METHODS AND TECHNIQUES ASSOCIATED WITH SECURITY OF THE CLOUD

S.Anitha Rajathi, Assistant Professor, R.M.D. Engineering College,Chennai

Dr.J.Devagnanam, Associate Professor, Thiruthangal Nadar College, Chennai

anitharajathi91@gmail.com, jdevagnanam@gmail.com

Abstract: The most modern computing is cloud computing. Since the ability of providing all the resources including the infrastructure, from small to giant business people prefer the cloud computing to reduce the maintenance cost. They trust the cloud service provider that they receiving the quality service without any comprise in security aspect. So the cloud provider always aims for providing the quality service with recent technologies and algorithms used by standard industries. The researchers also turned their eyes from development to deployment .Because the cloud used by various group of people, the transaction needs more privacy and security. The security issues and solution may vary time to time, since the cloud and cloud computing use become inevitable in not only business but also in personal. This paper provides the various security issues in the contemporary market and suggests few solutions.

Key words: Cloud, Security, QoS, security techniques, DS, Encryption

Introduction:

Cloud computing is preferred by the industries because of its simple access. If anyone having the internet facility, can use the cloud service from the leading cloud providers (CP). The services of cloud is provided in three categories as follows:

A. PaaS

B. IaaS

C. SaaS

The above services given to the user based on the rental basis for the particular time. The services should be interrupted and reliable to the user for the whole period which is accepted by both cloud provider and cloud user. Brief information of each service make us to understand the cloud services and it’s important.

A. PaaS (Platform as a Service):

As the name suggests, Paas supplies the computing platforms which includes OS (operating system), web server, Database, Programming Developing environment,etc. Apache Stratos, Windows Azure, Google App Engine, AWS Elastic Beanstalk are well known real time examples for Platform as a Services.[1]

B. IaaS (Infrastructure as a Service):

IaaS (Infrastructure-as-a-service), also identified as cloud infrastructure services, in which Information Technology infrastructures (servers, storage and networking hardware, as well as the virtualization or hypervisor layer.) is given to cloud users via the internet. Google Compute Engine (GCE) Amazon Web Services (AWS) Elastic Compute Cloud (EC2), Microsoft Azure, and Rackspace are well examples for Infrastructure as a service.[1]

C. SaaS(Software as a Service):

SaaS (Software as a service) is a technique of sending applications via the Internet as a service. There is no need of installation and maintaining a software but simply you can access through the internet. It helps us to no concentration on complexity of the service and managing the hardware. Zoom, Google Applications (G Suite), Netflix, Salesforce are very good examples for Software as a service.[1]

The cloud provider need no longer manage the cloud infrastructure along with services, network and application. It reduces the need of maintenance of control and run all the resources. While enjoying the benefits of cloud computing, safety is always making people to afraid. Security and privacy are primary elements in cloud computing, it should be concentrated more to ensure the quality services of cloud computing.[2]

Literature Review

Transferring the information in the IOT while connected to cloud brought safety threats while layout and configuration of technology is improper[3].by using the stenography and cryptographic strategies, it offered the transformation of information without considering the nearby storage cloud users[4] because, cloud computing is dynamic generation. Cloud environment and client can use the services of the cloud without any issues since the cloud computing use the Security as a Service [5].In this paper encryption and decryption was discussed seriously by the author.

After increasing the usage of cloud after 2016, authors mentioned concerning cloud computing platform is utilized and planned to use web solicitations and proportion by means that of web such kind of technology designed exploitation OpenStack framework, hospitable multimodal enhancements associate degreed abusing fingerprints is an accurate biometric practise for user verification, the platform provide cozy get right of ticket to for quite one clients guarantees and provide whole logical detachment of knowledge resources and computation associated with specific enterprise[6] outlined topics associated with cloud protection, the security of knowledge storage on public cloud servers and authentication of logical user having access to the cloud. In cloud, multi-cloud storage is one in all the necessary downside. this can be accustomed save and obtain entry to cloud statistics distantly, and storage are skilled of encrypting and hold records in amazing cloud drives [7] planned model, that supply account account assault, privateness for one-of-a-kind documents uploaded through good customers, associated localised distribution of statistics storage the employment of an index based mostly cryptological information .

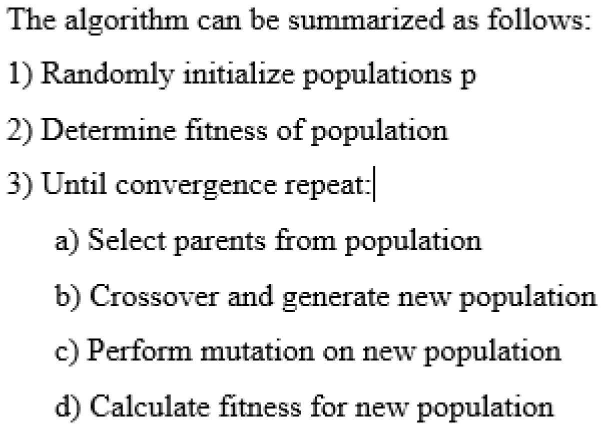
Cloud protection becomes the essential and important concern for researchers of the cloud. While cloud customers using new proposed safety architecture for cloud framework that offer great conversion and protects information from data leakage, unauthorized spots are also was grow up[8]. An impartial approach is necessary to ensure that cloud information is hosted effectively within the cloud server [9] mentioned unique security strategies for secure data stored on the cloud. Data owners and cloud servers have different identities, this framework offers records storage and feature unique security issues. In order to supply the required provider with the resource of a cloud character, cloud computing uses "Utility Computing" and "Software as-a-Service." Cloud protection is a significant and important fact, but it also has a number of issues and difficulties related to it [10]. Listed a number of factors that may have an impact on security and reveal security difficulties and problems encountered by customers and cloud service providers, including data privacy, security concerns, and infected software.

3. METHODS FOR SECURING DATA SET

A. Genetic Algorithm

Genetic Algorithm is a considering method used to find the near or specific resolution to optimization and problem [11]. It changes the huge domain problem to a model by using chromosome and the set of rules with a random choice of the population of chromosomes.

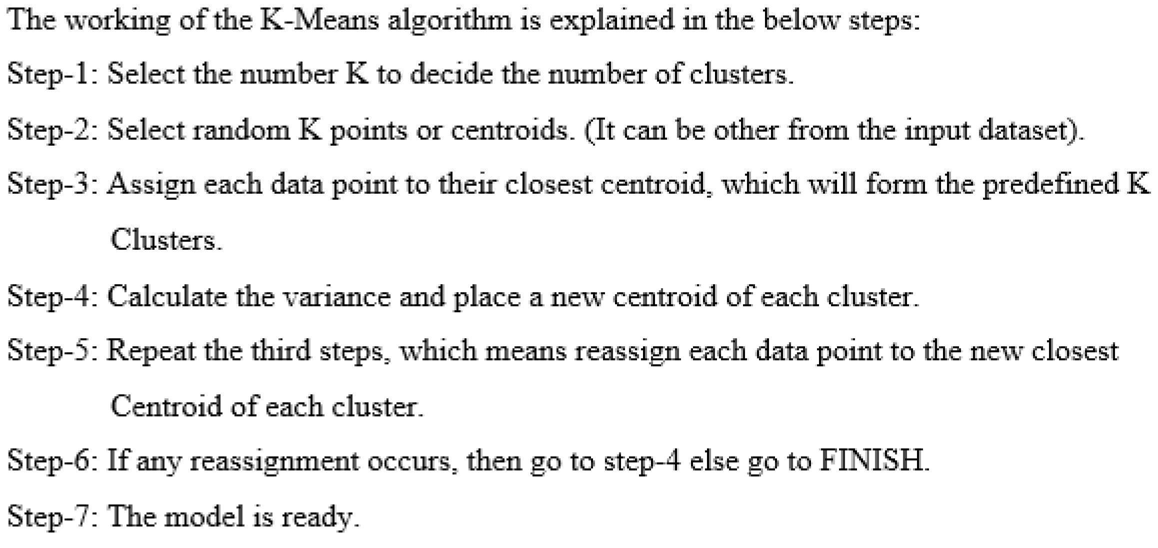
These are transformed into numbers or bits reliable with the problem [12]. Natural and subsequent guidelines are advanced thru Genetic Algorithm that ideas are employed for community site visitors that distinction between every day or spectacular web site guests.



```
The algorithm can be summarized as follows:
1) Randomly initialize populations p
2) Determine fitness of population
3) Until convergence repeat:
    a) Select parents from population
    b) Crossover and generate new population
    c) Perform mutation on new population
    d) Calculate fitness for new population
```

B. K-Mean Algorithm

K-propose is a suitable set of partitioning strategy suggestions for clustering evaluation [13]. This set of guidelines aims to minimise the square errors feature of a target function.



The working of the K-Means algorithm is explained in the below steps:

Step-1: Select the number K to decide the number of clusters.

Step-2: Select random K points or centroids. (It can be other from the input dataset).

Step-3: Assign each data point to their closest centroid, which will form the predefined K Clusters.

Step-4: Calculate the variance and place a new centroid of each cluster.

Step-5: Repeat the third steps, which means reassign each data point to the new closest Centroid of each cluster.

Step-6: If any reassignment occurs, then go to step-4 else go to FINISH.

Step-7: The model is ready.

4. Techniques for Cloud Security

Encryption of cloud data is not a solution for data that would maintain faith in cloud security. It can be done by applying modern security techniques including authentication and identity, encryption, integrity checking, access control, cosy detection, and data covering, which are all security techniques that apply to cloud data.

i) Authentication of OTP

In the current context, many banks offer authentication using the One Time Password (OTP) method. This method is utilised to authenticate the cloud user and is eventually used for one-time authentication known as device aspect authentication, as seen in figure 3. When used for two-factor authentication, it is sometimes known as a multiple authentication factor.

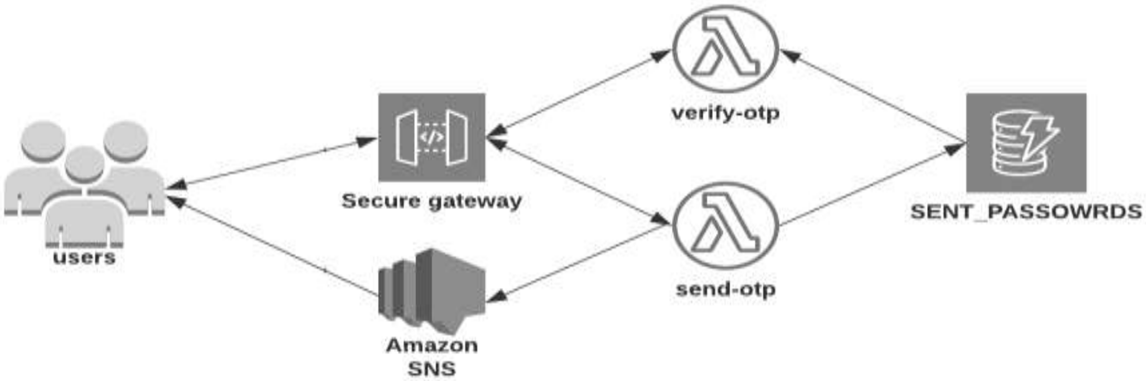


Fig.

ii) Checking Integrity

The security of cloud data ensures that only authorised users are able to view or modify cloud records. In plain English, it is a cloud-based system that completely verifies the accuracy and adherence to the fundamental principles of data integrity of the information. It is possible to ensure the accuracy of cloud data stored on a remote server using Provable Data Possession (PDP), and Proof of Retrievability (POR) can be used to find and confirm the evidence that the cloud data was stored by the individual and was not altered [14].

iii) Access Control

Due to access manipulate cloud statistics are excluded from amendment or unauthorised disclosure of records. Access manipulate cloud statistics owner can execute some restrictive permission to get proper of access to their facts outsourced to cloud and records owner's felony customer can access cloud facts at the same time as unauthorised customer can't.

iv) Secure Deletion

Understanding how the data is removed from the server is essential. Deletion makes use of innovative approaches like clearing. Using this method, we destroy the media before reusing them and simultaneously provide security for accepting the data that was previously stored in the media. Sanitation, in this location, the security for receiving historical statistics isn't always provided, and this type of information is frequently disseminated for lower degrees of kind [15].

v) Encryption

Cloud security offers data encryption services to encrypt cloud data before it is moved from local storage to the cloud. Encrypted data can only be accessed with a certified user's decryption key and is best possible to recognise from any machine, database, or report. Separating encrypted data from encryption keys is essential for maintaining the security of cloud data. The encryption and decryption system is explained in Figure 4 below.

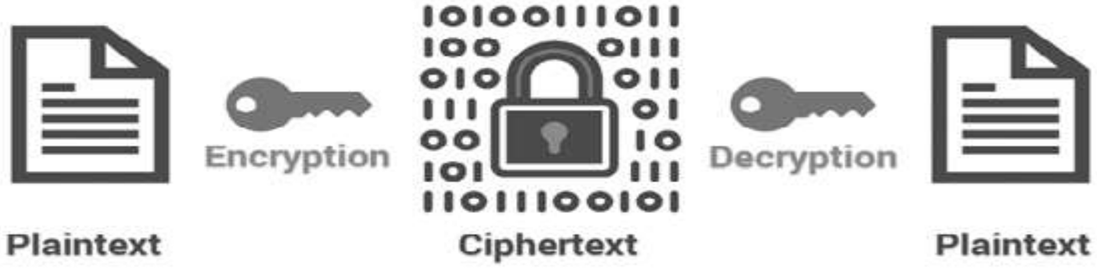


Fig.

vi) Data Masking

Data protection is a method of safeguarding and concealing cloud facts from attackers and theft. It also ensures that the records are replaced with plausible but false records. People frequently use the terms "data de-popularity," "data cleansing," and "data the time period defining the hard machine" interchangeably. Although data overlaying is a public knowledge set, it is not the most efficient collection of rules. Static Data Masking (SDM), which is utilised by the majority of enterprises when developing checks, is the only technique of protection that is viable even when using outsourced developers in a different site or business. There are excellent approaches or tactics for masking cloud data. It is crucial to duplicate the database in those circumstances. Depending on their position inside the company, Dynamic Data Masking (DDM) grants access [16].

vii) Intrusion Detection System[IDS]

An intrusion detection system (IDS) is a software programme or device that keeps an eye on device activity or community visitors and detects any illicit activity. In today's technology, the majority of hackers employ various assaulting techniques to find consumers' sensitive data. Any unauthorised access to or malicious use of IT resources is considered an incursion. The intruders look for unlawful access to sensitive information or dangerous behaviours. Host-Based Intrusion Detection System (HIDS) is connected to a specific system or server and displays illegal activity on that device. Network-Based

Intrusion Detection System (NIDS) is observed in a devices or computer connected section of a company's community and monitors network website traffic and keeps an eye on ongoing assaults.

5. Conclusion

According to the presentation above, there is a lot of scope for the development of new security techniques to protect the statistics set. The significance of each method has been briefly discussed, but only those that can be used to secure cloud records have been discussed in detail above after consulting extensive literature.

Reference

[1]. M. U. Bokhari, Q. M. Shallal and Y. K. Tamandani, "Cloud computing service models: A comparative study," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 890-895.

[2] Rajathi, S. Anitha, and J. Devagnanam. "Exploring and Understanding The Cloud Environment with Resource Allocation Techniques." *Journal of Science and Technology* 6 (2021): 7.

[3. A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework," Proc. Int. Conf. Internet things Cloud Comput. - ICC '16, pp. 1–5, 2016.

[4]. B. Pathankot, "Review Paper on Enhancing Data Security for Cloud Environment Cryptography and Steganography," International Journal of Engineering Applied Sciences and Technology, vol. 2, no. 1, pp. 44–48, 2016.

[5]. D. H. Sharma, C. A. Dhote, and M. M. Potey, "Intelligent Transparent Encryption-Decryption as Security-as-a-Service from clouds," 2016 Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. CSITSS 2016, pp. 359–362, 2016.

[6]. G. L. Masala, P Ruiu, E Grosso, "Biometric Authentication and Data Security in Cloud Computing," Comput. Netw. Secur. Essentials, pp. 337–353, 2017.

[7]. K. Subramanian and F. L. John, "Secure and Reliable Unstructured Data Sharing in Multi-Cloud Storage using the Hybrid Crypto System," IJCSNS, vol. 17, no. 6, pp. 196–206, 2017.

[8]. A. Hussain, C. Xu, and M. Ali, "Security of Cloud Storage System using Various Cryptographic Techniques," International Journal of Mathematics Trends and Technology (IJMTT), vol. 60, no. 1, pp. 45–51, 2018.

[9]. A. Venkatesh and M. S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," IJSRCSEIT, vol. 3, no. 1, pp. 1741–1745, 2018.

[10]. G. Jain and A. Jaiswal, "Security Issues and their Solution in Cloud Computing", Concepts journal of applied research(CJAR), vol. 02,no. 03, pp. 1-6, 2018.

[11]. Y. Guo and B.Wang et.al., "Feature Selection Based on Rough Set and Modified Genetic Algorithm for intrusion Detection" , The 5th International conference on Computer science & Education Hefei, China, pp. 1441-1446, 2018.

[12].T. Singh, S. Verma, V. Kulshrestha and S. Katiyar, "intrusion Detection System Using Genetic Algorithm for Cloud",International journal of Advances in Electronics and Computer Science, pp. 1-6, 2016

[13]. Data clustering algorithms[online] https://sites.google.com/site/dataclusteringalgorithms/k- means-clustering-algorithm (Accessed 08 March 2019).

[14]. S. Sharma, "Data Integrity Challenges in Cloud Computing", 4th international conference on recent innovations in science engineering and management, pp. 736-7436, 2016

[15]. CloudCodes[online] https://www.cloudcodes.com/blog/ data- protection-controls-techniques.html (Accessed 20 December 2019).

[16]. G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", International journal of engineering science and Technology, vol. 3, no. 6, pp. 5150-5159, 2011.