India. She has published many research articles in the National/International conferences. Her research interests include Cloud Computing.