Cloud Computing Security Issues and Its Challenges: A Comprehensive Research

Jaydip Kumar

***Abstract:** Cloud computing is used by many of the organizations for storing the huge amount of data on the clouds. Therefore, there is need to secure the data which may in the form of text, audio, video, etc. There are numerous algorithms designed by the researchers for securing the data on the cloud. The present paper by Jaydip Kumar is an attempt to elaborate some of the important algorithms for the security of data for this purpose, exhaustive literature has been conducted.*

***Index Terms:** Cloud Security, Genetic Algorithm, Data Encryption, Intrusion Detection System, Security Techniques.*

I. INTRODUCTION

The term “Cloud computing” has defined by National Institute of Standards and Technology (NIST) is comprehensive and rising technology in the daily life for every one provides on demand web services like networks, storage, servers and applications with flexibility and cost efficiency for users. Cloud computing is a technology that increase or reduce the storage capacity as peruse without investment in new infrastructure. The process of cloud storage contains four layers newly storage layer that store data on cloud data center, management layer which ensures privacy and security of cloud storage, application interface layer that provide cloud application service platform, and finally cloud access layer which provide accessibility to the cloud user. The cloud models are classified with different services like Infrastructure as a Service (IaaS): is most prevalent and developed market segments of cloud that deliver customized infrastructure on demand, Platform as a Service(PaaS): that provides platform and environment to the developers that build cloud services and application on the web and that services are stored in the cloud and accessed by cloud users using web browser, Software as a Service (SaaS): that provides its own application running on a cloud infrastructure. The cloud user need not control or manage the cloud infrastructure including storage, operating system, services, network and application. It also reduces the need of computers, server, storage and manage and run all application. In cloud computing data are growing exponentially but security of data is still questionable. Due to the transfer of data to the cloud data center, the security problem occurs and data owner loss their control on data. Security and privacy for cloud data is a major aspect of cloud computing that is still not solved. These cloud security challenges include unauthorized access, data leakage and user’s sensitive information leaks.

II. REVIEW OF LITERATURE

Firstly considering the In the year 2011, authors presented a work related to cloud computing services like networks, storage, servers, services and applications without physically receipt them. As per observation in the paper it is found that overhead of the large system has been reduced of risk, data leakage etc [1]. cloud computing provide on-demand web services. If a company providing internet services need to invest large capital money for infrastructure and problems like machine failure, disk failure and software bugs etc. due to this cloud is best solution for those who does not want to setup infrastructure in own system. [2] According to this paper cloud user no need to invest money on infrastructure and pay as per services use.

In the year 2012, authors discussed about cloud security that data growing exponentially but security of an open-ended and rather easily accessible resources is still questionable and investigates risks of security from cloud computing environment, characteristics, cloud delivery model and the cloud stakeholder [4] . The authors brief discussed about cloud security. In these days more and more people are using clouds that have sensitive data and send, receive and store in network so that cloud network security has become major issues [5] in above work author discuss some Violation of confidential data, man-in-middle attack, data corruption are risk issues that impact cloud security. Cloud is one of the most technological research area because of its flexibility and cost efficiency and transformation of data between client and server. [6] this paper elaborates to ensure the strong data security is managed with the help of reputation management system also maintain the transaction table that contains the information. In cloud, virtualization is crucial for cloud computing but the security for virtualization is not adequately studied [7]. This paper analysis of cloud security focuses on how virtualization attacks affects different cloud computing service model. The cloud computing provides platform for sharing of resources that comprises software and infrastructure with the help of virtualization [8]. Which discuss cloud environment makes try to be flexible and reliable to provide services. Cloud security provides some kind of security pattern which cloud service provider cloud comply and uses RSA algorithm with Digital Signature is used to encrypt cloud data While data are transferred in network [9] is described the security management models and security standards and RSA algorithm with Digital Signature to increase cloud data security in cloud.

In the year 2013, it is found that multi-clouds providers to manage security has secured

Revised Manuscript Received on June 10, 2019.

Jaydip Kumar, Department of Computer Science , Babasaheb Bhimrao Ambedkar University, Lucknow, India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

less attention from the research community than the use of single cloud provider [10] the main attention of this paper is use of multi-clouds, reduce security risks and data security. Cloud user’s causes loss of control from the owner’s side due to moving data outward from organizational boundaries and access them through internet. [11] provides brief description about data securing and maintain a level of trust among data owners is become an important issues for cloud providers. The nasty people have second option to cause damage to people’s sensitive information by doing cyber attacks rather than physical attacks and to prevent the cyber attacks needs time and sake of securing business, personal information and nation [12]. In this paper discussed assuring cloud data security, data mining and algorithms contribute tremendously.

In the year 2014, the most important techniques in our life is Internet of Things (IoT) and cloud computing. Their leased and use is expected to increase further, due to this reason will become most required component on internet [13] provide attention on integration of IoT and cloud computing, which is introduced as CloudIoT. Cloud provides virtual pool of resources to the cloud users as service through a web interface and Cloud resources include infrastructure, network, platform, software, storage and most of the organization are migrating their data over the cloud, it is imperative to ensure security and integrity of cloud user’s data [14] has discuss the security risks posed to data on the cloud computing. The fast increment in the field of cloud computing also increases server security problems and it is difficult to track the security threats and one of the most genuine threats comes in the Diversity of a Denial-of-Service(DOS) and its bigger aspect is Distributed Denial-of-Service(DDOS) attack these are the different types of network intrusion in cloud computing environment [15] are proposing a method which are able to filter and detect mostly attacked traffic within a very less period of time.

In the year 2015, found that Distributed Denial of Service Attack is one of the major issues, it is a type of attack where a group of intruder start attacking in a single target that enable to avoid from services for the user of the targeted system [16] described the various Distributed Denial of services attack detection and prevention techniques. Investigation of cloud security is more difficult instead of investigating digital forensic, many challenges are faced by investigator in forensic investigation, to extract evidences from the cloud forensic investigations may become complicated [17] author presented the complexity of cloud and how to affects digital investigations. Cloud is a form of distributed computing where resources and application are shared over the internet and cloud user can pay on utilization basis [18] the aim of this paper is to discuss various unsolved security risks that affecting the cloud computing and also discuss the advantages and disadvantages of existing cloud security plans and also introduced cloud security issues such as data segretation, security and data integrity.

In the year 2016, found that Internet of things (IoT) defines everything, that are connected to Internet with capability to transfer data over network but the design and configuration of technology improperly will caused to security threats [19] described the security threats of Internet of things (IoT) and then proposed the security framework to reduce the security threats. Cloud computing is dynamic technology, that gives the transformation of data and avoid the burden of local storage of cloud users [20] proposed a method to improve the security aspects by using stenography and cryptographic techniques. Security-as-a-Service(SaaS) model provides security in cloud environment and user can easily use these services using web browser and algorithm is canny in a way the Encryption into multiple encryption [21] In this paper author worked in encryption and decryption in cloud service in intellectual and transpicuous manner.

In the year 2017, authors discussed about cloud computing platform is implemented and designed to use web applications and share by internet such type of technology built using OpenStack framework, open to multimodal improvements and exploiting fingerprints is an original biometric approach for user authentication, the platform provide secure access for multiple users guarantees and provide complete logical dissociation of data resources and computation related to different organization [25] described topics related to cloud security, the security of data storage on public cloud servers and authentication of logical user accessing the cloud. In cloud, multi-cloud storage is one of the necessary service which is used to store and access cloud data remotely, and storage are able to encrypt and store information in different cloud drives [26] proposed model, that provide solution for different insider’s attack, privacy for different files uploaded by different users, and decentralized distribution of data storage using an index based cryptographic data.

In the year 2018, the cloud security become biggest concern for cloud researchers due to unauthorized activities are growing on according to cloud users [27] proposed new security architecture for cloud framework that provide more secure data transformation and protect data from data leakage. Data owners and cloud servers have different identities, this framework provide data storage and have different security issues, an independent procedure required to make sure that cloud data is hosted correctly in the cloud server [28] discussed different security techniques for secure data storage on cloud. Cloud computing uses “Utility Computing” and “Software-as-a-Service” to provide required service by cloud user, cloud security is a main and critical fact, has numerous issues and problem related it [29] Described the list of parameters that are affected the security and explore security issues and problems are faced by cloud service provider and consumers like data privacy, security issues and infected application.

III. METHODS FOR SECURING ROUGH DATA SET

A. Genetic Algorithm

Genetic Algorithm (GA) is a searching technique that is used to find approximate or exact solution to optimization and search problem [30] GA convert distinct domain problem to a model by using chromosome and the algorithm process starts with a random selection of the population of

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

chromosomes. Chromosomes are converted into bits or numbers according to the problem [23]. Natural and successive rules are developed by Genetic Algorithm that rules are used for network traffic that differentiate between normal or abnormal traffic.

Pseudo code of Genetic Algorithm

- Select initial populations
- Repeat
- Find out the individual fitness of a certain proportion according to the population
- Choose the best ranking individuals pair to reproduce
- Use crossover and mutation operator
- Repeat the process until the termination condition occurred

B. K-Mean Algorithm

K-mean is the easiest algorithm of partitioning method for clustering analysis. The aim of this algorithm is to minimize an objective function known as square error function is given below.

$$J = \sum_{i=1}^{K} \sum_{j=1}^{Ki} (\| Pi - Ci \|)^2 \qquad (1)$$

$\|Pi - Ci\|$ is Euclidean Distance between P_i and C_i
'k' is the number of cluster centers
'k_i' is the number of data points in i^{th} cluster [31]

Algorithm for k-Mean Algorithm

Let P={p_1, p_2, p_3, p_4, p_5, ………., p_n} is the set of data points and C={c_1, c_2, c_3, c_4, c_5, …, c_n} is the set of center.

- Randomly select K points as initial value of the cluster center
- Calculate the distance between each data points and cluster centers.
- Assign each data points to the cluster of the nearest points measured with a specific distance metric.
- Re-compute new cluster center using

$$Ci = (1/Ki)\sum_{j=1}^{Ki} Pi \qquad (2)$$

Where ki shows the number of data points in ith cluster

- Find new cluster center by using re-computation of distance between all data points
- Stop algorithm if no new data points reassigned otherwise repeat algorithm from step 3.

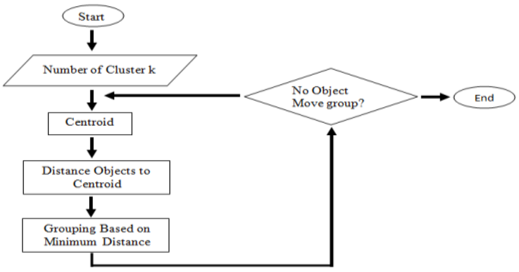
Start
Number of Cluster k
Centroid
Distance Objects to Centroid
Grouping Based on Minimum Distance
No Object Move group?
End

Figure 1: Flow Diagram for K-Mean Algorithm

C. KNN (K- Nearest Neighbor) Algorithm

KNN Algorithm is used for both classification and regression predictive problems and based on feature similarity: choosing the correct value of k is a process called parameter tuning that is important for better accuracy.

Pseudo code for KNN Algorithm

- Initialize k from your chosen number of neighbors
- Calculate distance between the points using Euclidean distance
- Arrange the calculated Euclidean distance in ascending order.
- Select the first k entries from the sorted list.
- Find those k-points corresponding to these k-distances.
- If KNN is used for regression problem the prediction is based on the mean and if KNN is used for classification, the output can be calculated as the class with the highest frequency from the k-most similar instances.

D. Naive Bayesian

Naive Bayesian is a classification technique based on Bayes Theorem. It is easy to use and particularly used for huge data set along with simplicity and calculates the probability of a hypothesis to given prior knowledge.

Bayes' Theorem

$$P(\frac{n}{m}) = \frac{P(m/n)P(n)}{P(m)} \qquad (3)$$

$$P(\frac{n}{m}) = \left[\prod_{i=1}^{n} P(Mi/n)\right] P(n) \qquad (4)$$

$P(\frac{n}{m})$ is the posterior probability

$P(n)$ is prior probability

$P(\frac{m}{n})$ is likelihood which is probability of predictor

$P(m)$ is the prior probability of predictor

IV. SECURITY TECHNIQUES FOR SECURING CLOUD

Cloud data encryption is not the solution for data which can keep faith over cloud security. It can be made by applying existing security techniques like Authentication and identity, encryption, integrity checking, access control, secure detection, and data masking are all the security techniques are applicable to cloud data. Figure 2 explains security techniques.

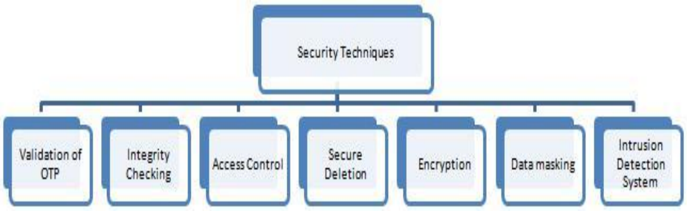

Figure 2 Security Techniques for Securing Cloud

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A. Validation of OTP

In the current scenario, many of banks are providing authentication through One Time Password (OTP) method which is generated through random under generation and used to verify the cloud user sometime it is used for one time authentication called as system factor authentication that is shown in figure 3. While sometime it is used for two time authentication called as Multiple Authentication Factor.

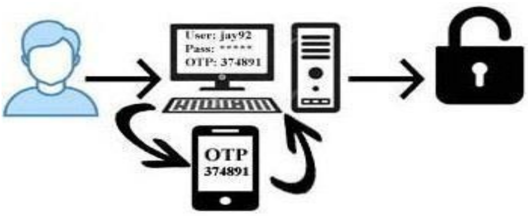

Figure 3 OTP Authentication

B. Integrity Checking

The integrity of cloud data is a guarantee that cloud data can only be changed or accessed by an authorized user. In simple terms, it is a cloud-based data verification process ensures that the data is unmodified, correct and the basic techniques of data integrity are Provable Data Prossession (PDP) is a technique to ensure the integrity of cloud data on a remote server and the technique Proof Of Retrievability (POR) to obtain and verify the evidence that cloud data is stored by the user on the server is not changed [24].

C. Access Control

Access control means cloud data owner can execute some restrictive permission to access their data outsource to cloud and data owner's authorized user can access cloud data while unauthorized user can't due to access control cloud data are protected from modification or unauthorized disclosure of data.

D. Secure Deletion

It is essential to understand how the data is deleted from the server. Deletion uses different techniques like Clearing, in this technique we delete the media before the reuse of these media and at the same time provide protection for accepting the data that contained in the media before deleted. Sanitization, here the protection for accepting previous data is not provided and this type of data is regularly circulated for lower level of classification [32].

E. Encryption

Cloud security provides data encryption service to encrypt cloud data before transfer from local storage to cloud storage and it is impossible to understand from any system, database or file to decrypt data without decryption key and encrypted data is only possible to access with an authorized user with the decryption key and separation of encrypted data and encryption key is necessary for keeping cloud data secure. Figure 4 explains encryption and decryption process given below.

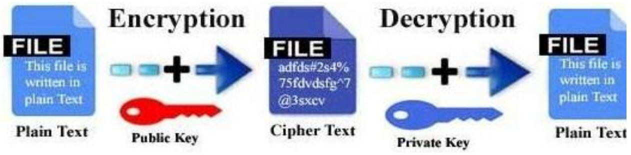
Encryption
Decryption
FILE
This file is written in plain Text
Plain Text
Public Key
FILE
adfds#2s4% 75fdvdsfg^7 @3sxcv
Cipher Text
Private Key
FILE
This file is written in plain Text
Plain Text

Figure 4 Data Encryption and Decryption

F. Data Masking

Data masking is a process of securing and hiding cloud data from attackers and theft and it also insure that the information is changed with realistic but not real information. While people interchangeably use terms such as data de-recognition, data cleansing and understanding the term defining the confusing process. Data masking is not only algorithm but also a public data set. There are different ways or methods are used to mask cloud data, Static Data Masking (SDM) is used by most organizations when creating tests and this is actually the only method of masking possible when using outsourced developers in a separate site or company. In these cases, it is necessary to duplicate the database. Dynamic Data Masking (DDM) provide access based on their role in the organization [3].

G. Intrusion Detection System

Intrusion Detection System (IDS) defines as a software applications or devices that keep eyes on system activities or network traffic and find if any illegal activities occurred. In the recent era, most of the hackers use different attacking techniques for finding users sensitive information. An intrusion signifies any illegal access or evil activities for IT resources. The intruders try to find unauthorized access in sensitive information, causes harmful activities. The two types of Intrusion Detection System are defined, Network-Based Intrusion Detection System (NIDS) that present in a devices or computer connected segment of an organization's network and monitor network traffic and keep eyes on ongoing attacks, Host-Based Intrusion Detection System (HIDS) is installed on specific system or server and monitor illegal activities on that system.

V. CONCLUSIONS

In the above presentation, it is observed that there is a vast scope for the generation of new security algorithms for securing the data set. The importance of each method has been presented in brief however, these can be applied for securing the cloud data in the above where exhaustive literature has been consulted and explained in brief.

REFERENCES

1. R. Choubey, R. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 3, pp. 1227–1231, 2011.
2. R. P. Padhy, M. R. Patra, and S. C. Satapathy, "X-as-a-Service: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure and Force.com," *Int. J. Comput. Sci. Telecommun.*, vol. 2, no. 9, pp. 8–16, 2011.

3. 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.
4. A. Behl , K. Behl, “An Analysis of Cloud Computing security issues,” *2012 World Congr. Inf. Commun. Technol.*, pp. 109–114, 2012.
5. D Chopra, D Khurana, K Govinda, “CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION,” International Journal of Advances in Engineering Research, vol. 3, no. 2, 2012.
6. G. R. Vijay, “An Efficient Security Model in Cloud Computing based on Soft computing Techniques,” vol. 60, no. 14, pp. 18–23, 2012.
7. H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, “Threat as a Service?: Virtualization's Impact on Cloud Security,” no. February, pp. 32–37, 2012.
8. K. Kumar, V. Rao, S. Rao, and G.S. Rao, “Cloud Computing : An Analysis of Its Challenges & Security Issues,” IJCSN,vol. 1, no. 5, 2012.
9. K. D. Kadam, S. K. Gajre, and R. L. Paikrao, “Security Issues in Cloud Computing,” Proceedings published by International Journal of Computer Applications,pp. 22–26, 2012.
10. M. Shrawankar, A. Kr. Shrivastava “Comparative Study of Security Mechanisms in Multi- cloud Environment,” vol. 77, no. 6, pp. 9–13, 2013.
11. N. Aggarwal, P. Tyagi, B. P. Dubey, and E. S. Pilli, “Cloud Computing : Data Storage Security Analysis and its Challenges,” vol. 70, no. 24, pp. 33–37, 2013.
12. P. Aggarwal, M. M. Chaturvedi, “Application of Data Mining Techniques for Information Security in a Cloud: A Survey,” *Int. J. Comput. Appl.*, vol. 80, no. 13, pp. 11–17, 2013.
13. A. Botta, W. De Donato, V. Persico, and A. Pescape, “On the integration of cloud computing and internet of things,” *Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, FiCloud 2014*, pp. 23–30, 2014.
14. D. Panth, D. Mehta, R. Shelgaonkar “A Survey on Security Mechanisms of Leading Cloud Service Providers,” *Int. J. Comput. Appl.* , vol. 98, no. 1, pp. 24–34, 2014.
15. D. Porwal, P. Mohmood Khan and D. Shankar Ray, “Cloud Computing Security Threats and Countermeasures”, International journal for innovations in Engineering Science and Management, vol. 2, no. 4, pp. 1-4, 2014.
16. D. Parwani, A. Dutta, P. Kumar Shulka, and M. Tahilyani, “Various Techniques of DDoS Attacks Detection and Prevention at Cloud: A Survey,” *Orient. J. Comput. Sci. Technol.*, vol. 8, no. 2, pp. 110–120, 2015.
17. G. Al, “Cloud Computing Architecture and Forensic Investigation Challenges,” *Int. J. Comput. Appl.*, vol. 124, no. 7, pp. 20–25, 2015.
18. M. U. Shankarwar and A. V. Pawar, “Security and Privacy in Cloud Computing: A Survey,” *Adv. Intell. Syst. Comput.*, vol. 328, pp. 1–11, 2015.
19. 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.
20. 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.
21. 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.
22. B. Mahesh, “Data Security and security controls in cloud computing”, International journal of advances in Electronics and Computer Sciecne, pp. 11-13, 2016.
23. 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
24. S. Sharma, “Data Integrity Challenges in Cloud Computing”, 4th international conference on recent innovations in science engineering and management, pp. 736-7436, 2016.
25. G. L. Masala, P Ruiu, E Grosso, “Biometric Authentication and Data Security in Cloud Computing,” *Comput. Netw. Secur. Essentials*, pp. 337–353, 2017.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. Data clustering algorithms[online] https://sites.google.com/site/dataclusteringalgorithms/k-means-clustering-algorithm (Accessed 08 March 2019).
32. CloudCodes [online] https://www.cloudcodes.com/blog/ data-protection-controls-techniques.html (Accessed 20 December 2019).
33. DIGITAL GUARDIAN [online] https://digitalguardian.com/blog/what-cloud-encryption (Accessed 25 December 2019).

AUTHORS PROFILE

Jaydip Kumar received his Bachelor degree in Computer Application from Indira Gandhi National Open University, India, in 2013. He received his Master degree in Computer Application from Indira Gandhi National Open University New Delhi, India, in 2015. He is currently pursuing his PhD in Department of Computer Science, Babasaheb Bhimrao Ambedkar University Lucknow, India . Since 2018, his research interests focus on Cloud Security.