Cloud Data Center Security and Cryptography a Survey

Mr.KanwarLal Dhakar[1], Prof. SavitaRathod[*2]

Computer Science& Engineering, Truba College of Engineering & Technology,

Indore (RGTU Bhopal) India

Abstract—*Cloud computing is a powerful weapon for human now in these days, these data environment is able to provide the computational ability, software services, data storage and other important applications remotely. Using these remotely accessible services is used for various levels of application development and deployments. The proposed work is intended to design a security system for cloud data centers, these data centers are used for storage of various sensitive and confidential data therefore security is a major concern about the data.in this presented work a survey on the cloud computing technology and the existing security techniques are provided. Additionally a new security technique is proposed which is used to prevent the data during the authentication based issues, transmission based issues and storage based issues.*

Keywords*— cloud servers, data outsourcing, network transmission, cryptographic cloud, data exchange;*

I. Introduction

Cloud storage is a model of networked venture storage anywhere data is stored in virtualized pools of storage which are generally hosted by third parties. Cloud service Hosting companies operate large data centers and people who require data to be hosted buy or lease storage capacity. The data center operators, in background, provide the resources according to the supplies of the client and representation them as storage available, which the customers can themselves use to store files or data objects. Actually resource may span across multiple servers and multiple locations. Safety of the records depends winning the hosting companies and on the applications that leverage the cloud storage. [1]

Now in these days in the area of cloud computing different security models and algorithms are uses. Unfortunately these models have abortive to resolve every the majority all the security threats. Additionally for E-commerce and different types of online business, requirement of imply high capacity security models in cloud computing domains. Security models that are developed and presently used in the cloud computing situation are mainly used for providing security for a file and not for the communiqué. In addition there security models are sometimes uses secured channel for communication. Though, this is not cost efficient process. Yet over, it is rare to find a combined work of main server security, operation among them and so on. Few models attempt on discussing about all, but they are completely dependent on user approach. The simulations usually fail to use machine intelligence for generating key and newer available model. Few models have future regarding hardware encryption system for secured communication system. The concept is usually direct, but the performance is rather difficult. Moreover, hardware encryption is helpful only for the database system, not for other security problems. Authenticated user detection technique is currently very important thing. This technique is rarely converse in the only just used models for ensuring security in cloud computing. Cloud computing has a mixture of individuality, with the main ones being: [2]

- ***Shared Infrastructure* —** Uses a virtualized software model; permit the contribution of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of operation model, seeks to make the mainly of the presented infrastructure across a number of users.
- ***Dynamic Provisioning*** — Allows for the stipulation of services based on existing demand requirements. This is done automatically using software automation, permit the increase and reduction of service capability, as needed. This dynamic scaling needs to be done though maintaining high levels of consistency and security.
- ***Network Access* — *needs*** to be accessed across the internet from a minor road range of devices such as PCs, laptops, and mobile devices, using standards-based APIs (for example, ones based on HTTP). Deployments of forces in the cloud include everything from using business applications to the newest application on the most recent smartphones.
- ***Managed Metering*** — uses metering for managing and optimizing the service and to provide exposure and billing in sequence. In this way, consumers are billed for services

according to how much they have in fact used through the billing episode.

In short, cloud computing permit for the sharing and scalable deployment of services, as required, from approximately any location, and for which the customer can be owed based on actual usage.

Advantages and Disadvantages

Several key profit to use cloud computing which is known in [3] are as:

- ***Reduced Cost*****:** Cloud technology is waged incrementally (you pay only for what you require), saving association money in the short run. Capital saved can be used for other significant income.
- ***Increased Storage:*** Organizations preserve store more data than on confidential computer systems.
- ***Highly Automated:*** IT personnel not required to keep software up to date as continuation is the job of the provision contributor on the cloud.
- ***More Mobility:*** Employees can admittance in sequence where they are, quite than have to wait at their desks.
- ***Allows IT to Shift Focus:*** No longer having to concern regarding regular server updates and other computing problem, supervision organizations will be free to concentrate on innovation.

In addition of some limitations are also provided in [3] are:

GNU founder Richard Stallman says that the exciting thing regarding cloud computing is that we've redefined cloud computing to include everything that we already do. One because you must not use web applications to do your computing is that you lose control. It's just as bad as using a proprietary program [4]. But certainly shifting to cloud computing has other problems including:

- ***Security:*** Is convenient a security standard?
- ***Reliance on 3rd Party:*** Control over own data is lost in the hands of an “difficult-to-trust” contractor
- ***Cost of transition:*** Is it practical for me to move from the existing architecture of my data centre to the construction of the cloud?
- ***Uncertainty of benefits:*** Are there any long term benefits?.

II. LITERATURE SURVEY

This section includes the various previously made efforts; those are contributed on providing security over cloud environment.

Cloud computing is the extended dreamed idea of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality request and services from a shared pool of configurable computing capital. While data out sourcing reduce the proprietor of the load of local data storage and maintenance, it also reduces their corporeal control of storage dependability and security, which traditionally has been estimated by together venture and individuals with high service-level requirements. In order to facilitate express deployment of cloud data storage service and improve security reassurance with outsourced data depend ability, resourceful technique that enable on-demand data accuracy verification on behalf of cloud data owners have to be designed. In this article ***Cong Wang et al [5]*** recommend that overtly auditable cloud data storage is gifted to help this nascent cloud economy develop into fully established. With the help of public audit ability, a trusted entity with expertise and capabilities data owners do not possess preserve be hand over as an exterior audit party to review the risk of outsourced data when required. Such an auditing service not only helps save data owners' computation income but also provides a see-through yet commercial technique for data proprietor to enlarge trust in the cloud. They explain approaches and system requirements that must be brought into consideration, and outline challenges that require being determined for such in public auditable secure cloud storage service to become a reality.

John Harauz et al [6] in 2009 published an article according to their article, In the 1990s, the world was establish to the Internet, and we began to see distributed computing power realized on a big scale. Today, we have the aptitude to utilize scalable, distributed computing environments within the confines of the Internet, a practice recognized as cloud computing. This situation strives to be vibrant, reliable, and customizable with an assured quality of service. Inside this system, users have a myriad of virtual resources for their computing needs, and they don't need a complete understanding of the communications, Cloud computing arrival has made the declaration by Scott McNealy, Sun Micro systems' founder, that “The network is the computer's veracity and given the old Sun marketing motto a new life.

Balachandra et al [7] in 2009 provides an study about the security in cloud environment, according the given architecture, In past three decades, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the practical centralization (Cloud Computing). Location of data and processes makes the dissimilarity in the empire of computation. On one hand, an person has full control on data and processes in his/her system. On the further hand, we have the cloud computing where in, the service and data preservation is provided by several vendor which leaves the client/customer ignorant of where the procedure are running or where the data is stored. So, rationally language, the client has no manage over it. The cloud computing uses the internet as the communication media. When we appear at the security of data in the cloud computing, the merchant has to provide several assurance operating level agreements (SLA) to convince the consumer on security problem.

The cloud computing platform gives community the opportunity for sharing capital, services and in sequence between the communities of the complete world. In private cloud system, information is shared between the persons who are in that cloud. For this, security or individual in sequence hiding process hampers. In this paper ***KawserWazedNafi et al [8]*** have proposed new security architecture for cloud computing platform. This ensures secure communication system and defeat in sequence from others. AES based file encryption scheme and asynchronous key system for exchanging information or data is incorporated in this model. This constitution can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model in addition comprises once password system for user authentication process. The given work mainly contract among the security system of the entire cloud computing platform.

Cloud computing has been considered as one of the promising resolution to our growing require for accessing and using resources provisioned over the Internet. It offers influential processing and storage income as on-demand services with reduce cost, and amplify competence and presentation. All of these features and more support enterprise, governments and even critical infrastructures providers to migrate to the cloud. Serious infrastructures are measured as a backbone of modern societies such as power plants and water. Though, among all of these capable facilities and profit, there are still a number of technical barrier hinder utilize the cloud such as refuge and quality of services. The target of this survey given by ***Younis A. Younis et al [9]*** is to discover possible security concern connected to securing cloud computing for critical communications providers. It things to see security challenges in cloud computing and consider the security requirement for a variety of critical communications providers.

Cloud computing is a recent trending in IT that moves computing and data away from desktop and portable PC sin to large data centers. It refers to applications delivered as services over the Internet as well as to the definite cloud communications—namely, the hardware and systems software in data centers that provide these type of services. Various organizations use cloud computing as a service infrastructure; decisively like to examine the security and confidentiality issues for their business serious insensible request. Yet, guaranteeing the security of corporate data in the "cloud" is complicated, if not not possible, as they provide different services like Software asa service (SaaS), Platform as a service (PaaS), and communications as a service (IaaS). Each service has their, possess refuge issues. In this paper ***adhuChauhan et al [10]*** presents different types of security problems related with cloud computing, and its possible solution.

III. PROPOSED WORK

To overcome the discussed problem associated with the presented security architecture in [8]. A new solution is proposed for secure access of data. Thus a new cryptographic scheme is introduced to provide security using. The below given figure 1 provides the involved security process. According to above given system there are three individual identities are involved namely the client, cloud storage server and a security server.

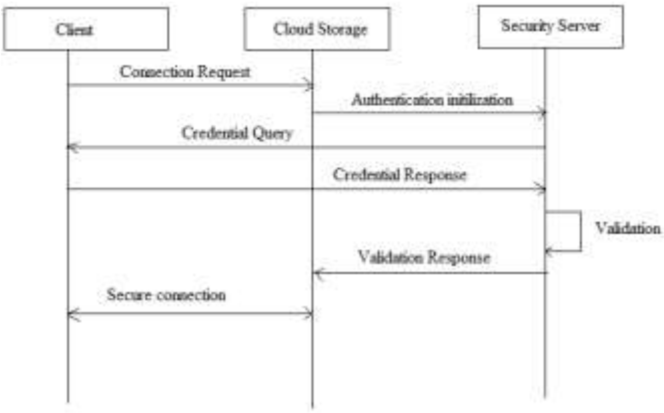

Figure 1 security architecture

Client is a device which used by any client to connect with the cloud server for data storage. Third is a security server which keeps in track the security between both parties. The figure 1 includes the arrows to demonstrate the steps followed for secure communication and authentication. These steps are summarized as:

1. ***Client connection request:*** to access services by client device a request to the server is made. If the client is registered previously than, the server triggers a method to call the authentication or security server.
2. ***Authentication initialization*****:** in this step cloud server initiate the authentication using the secure third party server.
3. ***Credential query:*** the secure server ask the credential query randomly to the client such as date of birth, PAN card number or other

information which is submitted during registration process.

4. ***Credential response:*** in this step client answer the query asked by the authentication server, during this process server send the one time password also to verify the user identity.
5. ***Validation response*:** the user submitted credentials and the one time password is validated from the existing database.
6. ***Validation response:***if the user provides the correct information the secure server response to the cloud server for authentication steps are completed. Otherwise the secure server do not complete the user connection request.
7. **Secure connection:** after successfully validation of user the system enable the user and server to communicate each other and utilize the different utility implemented on server using cryptographic techniques.

Encryption process:

Genetic algorithm is a search algorithm and now in these days used in various other applications of problem solving, classification and cluster analysis etc., in order to provide security there are also some algorithms are available. During the study of literature we found a large amount of papers and articles that working with the domain of DNA encryption based security architecture. Each and individual authors are propose and design a new algorithm for encrypting and decrypting the data. The proposed architecture in [6] and others may use the AGTC code book for encryption and decryption due to static code book an attacker can be brake the cypher text and recover the original text.

The compression ratio is another issue in the DNA cryptographic approach the previously derived maximum techniques are based on converting the actual text to binary strings and again converting those into AGTC codes these codes are generate a large amount of cypher text this cypher text size is always the having greater than the size of the original text.

According to the above discussion we need to enhance the approach of encryption and decryption and required to improve the following deficiencies in the previously proposed architecture.

1. Use of static code book.
2. Size of cypher text
3. Low level of security of data

In order to find the solution for the identified problem in the previous method of DNA cryptography we propose the following solution to according the problem domain before providing the solution we make a small review of the previously designed DNA cryptographic algorithm.

This paper has as main purpose to provide the understanding of principles and some techniques of the new natural pasture of DNA steganography and cryptography. The presentation is illustrated with small examples using bioinformatics toolbox for parts of the algorithm not need DNA laboratory experiments, very expansive at this moment.DNA, the major support of genetic in sequence (genetic blueprint) of any organism in the biosphere, is composed of two long strands of nucleotides, every contain one of four basis (A – adenine, G – guanine, C – cytosine, T – thymine), a deoxyribose sugar and a phosphate group. The DNA strands include chemical schism, meaning that on each end of a molecule there are different groups (5' – top end and 3' – bottom end) [7].

The DNA strands can be chemically synthesized using a machine, known as DNA synthesizer. The single-stranded chains acquire synthetically with the DNA synthesizer are named oligonucleotides having frequently 50-100 nucleotides in length. In the present paper the individual strands will be referenced as single-stranded DNA (ssDNA), and the dual whorl as double-stranded DNA (dsDNA). Individual ssDNA can, under certain conditions, form dsDNA among other matching ssDNA. This process is called hybridization, because the double-stranded molecules are hybrids of strands coming from different sources.

Gene is a segment of DNA that contains coding sequences (exons) and non-coding series (introns) that decide when a gene is active (expressed). When a gene is active, the coding series is imitative in the transcription process in mRNA and in the translation process, the mRNA direct the protein synthesis via the genetic code. Dictation is governed by regulatory elements, which are short (10-100 base pairs) DNA series that control gene appearance. Genetic material is a large organized constitution of DNA coiled around proteins; contain genes, narrow essentials and other one is nucleotides sequences. It replicates autonomously in the cell and segregates during cell division.

The entire DNA content of a cell, containg nucleotides, genes and chromosomes are known as the genome. Each being contains a unique genomic series with a unique structure. Polymerase chain reaction (PCR) is a molecular biology technique used to exponentially amplify some regions of DNA using enzymatic duplication and starting with the DNA portion (primer) to be amplified. The technique of Recombinant DNA technology (gene splicing, genetic engineering) uses enzymes to cut and paste DNA "recombinant" molecules. Recombinant DNA enables the separation and cloning of a gene and PCR its amplification.

Previous architecture of DNA cryptography:

In this approach the user plain text is supplied and massage is converted into HEX code and then converted into binary codes of the original massage. The complete binary message is converted into two equal parts and combined using the XOR operation. After combining the message the complete binary string is converted into DNA encoding using the AGTC code book. The generated encoding is supplied into a PCR amplifier for amplification the amplified message is goes through the compressor to compress the message and final cipher text is obtained.

In the previously proposed system there are a large number of process are involved and found less quality of cypher text. In this paper we suggest some of the changes over the traditional architecture of the DNA encryption algorithm. To find the solution of the identified problem we propose the following solution and a new architecture for generating the cypher text from the original text.

1. ***Plain text*:** that is a simple user input or the text message that is required to evaluate and encrypt.
2. ***Intermediate format conversion*:** here the complete string is divided into 256 lengths of strings and this string is converted into the binary strings.
3. ***XOR operation*:** each slice of the original binary string is produces into XOR operation this process is repeated till the entire message converted into 256 size block.
4. ***Password:*** a user password is required to convert the complete code into new format suppose a user enters a password “admin” then a dynamic encoding table is created that help to encode the massage. As given in table 1.

A	00
D	01
M	10
I	11
N	000

Table 1 encoding table

5. ***Remark*:** some time any password string may contain the same characters then the duplicate characters are removed which is found in last. Like user provide the password “Administrator”. Here “a” repeats 2 times “t” repeats 2 times then we drop the last found characters. We generate this table 2 as.

A	00
D	01
M	10
I	11
N	000
S	100
T	101
R	110
O	111

Table 2 complex encoding

The encoded message is forwarded into encrypted using this encryption the encryption process taken place. After that cypher text required to reduce more. That purpose we use compression algorithm for compress the complete cypher text now the cypher is ready to send at user end.

IV. Conclusions

The proposed security architecture is an enhance hybrid security architecture which is designed through DNA based cryptographic approach and an authentication server implementation. The given security architecture follows the OTP (one time password scheme) for authenticating the users and for data storage and transmission secure DNA cryptographic scheme is works. Therefore the security scheme following client server mutual authentication scheme for security improvement, and can adoptable for banking system, high secure data transfer and mobile computation too. In near future the proposed technique is implemented using the JAVA technology and their performance is published.

References

[1] Nidhi Khurana, Dr. Rattan Datta, Logical Data Model For Cloud Computing, Volume 3, Issue 4, April 2013 ISSN: 2277 128XInternational Journal of Advanced Research inComputer Science and Software Engineering.

[2] Introduction to Cloud Computing, White Paper,Dialogic, 2013.

[3] Nariman Mirzaei,CloudComputing,Fall 2008,Community Grids Lab, Indiana University Pervasive Technology Institute.

[4] Mike Ricciuti, “Stallman: Cloud computing is 'stupidity'”, http://news.cnet.com/8301-1001_3-10054253-92.html.

[5] Cong Wang and Kui Ren,Wenjing Lou,Jin Li, Toward Publicly Auditable Secure Cloud Data Storage Services, IEEE Network July/August 2010,0890-8044/10/$25.00 © 2010 IEEE.

[6] John Harauz,Lori M. Kaufman,BrucePotter,Data Security in the World of Cloud Computing, JULY/AUGUST

200915407993/09/$26.00 ©2009IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES.

[7] Balachandra Reddy Kandukuri, Rama Krishna Paturi V, Dr. Atanu Rakshit, Cloud Security Issues, 2009 IEEE International Conference on Services Computing, 978-0-7695-3811-2/09 $26.00 © 2009 IEEE, DOI 10.1109/SCC.2009.84, 517, 2.

[8] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing securityarchitecture, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 3, No. 10, 2012.

[9] YounisA.Younis,MadjidMerabtiandKashifKifayat,Secure Cloud Computing for CriticalInfrastructure:ASurvey, ISBN: 978-1-902560-27-4 © 2013 PGNet.

[10] Adhu Chauhan, Riidhei Malhotra, Muku Pathak and Uday Pratap Singh, DIFFERENT ASPECTS OF CLOUD SECURITY,Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com, Vol. 2, Issue 2, Mar-Apr 2012, pp.864-869.