A Review: Different Challenges in Energy- Efficient Cloud Security

Poonam Kumari¹, Meeta Singh²
Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India

E-mail: pnmdv211@gmail.com¹, meeta.sangwan@gmail.com²

Abstract. Cloud Computing is the hottest research area today because of its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing is Internet based computing because it provides on demand dynamically to consumers by sharing resources and providing information to the software. Cloud Computing is one of the fastest growing technology IT trade for business. Cloud computing security has become a major cause of hindrance in its development. Cloud computing security is set of policies, procedure, controls, roles, permissions and technologies that work together to protect cloud based system and data. Cloud computing security has become a latest topic in academic research and industry because Cloud users have to save their data in the cloud so lack of security in the cloud can loss the user’s trust. This paper discusses review of security in cloud computing. The study is based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) and the deployment model (Private, Public, Hybrid, and community cloud).

Keywords: Cloud computing, Cloud Services, Cloud security, Genetic algorithm, Two Factor algorithm.

1. Introduction

Cloud computing is a network solution for providing inexpensive, reliable, easy and simple access to IT resources. Cloud computing is service oriented but not application oriented [1]. In cloud, the user can access the cloud resources, application and cloud data at anywhere and anytime without concerned about maintenance, technical and physical management issues of the original resources [2]. Cloud computing is on demand accessibility of computer resources, data storage, computing power without direct management by the user. Cloud Computing is one of the fastest growing technology IT trade for business which will provides on premises datacenter. Organizations have to manage everything, for example purchasing virtualization, installing the operating system and installing hardware and other applications and setting up storage for data with on premises.

Cloud computing security is very important topic in academic research and industry. It is very important for the cloud service to ensure the data integrity, privacy and protection. Cloud security is very much important as this will provide the trust and confidence to the user to transmit & store their data on the cloud.

In cloud security, the data or information is very important for client on the cloud platform but the hacker pays more attention to hack that data due to cloud system must be protected more carefully than tradition method [3][16]. Today, cloud computing security is major issue because our data or information stored on the cloud than arises the security issue or questions that how the data or information is secure or when data is too sensitive to be stored on public cloud. For example, national security data or highly recommended data or future product details etc. than this type of information can be extremely sensitive and the consequences of exposing information on public cloud can be serious. In such cases highly sensitive data store on private cloud for privacy of data or secure the data [1][18]. In cloud computing, Figure 1 discusses about the architecture of cloud computing including cloud services, cloud deployment model and characteristics of cloud [4][17].
(where SaaS: Software as a Services, Paas: Platform as a Services & IaaS: Infrastructure as a Services) Cloud computing can also discusses about the grid computing, virtualization, distributed computing, network computing etc. and some characteristics of cloud computing which is shown in figure 1.

- On demand self service
- Network access
- Rapid Elasticity
- Resource Pooling
- Pay per use

Cloud deployment models are mainly four type: public, private, community and hybrid clouds. A cloud computing that is accessible for multi-tenants and is accessible to the public is called a public cloud. A private cloud is available for a particular organization or within institutions and community cloud is available for a specific organization of customers or employees. Hybrid cloud is a combination of two or more clouds private and public or (public and community) and vice versa (private, community, or public cloud) [5].

2. Attributes of Cloud Computing

In cloud computing, there are certain attributes that service has to provide before it can accurately be called cloud service. Few attribute of cloud computing are discussed below:
Multi-tenancy (Shared resources)

Cloud computing is based on a business model and academic model in which resources are shared network level, host level and application level.

Massive scalability

Cloud computing provides the ability to scale to tens of thousands of system, as well as the ability massively scale bandwidth and storage space.

Elasticity

Users can rapidly increase and decrease their computing resources as needed.

Pay as you used

Users to pay for only the resources they actually use and for only the time they require them.

Self-provisioning of resources

User’s self-provision resource, i.e. additional system and network recourse.

3. Cloud computing models

Following are the different type of cloud computing service model:

Infrastructure-as-a-Service

In Infrastructure – as - a service, it is provide storage, rent processing system, models, hardware, servers and components networking tool etc. used to support an organization. In this services, users allow to run any application on cloud network of their own choice. It is provide environment and tools for creating new online application. For example- Google App Engine, Amazon Web Services etc. [6].

Platform-As-A-Service

Platform-as-a-service (PaaS) is a way to take the resources on the Internet hardware, storage, operating systems and network capacity. It offers runtime environment for the application. Lower cost: Customer does not need to purchases hardware and software. Scalability: resources can be scale increase and decrease easily. Operating system features can be upgraded and change to a geographically distributed development team. It is basically provide platform to develop application [6].

Software-As-A-Service:

Software-as-a-service (SaaS) provider is an application for customers on-demand, a subscription, a pay-as-you-go model, application for delivery. In this approach all of the utility computing where technology “cloud” as a service accessed over the Internet starting in model widely. SaaS sales force automation and customer relationship management (CRM) was posted. Now it is common to many business application, CRM application, Help Desk, human resource management application, financial, content management, including computerized billing, document management and service desk management [6].
4. Literature View

In order to understand the basics of cloud computing and storing data securely on the cloud, several resources have been consulted. This section provides a review of literature to set a foundation of discussing various data security aspects.

- Ahmed Albugmi et al., (2016). In this paper, they have discussed two states of data normally having threat to its security in clouds: Data at Rest and Data in Transit. Data at rest means data is stored on cloud and data in transit means data in processing. Authors also explain the security algorithm in cloud computing with the help of cryptographic algorithms. In cryptographic algorithms, authors explain stream cipher algorithm, block cipher algorithm, and hash function for the privacy of data in cloud computing. This paper provides the study about risk and security concerns in cloud computing and also discussed about the challenges of cloud security [1].

- Jaydip Kumar has provided a standard algorithm to overcome the security issues in cloud computing and have discussed security techniques for secure cloud like Authentication and identity, encryption, integrity checking, access control, secure detection, and data masking. In cloud computing, data are growing exponentially but security of data is a challenge today because of the security problem occurs and data owner loses their data. Authors explain cloud challenges include unauthorized access, leaks of sensitive information of users and data leakage. This paper explains how to resolve data security problems with the help of genetic algorithm, k mean algorithm and KNN algorithm. In K-mean algorithm, the easiest algorithm of partitioning method for clustering analysis. The aim of k mean algorithm is to minimize an objective function [7].

- Mr. Sagar D. Rushi et al., (2014). There have proposed basic of cloud computing and also discuss the related work of security in cloud computing. In this paper, talk about the AES Algorithm and discuss about the architecture of cloud computing. AES algorithm can be used to resolve the security issue and uses the encryption and decryption of the keys [4].

- ShaluMall and Sushil Kumar Saroj (2018). There have proposed the genetic algorithm and representation of proposed communication (discuss three schemes: data owner, cloud service provider and many user associated with owner and explain how to communicate all three schemes). In this paper, the best explanation of genetic algorithm with the help of crossover, mutation, GA operations with smaller block size and Capability list [8].
- Adnaan Arbaaz Ahmed and Dr. M.I. Thariq Hussan (2018). They have discussed all services and deployment model of Cloud Computing. In this paper, authors have the best explanation of Security Issues and Research Challenges. Multi-tenancy is the biggest problem for security today, but authors have not given the best solution. Multi-tenancy means multiple users work on the same cloud, same hardware, and same operating system and same data storage system to share information and run on a single server [9].

- Harmeet Kaur (2013). In this paper, they discuss two-factor authentications using graphical password with passpoint scheme and comparison of data security in grid and cloud computing. In this paper, they explain the authorization and authentication with the user ID and password and use password image format when the password is forgotten or reset than data owner authenticates the user and the user resets the password (with the help of images) [10].

5. Representation of communication methods on cloud

In figure 3, discuss the three entities data owner, cloud services provider, and many users. First of all, every user is registered at the data owner, and users send their requirement information to the data owner. It was assumed that the user successfully sends the requirement to the data owner during registration than the data owner required information to the user safely in response.

Data owner is store the data to cloud service provider. After successfully authentication of the user to cloud service provider then the user can retrieve or store the data from cloud service provider with the help of secret key (secret manner). Presuppose that cloud services provider knows what are the mechanisms used to store and locate the data on cloud. Cloud service provider is a big organization to use such type of algorithm [8].

6. Existing algorithms

These algorithms already exist in cloud computing environment and play an important role for security purposes of cloud. These methods are based on genetic algorithm, two-factor algorithm using graphical method and cryptography techniques use in cloud security. Use the security mechanism for data is store, access and locates on cloud.
In this security mechanism, data is converted into ASCII values and these ASCII values are converted into binary bits and binary bits also divided into blocks and block size may be 8 bits, 4 bits, 2 bits etc. Following are the algorithms used for encryption and decryption process on cloud:

*Genetic Algorithm:*

Genetic algorithm [11] is collection of three processes. In this paper, genetic operations and pseudorandom number are used in encryption and decryption process of data.

*Crossover*

It is the process in which two blocks are taken to generate a new code. There are mainly three crossover operations.

*One - point crossover*

In one-point crossover, the two blocks (B1 and B2) are given randomly and two blocks are chosen. These blocks are broken into half then tails of two blocks is exchanged to obtain new code (C1, C2).

\[
\begin{align*}
B1 & \quad 10011111 \quad 10011001 \quad C1 \\
B2 & \quad 10001001 \quad 10001111 \quad C2
\end{align*}
\]

*Two-point or Multi-point crossover*

In two point crossover, the two cut points are created instead of one then one part of every block is exchanged to form a new block.

\[
\begin{align*}
B1 & \quad 10010010 \quad 10010110 \quad C \\
B2 & \quad 01111000 \quad 01110000 \quad C2
\end{align*}
\]

*Uniform crossover*

In uniform crossover, the bits are copied randomly from the 1\textsuperscript{st} and 2\textsuperscript{nd} point. In this crossover, random mask are generated and the mask determine which bit is copied from 1\textsuperscript{st} point and from 2\textsuperscript{nd} point.

\[
\begin{align*}
B1 & \quad 00011010 \quad 00110011 \quad C1 \\
B2 & \quad 10001000 \quad 10100001 \quad C2
\end{align*}
\]

*Mutation*

In mutation, mutation is based on random changes and its changes 0 to 1 and 1 to 0. It is performed on two selected blocks.

\[
\begin{align*}
B1 & \quad 10001100 \quad 10001000 \quad C1 \\
B2 & \quad 11111110 \quad 11011100 \quad C2
\end{align*}
\]
7. Two Factor Authentication:

In two factor authentication, use the password for authentication and protection services against unwanted access to resources and new graphical scheme can be proposed. Two factor authentication enable users to secure their login and password in cloud computing. Firstly, users login their username and password then authentication succeeds then we enter the secondary authentication they are offered a choice of authentication method. It allows the user to authenticate with what method is use such as pin code, ID card and smart card etc. Then user login securely [12].

![Two factor authentication working](image)

**Fig. 4 Two factor authentication working**

*Recognition Technique and Recall Technique*

It is graphical password based technique. Recognition and recall technique can be used. In recognition technique, it is a set of images to represented user from the cloud provider and the user is recognized and identified the image that he selected during the registration. In recall technique, user is created or selected earlier during the registration stage [13]

**Pass Point Scheme:**

I used the recall based technique. In this technique, user is created or selected earlier during the registration stage. This technique provides many types of authentication schemes such as Pass Point Scheme and Grid Selection Scheme etc. I take the pass point scheme for our authentication and which is used with two factor authentication. In pass point scheme, user click on an image to create a password [13].

Pass point is based on the number of pixels of a picture. In this technique, the numbers of pixels are calculated and combination of pixel create image that image is password.

8. Techniques to secure data on cloud

*Information integrity and Privacy*

Cloud computing gives the information and resources to valid users. Resources can be accessed through web browsers and by malicious attackers [14]. First solution information integrity is to provide mutual trust between provider and user. Another solution can be provides proper authentication, authorization and account controls for accessing information [14].

*Multi-tenancy*

A cloud model is built for like sharing of resources, memory and storage, shared computing [14]. Multi-tenancy gives the best efficient utilization of resources and low cost. It is implies sharing of resources, application and service storage with other resources on same physical or logical platform at cloud provider’s premises.
**Authentication and Identity**

Authentication and identity is very important in cloud security. Authentication of users and communicating systems is performed by various methods, but cryptography is mainly use (most common) [15]. Authentication of users use in various method like passwords that is known individually and in the form of a security token but create the one problem with using traditional identity approaches are faced in a cloud computing, whenever the organization uses multiple cloud service provider (CSP)[15]. Synchronizing identity information with the organization is not scalable.

**Data Encryption**

For storing sensitive information and large data store on the cloud then data encryption techniques then passwords following with the firewalls are better options for making the cloud more secure. When data is encrypted that cannot be read data without an encryption key. So the data is totally useless. It is a technique of translation of data into secret code with the help of secret keys. For reading the encrypted data, a secret key that is called encryption key [16] is required.

9. Comparative analysis

Following are the comparative analysis carried out in this paper and include different type of algorithm to provide complete cloud security:

| Related Area Under Review | Mechanism used | Implementation | Suitability for usage through findings | Reference |
|----------------------------|----------------|-----------------|---------------------------------------|-----------|
| Data security in cloud computing | Cryptographic Process | Possible | Encryption techniques for data at rest and data in transit can be different. | Ahmed Albugmi etal. [1] |
| Cloud Computing Security Issues and its Challenges | Genetic algorithm and K – mean algorithm | Not sufficient | Algorithm design for securing data on cloud. | Jaydip Kumar [2] |
| Data Security Issues in Cloud Computing | AES Algorithm | Not Sufficient | AES performs both software and hardware platform under wide range of environments. | Mr. Sagar D. Rushiet al. [4] |
| A New Security Framework for Cloud Data | Genetic algorithm | Possible | Genetic operations and pseudorandom number are used in encryption process of data | ShaluMall and Sushil Kumar Saroj[8] |
Cloud Security Issues and Challenges

| Multi-tenancy | Not sufficient | Only explain the security issues and challenges. | Adnaan Arbaaz Ahmed and Dr. M.I. Thariq Hussan [9] |
|---------------|----------------|-------------------------------------------------|--------------------------------------------------|

Comparison of data security in grid and cloud computing

| Two factor authentication using graphic password | Possible | Use of graphical password we secure the data is more suitable And focus how to use authentication between grid computing and cloud computing. | Harmeet Kaur [10] |

Conclusion

Conclusion is based on the finding analysis that is carried out in the paper which includes different type of algorithm to provide comprehensive cloud security. According to the method prescribed, it is clear that with the findings that security problem in the cloud computing can be achieved with the help cryptographic and genetic algorithms. It is apparently clear that these method will exhibits better results in terms of access and authentication of the data under multi provider environment as compared to other algorithm.

Future prospective is to propose and implement the best algorithm and find out the better result of cloud security which will emphasis on how the data is secure on cloud and any unauthorized person cannot access anyone else data.

References:

[1] Albugmi Ahmed, Alassafi Madini.O, Walters Robert, Wills Gary Data security in cloud computing Conference Paper DOI: 10.1109/FGCT.2016.7605062 (2016) 55-59.

[2] Gaikar Pratik, Agrawal Tanmay, Shirwadkar Ashay and Mukhopadhyay Debajyoti Securing the Data in Clouds with Hyperelliptic Curve Cryptography (2014) 201-205.

[3] Descher D, M., Masser, P., Feilhauer, T., Tjoa, A.M. Retaining data control to the client Conference on Cloud Computing IEEE (2009) 109-116.

[4] Mr. Sagar, D. Rushi, Makwana Prof. Pragan, Shekokar Prof. Kishori Total Survey of Data Security Issues in Cloud Computing International Journal of Engineering Sciences and Research Technology (2014) 5-7.

[5] H. Takabi, Joshi J. B. D. and G. Ahn Security and Privacy Challenges in Cloud Computing Environments, Security & Privacy IEEE (2010) 24-31.

[6] Mr. Omar Abd Al-kader Kalaf Security in cloud computing international Journal of Engineering Research and General Science 2 (2014) 495-504.

[7] Kumar Jaydip Cloud Computing Security Issues and Its Challenges: A Comprehensive Research International Journal of Recent Technology and Engineering (IJRTE), 8, (2019) 10-15.

[8] Shalu Mall, Sushil Kumar Saroj A New Security Framework for Cloud Data 8th International Conference on Advances in Computing and Communication Procedia Computer Science 143 (2018) 765–775.
[9] Ahmed Adnaan Arbaaz, Hussan Dr.M.I.Thariq Cloud Computing: Study of Security Issues and Research Challenges International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 7 (2018) 362-369.

[10] Kaur Harmeet Comparison of data security in grid and cloud computing International Journal of Research in Engineering and Technology 02 (2013) 135-145.

[11] Mehta P Srikanth, Abhinav, Yadav Neha, Singh Sahil and Singhal Shubham Encryption and Decryption Using Genetic Algorithm Operations and Pseudorandom Number IJCSN - International Journal of Computer Science and Network 6(3) (2017) 455-459.

[12] https://www.duosecurity.com/product

[13] M.Bhargav Graphical password Authentication /www.slideshare.net/akhilrocker 143/558-11294069

[14] Behl Akhil & Behl Kanika an Analysis of Cloud Computing Security Issues World Congresson Information and Communication Technologies (WICT) IEEE (2012) DOI:10.1109/WICT.2012.6409059.

[15] Adeja Yashpalsinh & Modi kirti cloud computing- concepts, architecture and challenges International Conference on Computing, Electronics and Electrical Technologies [ICCEET] (2018) 887-880.

[16] Singh M., Nandal P., Bura D. Comparative Analysis of Different Load Balancing Algorithm Using Cloud Analyst. In: Panda B., Sharma S., Roy N. (eds) Data Science and Analytics. REDSET 2017. Communications in Computer and Information Science 799 (2018). Springer, Singapore. https://doi.org/10.1007/978-981-10-8527-7_26

[17] Bura, D., Singh, M., & Nandal, P. Analysis and Development of Load Balancing Algorithms in Cloud Computing. International Journal of Information Technology and Web Engineering (IJITWE), 13(3), (2018) 35-53. doi:10.4018/IJITWE.2018070103

[18] Kamboj, N., Saggu, S., Lamba, A., & Singh, M. A Review: Analysis and Comparison of Different Detection Techniques of IDPS. Journal of Engineering and Applied Sciences 12(22) (2017) 5939-5943.