IJCSC 0973-7391 Volume 6 • Number 1 Sep - Mar 2015 pp.83-86 available online at www.csjournalss.com

A Review on Using Cryptography Techniques for Securing User Data in Cloud Computing Environment

[1]Ramandeep Kaur Bhinder, [2]Dr. Dheerendra Singh and[3]Er.Gurjot Singh Sodhi
[1]Student, M.Tech CSE, SUSCET, Tangori, Mohali, Punjab, India
[2]Professor &Head, Dept. of CSE, SUSCET, Tangori, Mohali, Punjab, India
[3]Assistant Professor, Dept. of CSE, SUSCET, Tangori, Mohali, Punjab, India
ramandeep.bhinder91@gmail.com, professordsingh@gmail.com, gurjotsinghcse@sus.edu.in

Abstract- At present, a large number of organizations are moving towards cloud for storing a large amount of data. Cloud Computing is a technology to provide services over the internet. Cloud act as Data Centre. A customer utilizes clouds resources and services and is charged accordingly. Security is the most important concern in cloud computing. There are many security issues of cloud computing which are related to trust, data confidentiality, authentication, access control etc. 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. The main focus is to study various issues and challengeswith the types of cryptographic algorithm implemented in cloud computing environment.
Index Terms- Cloud Computing, security, issues, challenges, Cryptography algorithms.

I. Introduction

Cloud Computing nowadays is the essential part of the computing world with every day increases in its usages and popularity. Large number of users is now dependent on Cloud Computing application for their day to day work of professional and personal life. Cloud Computing is a technology to provide services over the internet. Cloud act as data Centre. A customer utilizes clouds resources, storage and other services and is charged accordingly. Subscription to cloud is based on the type of services requires by users Iaas (Infrastructure as a service), Paas (Platform as service) and Saas (Software as a service). Therefore Cloud Computing has emerged as a means by which computational power storage, resources and application as provided to users as 'Utility' for meeting their demands.This cloud model promotes availability. It is composed of five essential characteristics, three service models and four deployment models. Five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Three service models are Infrastructure as a service (IaaS), Platform as service(PaaS) and Software as a service (SaaS). Four deployment models are Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud.

II. Issues and Challenges Of Cloud Computing

Cloud computing is emerging technology being used by large numbers of users worldwide. With every advantages and uses of cloud computing, there are numerous issues associated with it, and challenges which are to be overcome for more widespread adoption at different levels.

Privacy: Cloud storage has large amount of data stored in it, so there is greater risk bind with it of data being disclosed in either way–intentionally or unintentionally. Intermediaries or hosting companies that take service from Cloud Service Provider (CSPs) and made them available to end users, Intermediaries has greater amount of control they can monitor communication between Cloud Service Provider and end user and can also access data. So cloud service provider can complicate privacy of users and data with the help of virtual machines (visualization) and complicating cloud storage. The service provider or employees administrators working on cloud can access customer's data at any time. Hence privacy is major concern of Cloud Computing developers and service providers.

Security: Cloud Computing services security is the international issue which is stopping cloud computing from its much wider adoption for ensuring that the data links are not compromised. Data links are physically controlled and visually inspected. Solution of security issue is encryption and decryption using cryptographic techniques, improving virtual machine support use of multiple cloud providers etc.

Performance: In Cloud Computing environment running application capability define performance. Performance is suffered from lack of proper resources, disk space, limited bandwidth, network problems, connection, CPU speed, memory etc. User may prefer to use services from more than Cloud Service Provider (CSPs) then performance of one can affect other. Performance is major concern not only functioning of cloud system but also affects service delivery, bottom line revenues, numbers of customers etc.

Reliability and Availability: Reliability of the system is defined as the probability of proper functioning of system over a certain period of time under defined conditions. Availability of the system is defined as the prospect of using resources of the system whenever and wherever

required. Reliability and availability together gives measure of strength of system. Reliability and availability of cloud system not only deals with the whole system but also with each service resources or application required or used by the customer. To provide customers effective and good quality services, reliability and availability are important over to care for by the cloud service providers who are developing cloud system.

Scalability and Elasticity: Scalability of a system is defined as the ability of the system to administer increasing amount of work in efficient manner. As the cloud computing services are now used by large number of users, therefore cloud system must be capable of handling rowing numbers of users and their demands. Cloud system should work efficiently despite of increasing number of users. Elasticity of the system is defined as the amount to which a system is able to handle workload changes by allocation and de allocation resources in automatic manner. Elasticity of cloud computing system means handling varying i.e. increasing and decreasing demands of resources by the users.

Interoperability and Portability: Interoperability of system is defined by its ability to work with other systems or to run different applications, software programs from different vendors. In cloud computing system interoperability is defined as the ability of using tools, applications resources across CSPs platforms. Lack of open standards, standards interfaces serves as major problem in realization of interoperability. In cloud computing terminology portability is defined as the ability to move applications and its related data between one CSP to another or between cloud deployment models.

Resource Management and Scheduling: Resource management is defined as the effective and efficient use and management of resources. Such resources are disk space, threads, input output devices, memory, CPUs. Allocation and management of resources provides desired level of services for the customers. Scheduling is a method by which resources are assigned to different tasks on some basis and algorithm. In cloud computing environment resources are services, applications, software. Job Scheduling is another important issue. Job scheduling orders the execution of different jobs to optimize turnaround time, response time, throughput, etc. Partitioning of jobs in parallel tasks, prioritizing tasks, allocation to resources, execution, nature of job, topology, workload, and memory required. Synchronization and overheads are some of the examples of the important issues of job scheduling.

Energy consumption: Cloud data storage consists of large number of servers and other devices. A cooling infrastructure is developed and set up to remove heats generated by these servers. Cloud data storage as a whole (both servers are cooling infrastructures) consumes large amount of energy. This whole infrastructure is expensive to set up, operate and maintain. Servers and cooling infrastructure produces greenhouse gases (GHGs) which affects environment adversely. So the issue is not only to reduce energy consumption and reducing cost but also to maintain environment standards so that for achieving something small, we are not depleting the biggest and important factor of our lives- the environment.

Virtualization: In computing, virtualization refers to the act of creation of virtual models of something hardware, software, operating system, storage device or other resources. Virtualization splits resources, application, and software to multiple execution environments. It hides the physical characteristics of the resources. Sometimes for better performance, data is shifted to other location for execution of the location at which end user data was saved goes down or get damaged, then through virtualization. Cloud service provider shifts user data to other location. For cloud computing environment, visualization is a major issue. Virtualization benefits include supplied elasticity, cost effectiveness, scalability etc.

Bandwidth Cost: According to computing bandwidth means bit rate or throughput, data transfer rate measured in bits per second(bits/sec) for efficient working of cloud computing system, communication channel should be of high speed cost of working n cloud, for transferring data between the clouds is much higher. It also requires good handwritten which further increases cost. So for preparing data related problems, private clouds should be used instead of other deployment models such as public or hybrid.

III. Various Encryption Techniques

RESEARCH	DESCRIPTION	FEATURES
Prajapati and Rathod (2015) [1]	Bi-directional DNA encryption algorithm for enhancing security	Encrypts both Unicode and ASCII character. Provides two-level security.
Mishra et.al (2015) [2]	Various security issues in cloud computing Comparison of both symmetric and asymmetric encryption algorithms	AES algorithm is best among symmetric algorithms and offers higher security, performance, flexibility and requires less memory. RSA algorithm is best among asymmetric algorithms. It is faster and efficient.
Sivasakthi and Prabhakarn (2014) [3]	Encryption algorithm using RSA algorithm for authentication and Digital Signature	RSA encrypts user data files. Digital signature is done by both client and server using RSA algorithm. This offers high level of security.

Singh and Supriya (2013) [4]	Study of AES, DES, 3DES and RSA algorithms for security	AES encrypts and decrypts data in lesser time and RSA encrypts and decrypts data in longest time. AES provides highest security and RSA provides least security.
Jenson et.al (2009) [5]	Technical security issues in cloud computing	Security issues and challenges such as XML signature, browser securitywhich includes legacy same origin policy, attacks on browser based cloud authentication, cloud integrity and binding issues, flooding attacks etc. were discussed.
Li et.al (2012) [6]	Attribute based encryption (ABE) of Personal Health Records (PHR)	Provides high security. Key management complexity is reduced. Enables break glass access under emergency situations. High performance achieved.
MT Nurpeti et.al (2014) [7]	Chaos based encryption algorithm using Logistic map on images	Reliable, secure and fast encryption method. Value distribution of pixels is uniform in encrypted image. Fully random key stream generated. Large key space hence offers high security.
Saparudin et.al (2014) [8]	Chaos based encryption algorithm using Henon map	Provides higher output quality, more secure, reduced data redundancy, resist Brute Force attacks, enhances execution speed and time, reduce overheads, effective and efficient.
Nagaraj et.al (2015) [9]	Voice Biometrics cryptography protocol for security	Protocol developed using Elliptic Curve Cryptography (ECC) was faster and efficient. Encryption and password protection algorithm provides high security and saves from Brute Force attack.
Madan and Mathur (2014) [10]	Cloud traffic handling using Cloud Network Management Model (CNMM)	Handles cloud traffic in effective and efficient manner. Reduced packet exchange. Secure and efficient communication.
Sachdeva and Mahajan (2013) [11]	Study of AES, DES and RSA algorithms for security	RSA algorithm takes longer time for encryption and decryption than AES and DES. AES showed best results for encryption and decryption speed, efficiency and flexibility.
Sidhu and Mahajan (2014) [12]	Hybrid encryption algorithm using Hashing function for security	Hashing function encryption is performed in an easy and light process. Prevents inside attacks of cloud computing.
Sharma et.al (2014) [13]	Combination of authentication and file integrity technique for improving cloud data security.	Double encryption and cyclic modes increased randomness of cipher text. Provides high security and cost effective. Established trust bond between client and server.
HA and Agrawal (2014) [14]	Multilevel cryptography algorithm for security of data using meta data and lock approach	Customers can process data in multiple levels and multiple ways to provide more security according to sensitivity. Enhances reliability, effectiveness and efficiency.
Thakur et.al (2014) [15]	Security algorithm using RSA, SHA and MD5	RSA algorithm provides reliable and secure communication. MD5 algorithm provides hashing to user data.
Khedkar and Gawande (2014) [16]	Security of user data by data partitioning method	Provides high integrity of data, higher level of predicting and localization of errors, simple identification of unauthorized access and misbehaving client and server. Remote data integrity checking detects risks, issues and threats of cloud data storage.

REFERENCES

[1] Prajapati, Ashish, and AmitRathod. "Enhancing Security in Cloud Computing Using Bi-directional DNA Encryption Algorithm." Intelligent Computing, Communication and Devices.Springer India, 2015.349-356.

[2] Mishra, Neha. "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues." RIET-IJSET: International Journal of Science, Engineering and Technology 2.1 (2015): 59-68.

[3]Sivasakthi, T., and N. Prabakaran. "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing."International Journal of Innovative Research in Computer and Communication Engineering 2.2 (2014): 456-459.

[4] Singh, Gurpreet, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." International Journal of Computer Applications 67.19 (2013): 33-38.

[5] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." System Sciences (HICSS), 2011 44th Hawaii International Conference on.IEEE, 2011.

[6]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 24.1 (2013): 131-143.

[7] Suryadi, M. T., and Eva Nurpeti. "Performance of Chaos-Based Encryption Algorithm for Digital Image." TELKOMNIKA (Telecommunication Computing Electronics and Control) 12.3 (2014): 675-682.

[8] Saparudin, Saparudin, GhazaliSulong, and Muhammed Ahmed Saleh. "Multi Facial Blurring using Improved Henon Map." TELKOMNIKA (Telecommunication Computing Electronics and Control) 12.4 (2014).

[9] Nagaraj, Srinivasan, et al. "A Bio-Crypto Protocol for Password Protection Using ECC." Bulletin of Electrical Engineering and Informatics 4.1 (2015): 67-72.

[10]Madan, Mamta, and MohitMathur. "Cloud Network Management Model A Novel Approach to Manage Cloud Traffic." arXiv preprint arXiv:1411.2084 (2014).

[11]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).

[12]Sidhu, Aparjita, and Rajiv Mahajan. "RESEARCH ARTICLE ENHANCING SECURITY IN CLOUD COMPUTING STRUCTURE BY HYBRID ENCRYPTION." International Journal of Recent Scientific Research 5 (2014): 128-132.

[13]Sengupta, Shubhashis, Vikrant Kaulgud, and VibhuSaujanya Sharma. "Cloud computing security--trends and research directions." Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[14]Annappaian, DineshaHagare, and Vinod Kumar Agrawal. "Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud."Transactions on Networks and Communications 2.6 (2015): 47-55.

[15]Thakur, Namrata, VimmiPandey, and Brejesh Singh. "An Innovational Approach to Security in Cloud Environment." (2014): 52-54.

[16]V Khedkar, Swapnil, and A. D. Gawande. "Data Partitioning Technique to Improve Cloud Data Storage Security." International Journal of Computer Science & Information Technologies 5.3 (2014).