International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Security Techniques for Protecting Data in Cloud

Smile Mahajan, Sandeep Sharma

ABSTRACT: ***Cloud computing can store and manage the large amount of data. Storing the data on to cloud is widespread among companies additionally as private users. It permits its users to access the cloud services from the different locations. It wants solely a working internet connection to access the cloud services. A lot of attention is gained by cloud still there are some problems that need to be taken in considerations(i.e. data security, privacy and reliability)in which data security is one in all the most problems. The biggest challenge in the cloud is to maintain the integrity and confidentiality of data. Many techniques are urged for data protection in cloud. This paper focuses on the present security techniques for shielding the data in cloud. The paper has been carried out on the basis of cryptography, intrusion detection, attacks solutions, Data integrity and privacy as well as authentication and identity.***

Keywords- Cloud Computing, Data protection, Security techniques.

I. INTRODUCTION:

According to definition of the term cloud computing given by National Institute of Standards And Technology (NIST) "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared a pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].During this quick paced life, people are greatly inclined to the technology and also the world can become additional tech savvy as compare to former timings and during this time, cloud has been one among the favorite technical paradigm within the field of computation and provides a varied services as required by users which incorporates data centers using the Internet to fulfil the demands of their clients. The cloud model consists of five characteristics, four deployment model are as follows:

a) Community Cloud
b) Public Cloud
c) Private Cloud
d) Hybrid Cloud

The three service model are

(a) Infrastructure as a Service (IaaS)
(b) Platform as a Service (PaaS)
(c) Software as a Service (SaaS)

The two security issues in cloud are:

(1) Security threats faced by their customers (2) Security related problems faced by the cloud providers.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Smile Mahajan*, Dept. of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India
Dr. Sandeep Sharma, Dept. of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India

1.1 ISSUES REGARDING SECURITY OF CLOUD:

To protect the user's data from any risk a layer of security is provided by cloud vendors. Password guessing attacks, man in middle attack are some sorts of attacks in the cloud. Security challenges in the cloud are:

i. Data Protection and Misuse: The data is at risk when the data is stored on cloud by different companies and there is an imminent need to secure the data from the risk. Authentication and restrict access can be used to secure the data.
ii. Integrity: In order to provide security the system should be control so that only authorized person could access the data. To avoid the data from any loss the integrity of data should be maintained.
iii. Access: The data management and security of data policies regarding the access are necessary. The owner of authorized data are required to give individuals the half access so that the specified data access stored within the data mart are accessible to everyone.
iv. Confidentiality: In the cloud, lot of sensitive information could be stored. The possibilities of breeches and phishing attacks can be scale backed to further layer of security in the data and this could be possible through service provider and organization. Data confidentiality, however as precaution ought to be vital priority for sensitive material.
v. Breaches: Breaches are common in the cloud. The confidential data for organization could be stealed through hackers breaching security parameter among the cloud. On the other hand , breach are often internal attack, thus unwanted attacks on stored data could be avoided by giving specific stress in tracking employee's actions by the oragnizations .

1.2 SECURTIY TECHNIQUES IN CLOUD COMPUTING:

Latest security techniques in cloud computing are:

a. Biometric: The biometric security system in cloud computing is increasingly in terms of usage as a result of which it gives benefits over traditional authentication methods such as passwords and IDs. The rendered services are ready to give better reliability and accuracy to these systems with the high level security.
b. Cryptography: Cryptography converts an original message into an encrypted form i.e. not readable for outsiders which is called encryption and converts it back to an original message called decryption. It offers a collection of economical solutions to shield sensitive information by encoding a message into cipher-text and decipher it back into plain text.
c. Flooding Attack: Denial of service attacks are DOS and DDOS. The attack works by requesting so many resources from a server that the server cannot reply to the legitimate requests.

A DoS attack originate from a one device and DDoS involves traffic from multiple devices. The security techniques used in case of DoS attacks like deep packet inspection and application hardware placed on the network to analyze the packets. EDoS attack could be sort of DDoS attack .A technique referred to as SPART is used to mitigate the EDoS attacks within the cloud computing.

d. Intrusion Detection: It provides protection of privacy and shield against cloud resources and asset. IDS play a vital role in detection of attacks in the cloud. Since it is very challenging matter, still susceptible to the intruders is made through the distributed architecture of the cloud.

II. LITERATURE SURVEY:

Abhishek Sharma and Shilpi Sharma [2] focuses on various encryption techniques that has efficient computing time and focuses on the algorithm used for security, efficiency and complexity.

Madhvi Popli and Gagandeep [3], flower pollination original form is presented with DNA cryptography in order to achieve optimized technique to enhance cloud security. Flower pollination algorithm helps us to search out best solution whereas DNA cryptography helps to encrypt data in few grams of DNA.

Medhat A.Tawfeeq and Ashraf B.El Sisi [4], proposed a system (called network intrusion detection system) which examine and monitor the network traffic flows.

Preeti Daffu, Amanpreet Kaur [5], proposed a technique known as a SPART enforced to mitigate the EDoS attacks in cloud that consumes less energy as compared to the previous existing models.

Jing Qin, Wenting Shen Rong Hao and Jian

Kun Hu [6], worked (remote data integrity auditing scheme) on sharing of data with sensitive information hiding and during which a sanitizer is used to sanitize the blocks of data and converts these blocks of data signatures for the sanitized data.

Ramraj Dangi and Satish Pawar [7], proposed a secure three factor authentication model that help us to replace the dependency of the device and the parameters with low computation, three-factor security model is very effective.

Mohammed Shuaib and Abdus Samad [8] had studied different IDP techniques and in order to provide security various weaknesses and strengths are analyzed on different parameters. In comparison to traditional IDP techniques, distributed and hypervisor IDP have shown promising security features.

Vaibhav Aggarwal, Satish Chand, Jai Prakash Sah and Shilpha N.R [9] compare a Hybrid Cryptography Algorithm (HCM) that joins the benefits and downside of both symmetric and asymmetric encryption bringing about the protected cloud environment.

Ashima Narang, Dr Deepali Gupta [10] a comparison of three different existing security architectures are coated and on the basis of Computation Time, Computation Cost and Cipher Text Size are compared.

Pietro Ruiu, Giovanni L.Masala and Enrico Grosso [11] guarantees the identity of users by using the system called biometric authentication which is based on fingerprints.

Vahid Shaker, Amin Hatef Mohammad Reza Jabbarpour and Zarrabi [12] presented an HIDCC solution that prevent and detect intrusions in cloud and the result shows that there is a reduction in false warnings and the accuracy of intrusion detection, intrusion coverage, availability and reliability in cloud are increased.

Suyel Namasudra [13], developed a model that are secure and efficient enough to share the knowledge and resources by using DHT, ABE and identity based time release encryption.

Santosh Kumar, Amit Kumar Singh, Sanjay Kumar Singh, Sanjay Kumar Singh and Ravi Shankar Singh [14] focuses on privacy problems and security of cloud. It provide relevant solutions by using biometric face recognition followed by three steps (a) extracting and preprocessing the facial features (b) Encrypted biometric features are used to recognize the individual (c) acquisition of face images.

Burhan Al-Bayati, Nathan Clarke and Paul Downland [15] Multi-instance behavioral profiling framework is proposed to provide continuous identity verification in cloud services through monitoring user application activities

Table 2. Literature Survey

Author	Year	Security Method							Techniques/ Algorithm Used
		Biometric	Cryptography	Identity	Integrity	Attack	Authentication	Intrusion Detection	
Abhishek Singh et.al	2019	×	✓	×	×	×	×	×	Split Algorithm, Caesar Cipher And Vigenere Cipher
Madhvi Popli et.al	2019	×	✓	×	×	×	×	×	Flower Pollination Algorithm
Mahmoud M.Sakr et.al	2019	×	×	×	×	×	×	✓	Anomaly-based network Intrusion Detection system (NIDS)
Preeti Daffu et.al.	2018	×	×	×	×	✓	×	×	SPART(Supervised Pattern Attack Recognition Technique)

Wenting Shen,Jing Qin et.al	2018	×	×	×	✓	×	×	×	Identity Based Shared Data Integrity Auditing Scheme
Ramraj Dangi and Satish Pawar	2018	×	×	×	×	×	✓	×	Three Factor Authentication
Shadab Alam et.al	2018	×	×	×	×	×	×	✓	IDP Techniques

Author	Year	Security Method							Technique/ Algorithm Used
		Biometric	Cryptography	Identity	Integrity	Attack	Authentication	Intrusion Detection	
Vaibhav Aggarwal, Satish et.al	2018	×	✓	×	×	×	×	×	Hybrid Cryptography Algorithm
Ashima Narang, Dr Deepali Gupta	2018	×	✓	×	×	×	×	×	Blowfish, HASBE, Diffie Hellman , RSA &ECC
Giovanni L.Masala Pietro Ruiu et.al	2018	✓	×	×	×	×	×	×	Fingerprint Recognition
Mohammad Amin Hatef, Vahid Shaker et.al	2017	×	×	×	×	×	×	✓	Hybrid Method
Suyel Namasudra	2017	×	✓	×	×	×	×	×	ABE,DHT, IDTRE

Author	Year	Security Model							Technique/ Algorithm Used
		Biometric	Cryptography	Identity	Integrity	Attack	Authentication	Intrusion Detection	
Santosh Kumar, Sanjay Kumar Singh et.al.	2017	✓	×	×	×	×	×	×	Face Recognition
Burhan Al-Bayati, Nathan Clark et.al	2016	×	×	✓	×	×	×	×	Multi-level Behaviour Profiling

III. PARAMETRIC ANALYSIS

In this part parametric analysis of the studied papers has been done. The different parameters are used by the distinct authors that are accuracy, efficiency, throughput, threshold, energy consumption and time.

Table 3: Parameters

(1) Parametric analysis on cryptography and biometric

AUTHOR	PARAMETRS						RESULT
	Efficiency	Accuracy	Throughput	Threshold	Time	File Size	
Abhishek Singh And Shilpi Sharma	✓	×	×	×	×	×	High efficiency in split algorithm and low efficiency in Caesar Cipher And Vigenere Cipher

Author	PARAMETERS						Result		
	Efficiency	Accuracy	Throughput	Threshold	Time	File Size			
Madhvi Popli, Gagandeep	×	×	×	×	×	✓	Low		
Vaibhav Aggarwal, Satish Chand et.al.	×	×	×	×	×	×	Not mentioned		
Ashima Narang, Dr Deepali Gupta	×	×	✓	✓	✓	✓	RSA& ECC	Diffie Hellman	Blowfish & ABE
							Less Time	High time	Medium time
							High throughput	Low throughput	Medium thoughput
							Low file size	Low file size	Large file size
Suyel Namasudra	×	×	×	×	×	✓	Large		
Santosh Kumar, Sanjay Kumar Singh et.al.	×	✓	×	×	×	×	High		
Giovanni L.Masala ,Petro Ruiu And Enrico Grosso	×	×	×	✓	×	×	High		

(2) Parametric analysis on Attack, Integrity, Intrusion detection, identity And Authentication

Author	Parameters	Result
Preeti Daffu, Amanpreet Kaur	Energy Consumption	Less
Burhan Al-Bayati, Nathan Clarke, Paul Dowland	Accuracy	High
Jing Qin, Jia Yu, Rong Hao And Jiankun Hu	Time	Low
Shadab Alam, Mohammad Sahib And Abdus Samad	Security	High
Mohammad Amin Hatef, Vahid Shaker et.al.	Detection Accuracy False warning	High Low
Mahmoud M.Sakr,Medhat A Tawfeeq et.al.	Detection Accuracy False Alarm Rate	High Low
Ramraj Dangi And Satish Pawar	Time, Cost	Low

IV. GAP IN EXISTING LITERATURE

In this section we have discussed the work done and limitations

Author	Year /Publisher	Proposed work /Work Done	Gap
Abhishek Singh And Shilpi Sharma	2019 Springer	Provide security to clients and compare the different secured encryption techniques which have efficient computing time	The limitation of the paper is that only Three algorithms are compared on which efficiency is taken out.
Madhvi Popli, Gagandeep	2019 Elsevier	Optimization include random key values which can extend the level of security by implementing it and the time complexity of the work shows the feasible nature of the algorithm.	The file size limit is upto 3KB

Mahmoud M.Sakr, Medhat A Tawfeeq et.al.	2019 MECS	The NSL-KDD dataset is tested and trained by NIDS and the outcomes results in efficiency in normal behaviours recognition and the attacks are detected along with low rates of false alarm.	The evolutionary techniques and other optimal network feature selection strategies used in optimizing control parameter of classification algorithm is directed through future work.
Preeti Daffu, Amanpreet Kaur	2018 MECS	Energy consumption has been recorded in the form of residual energy.	Previous techniques are not explained.
Wenting Shen, Jing Qin, Jia Yu et.al.	2018 IEEE	Steps include for proposing the auditing scheme for data integrity is: hiding the sensitive information and the files can be shared and used by others that are stored in the cloud. The experiment show that the auditing scheme achieves efficiency and desirable security.	Need to execute the remote data integrity efficiently.

Author	Year /Publisher	Proposed work /Work Done	Gap
Ramraj Dangi And Satish Pawar	2018 Springer	A secure email-based OTP is developed which provide three-level security and focus is to make reliable and flexible interface over the cloud server so that anyone can share the data.	Not Mentioned
Shadab Alam, Mohammad Sahib And Abdus Samad	2018 Springer	Compare the different IDS and IPS techniques in which distributed and hypervisor based IDS provide the high level of security to the cloud based environment.	The major issues of the system are complexity and standardization that need to be addressed.
Vaibhav Aggarwal, Satish Chand, Jai Prakash Sah And Shilpha N.R	2018 IJARCS	Hybrid cryptography implementation method solves all the problems. Data security for any and all types of anticipated or unanticipated attacks pertaining to cloud storage.	Only three encryption methods (Hybrid cryptography, AES and RSA) are used for protecting data on cloud storage.
Ashima Narang, Dr Deepali Gupta	2018 ISSN	Diffie hellman based approach, hybrid HBASE and Blowfish And hybrid RSA&ECC were used and experiment was done by implementing these algorithms and results show that RSA&ECC outperform from other methods.	RSA &ECC can be considered for enhancement or to provide more secure environment to the cloud server.
Giovanni L. Masala, Pietro Ruiu et.al.	2018 Springer	Data management and web application are coupled with strong biometric authentication and data chunking solution is proposed that rely on distributed cloud storage architecture.	Biometric access can be extended through multimodal techniques and to the development of web server is needed to avoid the installation of local software

Author	Year /Publisher	Proposed work /Work Done	Gap
Mohammad Amin Hatef, Vahid Shaker et.al	2017 Wiley	HIDCC method has been implemented which shows that intrusion coverage, reliability, detection accuracy and availability are increased and false warning are reduced.	NSL-KDD has high accuracy and precision as compared to HIDCC.
Suyel Namasudra	2017 Wiley	Efficient and access method has been proposed by using ABE, DHT and IDTRE.	By developing novel authorization scheme we can improve the security system.
Santosh Kumar, Amit Kumar Singh et.al.	2017 Springer	Biometric based recognition system extracts the features of privacy preservation and the sensitive data is stored in the encrypted form.	The process of matching of facial data image encryption is time consuming and also this cause failure of better recognition of individual in small database.
Burhan Al-Bayati, Nathan Clark	2016 GSTF	Multi-instance behavioral profiling framework is able to provide continuous identity verification in cloud services through monitoring user application activities	Need to measure the discriminative value of the feature set.

V. CONCLUSION :

In the concern, the security technique in cloud is a challenge for protecting data. In this paper, different security techniques are studied and best solution comparison is done to provide the best information to the researchers. From the above mentioned techniques we will use the cryptographic algorithm using hybrid approach for the security purpose, in future for research work.

REFRENCES:

1. www.wikipedia.com Definition of Cloud Computing.
2. Abhishek Sharma and Shilpi Sharma, "Enhancing Data Security Using Split Algorithm, Caesar Cipher, and Vigenere Cipher and Homomorphism Encryption Scheme", Springer Publication, 2019, pp.157-166.
3. Madhvi Popli and Gagandeep, "DNA Cryptography: A Novel Approach for Data Security using Flower Pollination Algorithm", International Conference on Sustainable Computing in Science, Technology & Management, 2019, pp.2069-2076.
4. Mahmoud M.Sakr, Medhat A.Tawfeeq and Ashraf B.El Sisi, "Network Intrusion Detection System based PSO-SVM for Cloud Computing", I. J. Computer Network and Information Security, 2019, 3-22-29, doi 10.5815/ijcnis.2019.03.04.
5. Preeti Daffu, Amanpreet Kaur, "Energy Aware Supervised Pattern Attack Recognition Technique for Mitigation of EDoS Attacks In Cloud Computing", I.J. Wireless and Microwave Technologies 2018,1,42-49.
6. Wenting Shen,Jing Qin, Jia Yu,Rong Hao and Jiankun Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage", IEEE transactions on Information Forensics And Security,2018, VOLNO.2018.
7. Ramraj Dangi and Satish Pawar, "An Improved Authentication and Data Security Approach over Cloud Environment", Springer Publication 2018, pp.1069-1076.
8. Shadab Alam, Mohammed Shuaib and Abdus Samad ,"An Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing", Springer ,N. Yadav et.al, Harmony Search And Nature Inspired Optimization Algorithm, 2018 ,pp.231-240.
9. Vaibhav Aggarwal, Satish Chand, Jai Prakash Sah and Shilpha N.R, "A Framework: Encryption on Cloud Storage for Data Security", International Journal of advance Research in computer science, Volume 9, special Issue No 3, May 2018.
10. Ashima Narang, Dr Deepali Gupta, "Comparative Analysis of Various Cloud Security Frameworks", International Journal of Advanced Studies of Scientific Research, 2018, pp.379-384.
11. Giovanni L. Masala, Pietro Ruiu and Enrico Grosso, "Biometric Authentication and Data Security in Cloud Computing", Springer Publication, 2018, pp.337-353.
12. Mohammad Amin Hatef, Vahid Shaker, Mohammad Reza Jabbarpour, Jason Jung and Houman Zarrabi, "HIDCC: A hybrid intrusion detection approach in cloud computing",2017,wileyonlinelibrary.com/journal/cpe, pp.1-10.
13. Suyel Namasudra, An improved attribute based encryption techniques towards the data security in the cloud computing,2017,wileyonlinelibrary.com/journal/cpe,pp.1-15.
14. Santosh Kumar, Sanjay Kumar Singh, Sanjay Kumar Singh, Amit Kumar Singh and Ravi Shankar Singh, "Privacy preserving security using biometrics in cloud computing", 2017,p.11017-11039.
15. Burhan Al-Bayati, Nathan Clarke and Paul Downland, "Adaptive Behavioral Profiling for Identity Verification in Cloud Computing: A Model and Preliminary Analysis", GSTF Journal on Computing, 2016, Volume 5, Issue 1, pp.21-28.