International Journal of Recent Research and Review, Vol.VII, Issue 1, March 2014
ISSN 2277 – 8322

A Survey on Digital Archive as a Limitation in Cloud Computing

Vidhi Agarwal[1], Ms. Pooja Sharma[2]
M.Tech Scholar (Software Engineering), Poornima College of Engineering, Jaipur, India
Assistant Professor, Poornima Institute of Engineering, Jaipur, India
Email: [1]vidhiagarwal31@gmail.com

***Abstract*— Cloud is a virtualized server pool which can provide the different computing resources of their user's. In cloud computing, the data will be stored in storage provided by CSP (Cloud service Provider). Service providers must have a feasible way to protect their user's data, especially to prevent the data from disclosure by Malicious Insiders. This paper also illustrated the data privacy problem in cloud computing environment.**

***Keywords*— Encryption, Attacks, Security Issues, CRM.**

I. INTRODUCTION

In cloud computing, the data will be stored in storage provided by CSP (Cloud service Provider). Service providers must have a feasible way to protect their user's data, especially to prevent the data from disclosure by Malicious Insiders. Storing the data in encrypted form is a popular and common method of protecting user's data. If a cloud system is responsible for storage and encryption/decryption of data, then Malicious Insiders may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to user's data. This paper aims to provide a solution for cloud computing based on the concept of separating the encryption and decryption service from the storage service.

Furthermore, the Server responsible for the data storage must not store data in plaintext, and the Server responsible for data encryption and decryption must delete all data after the computation of encryption or decryption tasks.

A CRM (Customer Relationship Management) service is described in this project as an example to illustrate the Security Solution, Which deals with a unique ID among all the servers.

II. LITERATURE SURVEY

Security in cloud is one of the major areas of research. The Literature survey shows that, the researchers are trying to propose some efficient algorithms and encryption techniques to enhance the security in cloud data .But still they are not success in providing the real means of security for cloud users.

A. Rocha et al. showing a set of attacks

Rocha et al. [1] research works are showing a set of attacks that demonstrate how a malicious insider can easily obtain passwords, cryptographic keys, files and other confidential data. Also they discuss about some security mechanism and their limitations. Cryptography may be seen at first sight as the solution for data confidentiality in the cloud. For instance, a payroll processing application cannot process payrolls if all data is encrypted.

B. D.Kesavaraja et al. discuss about Session Controller Architecture

D.Kesavaraja *et al.* [2] implement a Cloud Data Server with Session Controller Architecture using Redundancy and Disconnected Data Access Mechanism. In their project, they generate the hash code usingMD5 algorithm. With the help of which they can circumvent the attacks, which are undefined by traditional Systems. In their proposed approach an activity analyzer takes care of intimating the administrator about possible intrusions and the counter measures required to tackle them. The efficiency ratio of their approach is 98.21% compared with similar approaches. But the main concern in

MD5 is Performance Limitation, due to which this is not much popular.

C. *N. Saravanan et. al implemented RSA*

N. Saravanan *et al.* [3], have proposed a method of providing security by implementing RSA algorithm using cloud SQL to the data that will be stored in the third party area. In there work, they implement RSA algorithm before storing the sensitive data in cloud. When the authorized user request the data for usage then data decrypted and provided to the user. Also they argued that the importance of security and privacy of stored data in cloud .But Breaking RSA, is not so hard just a factor the modulus into primes and derive the keys.This is dramatically simpler to do.

D. *Zhiyi Fang et al. designed and implemented AES Algorithm*

Zhiyi Fang *et al.* [4] has been designed and implemented Cloud storage system where they are using AES encryption algorithm, just as the security mechanism of users' files uploading and downloading .In their Designed Architecture When you register at the platform, you will get AppKey and AppSecret then you will receive an authentication named token, finally, authorization is done. These systems make a simple encapsulation to the platform interface, and provide a test of PHP SDK. Proposed Architecture is not secure against Malicious Insiders.

E. *Salvatore J. Stolfo et. al proposed Fog Computing*

Salvatore J. Stolfo *et al.* [5] have proposed a different approach for securing data in the cloud using offensive decoy technology. In that they are monitoring data access patterns by profiling user behavior to determine the authenticate and unauthenticated user,& Decoy documents which stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. But this is a heavy process, delay time is more in exchanging the information, so if an authorized user will request, he/she has to wait for a long time. Upto the verification phase. So, Not very much Succeed.

F. *Tim Gu¨neysu et al. used Cost-Optimized Parallel Code Breaker*

Tim Gu¨neysu *et al.* [6] used Cost-Optimized Parallel Code Breaker (COPACOBANA) machine, which is a low-cost cluster consisting of 120 field-programmable gate arrays (FPGAs) and high performer, which is used for Cryptanalysis of ciphers. Generally it involves massive computations. In addition, they introduce efficient implementations of more complex cryptanalysis on asymmetric cryptosystems, e.g., Elliptic Curve Cryptosystems (ECCs) and number co -factorization for RSA. In their work, as we mention they presented novel implementations for cryptanalytical applications on COPACOBANA.Also declared that DES can be broken within less than a week at an average throughput of 65.3 billion searched keys per second. And finally, they proposed a massively parallel implementation of the *Enterprise Content Management* (ECM) for factoring mid-sized integers typically obtained from the GNFS for RSA factorization. Main Drawback is Computational speed which proportionally related to delay time.

G. *G.Devi et. al proposed LMS (Learning Management System)*

G.Devi et al. [7] proposed LMS (Learning Management System) service which described in their project using Blowfish algorithm. It promotes more accessibility to LMS service providers to send their training modules and syllabus via Internet at any point of the hour much more efficiently. This gives rise to reduced cost of hardware and software tools, which in return would scale-up the e-learning environment. In the existing system RSA algorithm used. It requires more computation time for large volumes of data. To reduce this computation time we are using Blowfish algorithm. The LMS Service utilizes three cloud systems, including an encryption and decryption system, a storage system, and LMS application system. BF Algo.

H. Dr.A.Padmapriya et. al shows comparative study of several algorithms

Dr.A.Padmapriya *et al.* [8] discussed about cloud computing security mechanisms and presented the comparative study of several algorithms. They analyzed the importance of security [9] to cloud. Actually they compared three algorithms namely Data Encryption [10] Standard (DES), RSA, Homomorphic encryption for data security in cloud based on four characters; key used scalability, security applied to, and authentication type. DES algo is considered as an Insecure: A $10,000 Copacobana machine can find a DES key in an average of a week, as (probably) could a botnet with thousands of machines. RSA, is not so hard just a matter of factors the modulus into primes and derive the keys. This is dramatically simpler to do.

TABLE 1.1

Analyses of Different Approaches Suggested by Different Authors.

Period	**Approach**	**Suggested By**	**Security / Comments**
2008	Cost-Optimized Parallel Code Breaker	TimGu¨neysu et al.	Computational speed
2009	Demonstrate the Comparison of Encryption Algo.	D. S. Abdul. et. al	Performance Evaluation
2010	Used Discretion Algo. with IDS System	Jayalatchumy D et. al	Preserving the Data
2010	CDS with Session Controller Architecture	D.Kesavaraja et. al	Continual & Safe Service for the User
2011	FullyHomomorphic Encryption	Francisco Rocha et. al	Confidentiality of Data
2011	Discuss Challenges In the Cloud	Akhil Behl	No silver bullet to counter the threats
2012	Authentication Mechanism & Access Control Ploicy	Wentao Liu et. al	Data Privacy Issue
2012	RSA & MD5 Algo.	Ashutosh Kumar Dubey et. al	RSA Public Key Algo.
2012	Tool for Cloud file integrity Establishment & Monitoring	Sanchika Gupta et. al	Prototype Implementation
2012	Implemented RSA Algo.	N. Saravanan et. Al	Privacy of Stored Data
2012	Fog Computing	Salvatore J. Stolfo et. al	Monitor Data Aaccess in the cloud
2012	Proposed LMS (Learning Management System)	G.Devi et. al	Scale-up the E-Learning Environment
2013	Implemented AES Algo.	Zhiyi Fang et al.	Malicious Insiders
2013	Comparative Study of Several Algorithms	Dr.A.Padmapriya et. al	Importance of Security in the Cloud
2013	Broker Cloud Computing Paradigm	Amanpreet Kaur et. al	Unlimited Resource Provisioning

III. SECURITY ISSUES IN CLOUD COMPUTING

There are number of security of issues [11] which are related to Cloud Computing which scares the cloud customers to opt it for their business purposes and many more. Each issue is explained and accompanied on potential or real world measured impacts:

(1) User Access Rights: Cloud customer must have the knowledge about the people who are managing and assuring the integrity of the data [12] because of all the services are provided by third party which takes control over the physical, logical and personnel and makes it little bit risky.

(2) Data Location Constraints: When use the cloud, user is not known to the location [13] where the user data is hosted. User must ask providers that can they store and process data in specific jurisdictions and whether they can make an agreement to follow privacy requirements.

(3) Assurance of better encryption techniques: The cloud provider should confirm that encryption schemes [14] are designed and tested by experienced testers. It should be assured that encryption accidents will not make data unusable or more encryption will not affect data availability.

(4) Data availability: Ideally, cloud computing provider will never go broke or overtaken by a larger company [15]. But if this happen then our data that it will remain available even after such an event.

IV. CONCLUSION

The clients must make sure that the cloud in which they are planning to upload the data is safe from all the external threats and there must be a mutual understanding between the client and the cloud providers when it's the matter of security on Cloud. This paper, explored the importance of the cloud computing; but still there are a number of risks associated with the cloud computing process and procedure. This paper will provide a base for future research work in the field of data security of cloud computing system.

V. REFERENCES

[1] Rocha *et al.* , "Lucy in the sky without diamonds: Stealing confidential data in the Cloud",Published In 2011 IEEE/IFIP 41st International Conference.

[2] D.Kesavaraja& D.Sasireka (2010), "Implementation of a Cloud Data Server (CDS)for providing Secure Service In E-Business", IJDMS,Vo. 2,No.2

[3] N.Saravanan, A.Mahendiran, N.Subramanian &N. Sairam (2012), Maxwell Scientific Organization 4(19) "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL".

[4] Zhiyi Fang& Yao Sun(2013), "The Research of AES algorithm and application in cloud storage system",ICSSR, Published by Atlantis Press

[5] Salvatore J. Stolfo et. al , "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud" (2012)IEEE Computer Scoiety.

[6] Tim Guneysu, Timo Kasper, Martin Novotny (2008)," Cryptanalysis with COPACOBANA",VOL. 57, NO. 11, Published by the IEEE Computer Society.

[7] G.Devi, M.Pramod Kumar(2012) "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm",IJCTT vo.3Iss.4

[8] Dr.A.Padmapriya&P.Subhasri(2013) "Cloud Computing: Security Challenges & Encryption Practices",IJARCSSE Vo. 3, Iss. 3.

[9] Neeraj Shrivastava and Rahul Yadav, (2013), "A Review of Cloud Computing Security Issues", IJEIT, Vo. 3, Iss. 1

[10] Rachna Arora, Anshu Parashar (2013) "Secure User Data in Cloud Computing Using Encryption Algorithms",IJERA,Vol. 3, Issue 4.

[11] Leena Khanna & Prof.Anant Jaiswal (2013), "Security IssuesAnd Description Of Encryption Based Algorithms To Overcome Them", IJARCSSE Vo.3.

[12] Djamal Benslimane & Schahram Dustdar(2008), "Services Mashups ::The New Generation of Web Applications", Published By IEEE, P.1089-7801

[13] Mooga Masthan & Dora Babu Sudarsa(2013) " A Secure Cloud Computing Model Based on Multi Cloud",IJARCSSE, Vo. 3, Iss. 5,P.1424

[14] Jing-Jang Hwang and Hung-Kai Chuang (2012) "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service",IEEE.

[15] Nilesh N. Kumbhar & Mohit A.Badhe (2012), "The Comprehensive Approach for Data Security in Cloud Computing: A Survey",IJCA, Vo. 39– No.18