International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-1, January 2015

Data Security Models In Cloud Computing: A Review

Prof. Kavita Rathi, Narender

***Abstract*—Cloud computing is a vastly growing information technology and its space continues to evolve at an astounding pace. It provides efficient model for organizations to take services over internet. Its professional services such as computing, software, data storage, hardware and network are growing like no other. Data storage service has been used in engineering, medical, private sectors. Now in many countries government also looks towards cloud to store their data known as g-cloud. In current time if any industry is evaluating technology replacements, upgrades or acquisitions, cloud has to be on their list of considerations. Apart from these cloud services have limitations because of lack in data security due to which in past many time cloud services have been interrupted. Data must be secured in cloud by use of effective encryption algorithms in proper way with the help of data security models. This paper covers data security issues in cloud, data security models and their comparisons.**

Keywords: **Cloud computing, data security, data storage, g-cloud.**

I. INTRODUCTION

Cloud computing is the most rapidly growing technology which allows consumers and business to use applications without installation and access their personal files at any computer with internet access as shown in figure1. Cloud computing is a wireless networks and anyone can easily access the cloud because of its easy access, cost effectiveness and efficient nature people are moving towards it with a very fast rate. National Institute of standard technology define cloud computing as : "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Cloud provides many benefits to the users but with these benefits it has some problems, one of them is security. Due to poor security in cloud many times in past cloud services have been interrupted. In 2009 the major cloud computing vendors faced several accidents. Amazon's Simple Storage Service was interrupted in July 2009.

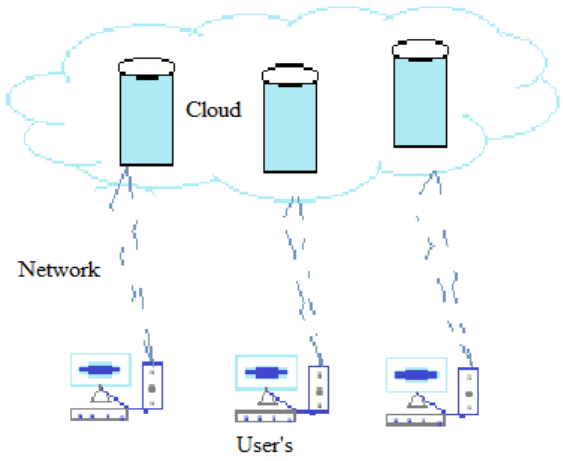

Figure1. Cloud computing

This accident resulted in some network sites rely on a single type of storage service. Security vulnerabilities in Google Docs led to serious leakage of user information in March 2009. It was exposed that there was security vulnerability in VMware virtualization software in May 2009[1]. In September 2014, security vulnerabilities in iCloud led to serious leakage of user information. So there is a need of security in cloud computing so that users can utilize this latest technology without fear. The remainder of this paper is organized into different sections. The first one is data security frame work. In sectionII discusses issues in data security. SectionIII is about different solutions for data security with data security models. In sectionIV conclusion and future work are mentioned.

DATA SECURITY FRAME WORK:

To protect data in cloud we have two ways, standard and non standard as shown in figure2. In standard way security is provided by encryption and in non standard way indexing and masking are the two ways. In data security model standard and non standard ways are used to protect data in cloud.

Manuscript received January 22,2015.
Kavita Rathi CSE Department, Deenbandhu Chhotu Ram Universityof Science and Technology, Murthal, India,890220999
Narender, CSE Department, , Deenbandhu Chhotu Ram Universityof Science and Technology, Murthal, India,9991277368

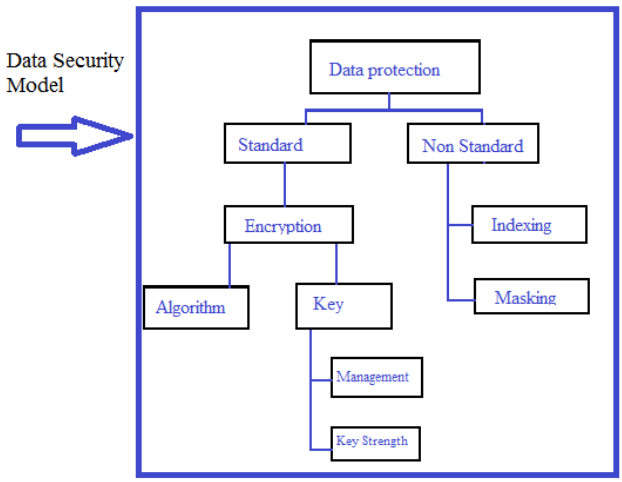

Figure2 [2] Data security framework

The data's that we place in cloud can classified in to either stagnant or vibrant. The stagnant data's are the one which will never change during the entire storage. Amazon's simple storage service (Amazon S3) offers such type of service. The security solution for stagnant data is to simply encrypt the data and store safely in the cloud. Whenever there is a need of data bring the data to the client site decrypt and use the data. The vibrant data's are the one which changes often and are to be handled in a specific manner. As in the case of stagnant data we cannot work on the vibrant data. So we need overall data security with the help of data security models [2].

II. ISSUES IN DATA SECURITY

Issues in data security are associated with the data life cycle [3] as shown in figure3. Following are the different-different phages:
Creation: Initial phase of data life cycle where data has to be created or altered.
Store: During this phase data need to be stored and data present at rest.
Use: This phase is to use the data and data reside in this phase at motion or processing.
Share: this phase share data with other jobs.
Archive: at this phase data reside for long time storage
Destroy: data permanently destroyed.

Figure3 [3]: Data security life cycle

From data creation to the destroy we need to protect data by providing proper security mechanism. In all the data life cycle phages data present in different- different state as shown in table1. To protect data in all these stages are major issues in cloud computing.

Data Security Life Cycle - Phases	Data Security in Cloud Computing
Create	Not Applicable
Store	Data – at – rest
Archive	
Use	Processing of Data
Share	Data – in – transit
	Data Lineage
	Data Provenance
Destroy	Data Remanence

Table -1[3]: Mapping from Data Security Life Cycle to Data Security in cloud Computing

Data security covers following major issues in cloud computing:
Data – in – transit [4]:
To protect the data in moving stage is a major issue in cloud computing and data in this stage can be secured with encryption algorithm and protocols. The protocol provides confidentiality and integrity. Protocols like Hyper Text Transfer Protocol Secure [HTTPS] and File Transfer Protocol Secure [FTPS] are useful for transferring data across the internet.
Data – at – rest [4]:
There is a need to protect the data which is at rest in cloud computing and with the help of encryption techniques data in this stage can be protected. IaaS (Infrastructure as a service) cloud service for simple storage encrypting data-at-rest is simple and easy. But encrypting data-at-rest for a PaaS(platform as a service) or SaaS(software as a service) cloud-based application is not always viable. Data-at-rest used by a cloud based application is not normally encrypted, because encryption would prevent indexing or searching of that data. So some special encryption techniques are required.
Processing of Data [4]:
There is a need to protect data during processing stage. When data is in processing stage then for short time data remain unencrypted form before June 2009. In June 2009 IBM announced the development of fully homomorphic encryption scheme [6] which allowed data processing by application without being decrypted. This advancement made data to be encrypted during its entire life cycle.
Data lineage [4]:
Recording the path of data (dataflow or data path) is known as data lineage and it is important for an auditor's assurance. The critical factor in data lineage is time consuming. Lineage is necessary for compliance purposes. Here exact records as to what data was placed in a public cloud, when it occurred, what VMs and storage it resided on and where it was processed are maintained.
Data Provenance [4]:

Provenance means that the data has integrity and also it is computationally accurate; that is, the data was accurately calculated. Data provenance provides a full accounting of data from its creation to the present, provides a means of determining the legitimacy of information as well as the manner of handling. Securing provenance is challenging for a number of reasons.

Data Remanence [4]:

The data remnants occur due to incomplete delete operation or through physical properties of the media. This is remnants of data present in the storage media. Data Remanence is a serious security threat through which sensitive information can be revealed. This threat becomes reality when the storage media with data remnants released into an uncontrolled environment.

Adding intelligence to network protection:

The network protection needs more protection to have the ability to provide extra control with analytics and insight into which user's are accessing what content and applications [5].

Data Location and Relocation [7]:

Cloud computing provides a high degree of data mobility. Consumers usually do not know the location of their data. However, when an enterprise has some private data that is kept on a storage device in the cloud, they may need to know location where the data are stored.

Agents in data security [8]:

To make the cloud computing data security task simple and to provide more reliable services there is a need of agents in cloud security. To add agents in cloud security is also a major challenge.

III. DATA SECURITY MODELS FOR CLOUD COMPUTING

To keep in mind that sensitive information leakage is more crucial so a distribution model for Data Leakage Prevention [9] was proposed to prevent data leakage. With the account of the users' guilt probability, the model can select an allocation plan with the least overlap between obtained file set of involved users. Hence the consequence the model can find out leakage sources with high probability, and measures could be taken to prevent further leakage. Model can distinguish malicious users, that is, the guilt probability of malicious is highest with contrast of honest or common users. Thereby the distribution model can effectively detect the leak source so as to protect information security.

A lot of research is still going on regarding the security of e-commerce to provide security in this field. E-commerce transaction security model based on cloud computing was proposed [10] which provide good security. Security engineering is all about ensuring that everything goes well in front of an intelligent and malevolent antagonist who wants to commit fault every time. There is a lot of issue concerning the security in e-commerce.

Enhanced Data Security Model [11] for Cloud Computing was proposed which provide data security on the bases of architecture of cloud computing and applied by EC2 Amazon micro instance.

A frame work of different specialized procedures and techniques was proposed [12] that can protect the data from the beginning to the end (from the cloud to the users). The classification of data is done on the basis of the value of three cryptographic parameters (Confidentiality, Integrity and Availability) given by the users. The strategy utilizes various measures such as the SSL (Secure Socket Layer) 128-bit encryption. MAC (Message Authentication Code) is used to check integrity of data, searchable encryption and division of data into three sections for storage in cloud. Three sections of data deliver simple access and protection of the data

A novel third party auditor scheme was proposed [13]. The obvious advantage of this scheme is the cloud service provider can offer the functions which were provided by the traditional third party auditor and make it trustful. So it indeed reduces the constitution's complexity in Cloud Computing.

Based on multi-dimension a new data security model was proposed [14]. The model adopts a multi-dimension architecture of three - layers defense. First of all, user authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can get relative operation on the user data, such as addition, modification, deletion. If the unauthorized user use illegal means to deceive the authentication system, the file entered the system encrypt and privacy defense levels. In this layer, user data is encrypted. If key has been got by the intruder. The user data cannot be got valid information even it is obtained through function of privacy protection. It is very important for commercial users of the cloud computing to protect their business secrets. The last is the file quick regeneration layer, user data can get maximum regeneration even when it is damaged through rapid regeneration algorithm in this layer. Each layer accomplishes its own job and combines with others to ensure data security in the cloud computing.

Different- Different data security models and their characteristic are shown in table2.

Author	Model	characteristics
Yin Fan and Wang Lina	A distribution model for Data Leakage Prevention[9]	This model can select a file allocation plan with the least overlap between obtained file sets of users, as the Consequence the model can find out leakage sources with high probability.
Wasin Treesinthuros	E-commerce transaction security model based on cloud computing[10]	This model provides confidentiality, integrity in e-commerce cloud computing.
EmanM .Mohamed and Hatem S. Abdelkader	Enhanced Data Security Model[11] for Cloud Computing	This security model of cloud computing based on the study of the cloud architecture, Finally apply this software in the Amazon EC2 Micro instance

Sandeep K. Sood	A combined approach to ensure data security in cloud computing[12]	This model provides integrity and authentication. This method achieves the availability, reliability and integrity of data traversing through owner to cloud and cloud to user.
Shuai Han and Jianchu an Xing	Ensuring data storage security through A novel third party auditor scheme in Cloud computing[13]	To ensure each data access in control and reduce the complexity of cloud computing, This model propose a scheme using RSA and Bilinear Diffie-Hellman techniques. Confidentiality of users' access privilege and authentication accountability can be achieved.
Zhang et. al.	Research on Cloud Computing Data Security Model Based on Multi-dimensi on[14]	The model adopts a multi-dimension architecture of three - layers defense. User authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can get relative operation on the user data, such as addition, modification, deletion.

Table2. Different models and their characteristics

Various data security models has been proposed but still data security issue persist so some good data security models are required to protect data in cloud.

IV. CONCLUSION AND FUTURE WORK

This paper describes various security approaches to secure data in cloud. Paper represents data security models with their characteristics. A large number of security models have been used to secure data in cloud computing yet more work has to be done to make it more efficient and secure. Because of lacking in data security in past cloud services been interrupted many time and make cloud as a disruptive business model so in future there will be requirement of a complete security models which protect data in all stages i.e. data at rest, during processing of data, data in transit, data provenance and data remanence.

.

REFERENCES

[1]Dr. P Dinadayalan, S Jegadeeswari and Dr. D Gnanambigai, "Data security issues in cloud environment and solutions", In IEEE, International conference on cloud computing, pp. 88, 2014.
[2] V.Nirmala, R.K.Sivanandhan and Dr. R.Shanmuga laks, "Data confidenciality and intigrity verification using user authenticator scheme in cloud", In IEEE, 2013.
[3] T V Sathyanarayana and Dr. L. Mary Immaculate Sheela, "Data security in cloud computing", In IEEE, International Conference on Green Computing, pp. 822-827, 2013.
[4] Tim Mather, Subra Kumaraswamy, and Shaid Latif, "Cloud Security and Privacy ".O'Reilly Media, Inc., 2009.
[5] sneha vasant thakre and deipali V.Gore, " Comparative study of CIA and revised CIA algorithm", In IEEE, Fourth International Conference on Communication Systems and Network Technologies, pp.713 to 718, 2014.
[6] Yubo Tan, Xinlei Wang, "Research of cloud computing data security technology" in IEEE, pp-2781-83, 2012.
[7] M. Sugumaran, BalaMurugan and D Kamalraj, "An architecture for data security in cloud computing", In IEEE, World Congress on Computing and Communication Technologies, pp. 252-255, 2014.
[8] Feng-qing Zhang and Dian-Yuan Han," Applying agents to the data security in cloud computing", In IEEE, International Conference on Computer Science and Information Processing, pp. 1126-1128. 2012.
[9] Yin Fan and Wang Lina, "A distribution model for data leakage prevention", In IEEE, pp 2617-2620, 2013.
[10] Wasin Treesinthuros, "E-commerce transaction security model based on cloud computing", In IEEE Proceedings, pp. 344 -347,2012.
[11] EmanM.Mohamed and Hatem S. Abdelkader, "Enhanced data security model for cloud computing", In IEEE, The 8th International Conference on INFOrmatics and Systems (INFOS2012), pp. 12-17, May 2012.
[12] Sandeep K. Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, pp. 1831–1838, 2012.
[13] Shuai Han and Jianchuan Xing, "Ensuring data storage security through a novel third party auditor scheme in cloud computing", In IEEE Proceedings, pp. 264-268, 2011.
[14] Zhang Xin, Lai Song-qing and Liu Nai-wen, "Research on Cloud Computing Data Security Model Based on Multi-dimension"

Prof. Kavita Rathi, CSE Department , Deenbandhu Chhotu Ram University of Science and Technology, Bachelors and Master's Degree in the field of Computer Science and Engineering. She has keen interest in the area of Cloud Computing, and has published several papers in National and International conferences and journals. Prof. Kavita Rathi has more than five years of experience in teaching undergraduate as well as postgraduate students. She has attended several workshops and faculty development programs.

Narender, Master of Technology, Computer Science and Engineering, Student, Deenbandhu Chhotu Ram University of Science and Technology, Murthal. Area of Interest: Cloud Computing