International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Security Concerns in Cloud Computing: Analysis and Solution

Jasmine Attri, Prabhpreet Kaur

Abstract: ***Cloud computing present comprehensive way for the user to interact with resources that they didn't possess. Using cloud computing, resources can be accessed on pay per use basis. Mass community of user access resources from cloud and due to presence of sensitive information presents within cloud, security mechanism become need of the hour. This paper discusses security mechanisms used within cloud along with shortcomings and future enhancement of each technique. DNA encryption mechanism is discussed in detail along with research gap and problem definition. Collision problem is discovered from DNA encryption and its rectification using future enhancement process of folding with chaining is also presented through this literature. Results obtained in terms of parameters such as key size and execution time is presented in tabular structure. DNA encryption with folding method has least execution time in key formation but collision problem hamper performance of DNA encryption. Parameters such as throughput, key size and execution time must be enhanced through collision detection mechanism and discussed through this literature.***

Keywords: ***Cloud computing, Security, Collision, DNA Encryption.***

I. INTRODUCTION

The cloud computing is an emerging technology among its users and the migration of virtual machines is an import aspect of cloud computing. The technique which is used for migrating virtual machines and selection of data centres are known as virtualization. The migration is done for reducing energy utilized, load balancing, fault tolerance and for maximizing the profits/ quality of services. The security of data during migration is required. This paper provides comprehensive study of techniques used to enhance security within cloud computing environment. The cloud computing provides unlimited resources over the internet and the cost is encounters on the basis of pay per use. As cloud computing provides number of benefits so large number of users utilized the services of cloud. The Intention of users is uncertain and some users may be malicious causing threats to cloud resources. Security threats in cloud significantly reduce performance of system. Data loss and increased cost due to security threats potentially reduce benefits provided through cloud. Cloud computing is a model for empowering comfortable, on-request access to a mutual system containing a pool of configurable computing resources that can be effectively utilized and discharged with services.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Jasmine Attri*, Pursuing M.Tech (CSE), Guru Nanak Dev University, Amritsar. India
Prabhpreet Kaur, Assistant Professor, Department of Computer Engineering and Technology ,Guru Nanak Dev University, Amritsar, India.

Currently cloud computing gives dynamic services like applications, information, memory, data transfer capacity and IT benefits over the web.

It is new way to access and manage user's data without physically located over there. The services can be accessed remotely by the user according to cost beneficial way without any worry about management of resources. The major advantage of cloud computing is that the same resources can be shared between the multiple users by Virtualization technique. To improve significance of cloud computing, security mechanism must be enforced within cloud computing.

This paper presents concise but all round analysis of security concerns associated with cloud computing. Section I gives detailed introduction about cloud computing and security. The Section II describes the literature survey and comparison table. Section III gives research gap and section IV defines the problem definition. The section V describes proposed methodology and Finally this paper present future security work leading to protection of cloud data.

II. LITERATURE SURVEY

This section presents the comprehensive analysis of security mechanisms used in cloud computing. Cloud computing security mechanisms along with distinct services provided are discussed as under Sohal and Sharma in 2018 [1] proposed a DNA based symmetric key algorithm for providing security in cloud. Cloud security services include phases such as file uploading, checking, encryption, downloading and decryption. All of these phases are discussed in this approach. Key generation is complex and execution time is reduced using this mechanism. the problem that occurs during key generation is collision. To rectify the issue, collision handling must be employed.

Kudtarkar et al. in 2015 [2] proposes technique for handling cloud security which is based on multiple cloud storage with enhanced encryption technique. In this file is split into chunks that is encrypted and stored on multiple clouds. This technique is efficient and increases the advisory of users. But it is not implemented on live storage cloud server.

Akhil et al. in 2018 [3] describes AES based technique for cloud security that increase the security of data during transmission. It ensures the correctness of data and handle large amount of data. It also avoids intruder access into the cloud data centre so provides efficient encryption technique. It only ensures secrecy of data to all other users who use the same server for data storage. Chase et al. in 2019 [4] proposed technique for cyber insurance provisioning and security in cloud computing. It utilized stochastic optimization technique that provides optimally both services.

It gives increased allocation and attack detection. It worked on honey pot data so accuracy can be further enhanced.

Shaukat and Hassan in 2017 [5] proposed an encryption strategy for cloud security that monitor the cloud server and maintain the SLA. It enhanced the availability and security of data centres. It encrypt the data when it is transferred from public cloud. It gives delegated authentication and authorization to user so that security can be enhanced. It cannot handle multiple user at a time so security of cloud must be improved.

Deshmukh in 2018 [6] describes a three level of protection technique for data over the cloud. It first of all encrypt the data, then provide privacy and security to data from unauthorized access. It provides more secure cloud data centre and also privacy preservation in public cloud. It does not considered cloud data storage that are significantly enhanced.

Esposito et al. in 2018 [7] proposes block chain based data access control mechanism in which private or secret keys are used at sender and receiver end. These keys can be used to easily encrypt and decrypt the information. These security strategies become critical as more and more users interact with the cloud.

Jana et al. in 2018 [8] proposed memory replication mechanism to enhance security concern within LTE cloud. Replication procedure includes copying of sensitive information at multiple places. In case of failure sensitive information can be recovered from other replicated images. Storage space was heavily used in this approach.

Meng et al. in 2018 [9] proposed hierarchal framework that process massive data in cloud computing. It utilized two alarms that firstly detect the serious attack and then indicate the user about the attack. It analyzes the data in clusters and the accuracy of cluster is increased. Storage space utilized is more.

Singh et al. in 2015 [10] proposed Elliptic Curve Digital Signature Algorithm (ECDSA) within cloud. This mechanism allows reduces redundancy along with encryption for security. It enhances the storage and retrieval of data in cloud data centre. This technique provides more security.

Awad et al. in 2018 [11] proposed chaos based encryption strategy that allow the cloud to store fuzzy and ranked based encrypted data. It guarantees the privacy and confidentiality of the user even in public cloud. It achieved effective retrieval of remotely stored encrypted data for mobile cloud computing scenarios. There no backup server is used.

Cloud computing mechanism provides advancement in terms of resource sharing. Resource sharing does not cause expense to enhance and hence it is becoming global needs for the users. As more and more users interact with cloud and share resources, chances of information leakage and maliciousness is always an issue. To handle issue exiting within cloud computing, cloud security is of prime concern. Cloud security enhancement strategies are discussed and future enhancements are also suggested through this literature.

III. RESEARCH GAP

The existing literature proposed DNA based encryption strategy where binary codes are employed after random sequence of codes is generated. The length of key generated is large and complex. This large key size causes high storage requirements. To resolve the issue folding method can be accommodated within the DNA encryption approach. DNA encryption mechanism uses high degree of complexity with key formation but overlapping problem last within the encryption process. Execution time and throughput that is enhanced through DNA encryption process, can be further enhanced using folding DNA approach. A problem extracted from the existing is given in next section.

Table I: Comparative analysis of different literature corresponding to security

Reference	Technique used	Parameter	Advantage	Disadvantage
(Kudtarkar et al .in 2015)	Multiple cloud storage with encryption	Number of files uploaded, encryption time	This technique is efficient and increases the advisory of users.	it is not implemented on live storage cloud server.
(Akhil et al. in 2018)	AES based cloud security	File size, decryption time, encryption time	It ensures the correctness of data and handle large amount of data. It also avoids intruder access into the cloud data centre so provides efficient encryption technique.	It only ensures secrecy of data to all other users who use the same server for data storage.
(Chase et al. in 2019)	Cyber insurance provisioning and security	Accuracy, localization error	It gives increased allocation and attack detection.	It worked on honey pot data so accuracy can be further enhanced.

(Shaukat and Hassan in 2017)	Encryption strategy	File size , time, accuracy	It enhanced the availability and security of data centres. It encrypt the data when it is transferred from public cloud.	It cannot handled multiple user at a time so security of cloud must be improved.
(Deshmukh in 2018)	Three level protection technique	Cost, time	It provides more secure cloud data centre and also privacy preservation in public cloud.	It does not considered cloud data storage that are significantly enhanced.
(Esposito et al. in 2018)	Block chain based access control	Accuracy, number of files	The accuracy of system increased	These security strategies become critical as more and more users interact with the cloud.
(Jana et al. in 2018)	Memory replication mechanism	Time , file size, number of users	In case of failure sensitive information can be recovered from other replicated images.	Storage space was heavily used in this approach.
(Meng et al. in 2018)	Hierarchal framework	Encryption time , file size	It analyzes the data in clusters and the accuracy of cluster is increased.	Storage space utilized is more.
(Singh et al. in 2015)	Elliptic Curve Digital Signature Algorithm (ECDSA)	Accuracy, time ,cost	It enhances the storage and retrieval of data in cloud data centre. This technique provides more security.	It must be optimized so that transmission process fastened.
(Awad et al. in 2018)	Chaos based encryption strategy	Number of users, accuracy	It guarantees the privacy and confidentiality of the user even in public cloud. It achieved effective retrieval of remotely stored encrypted data for mobile cloud computing scenarios.	There no backup server is used.

IV. PROBLEM DEFINATION

The problem with the DNA encryption is the generation of codes for distinct words within the file presented for encryption. In case of code generation, collision is the main problem. This means distinct words from uploaded file lead to same code and location causing the existing code to be overwritten. For example: let the content “4501” and “9100” are content of file. Folding method within DNA encryption generates “4+5+0+1=10” and “9+1+0+0” thus key location is overlapped causing loss of cipher text and decryption is unsuccessful. In addition DNA encryption space consumption and execution time is high. Thus DNA encryption in cloud has three aspect problems.

- High Execution time while encoding large file chunks.
- Collision due to same key location generation in case folding mechanism.
- Null values are not allowed within DNA map.

The parametric comparison table for essential and absent features in existing work along with future enhancement is given in table 2.

V. METHODOLOGY OF PROPOSE WORK

The methodologies of proposed work modify existing DNA approach to achieve key without collision and hence reliable key with least size requirement could be formed. The flow of system that can enhance DNA encryption

Table II: Parametric comparison with essential and absent features.

FEATURE	QUANTITY AND DESCRIPTION	PROBLEM
Number of phases	5 Phases follows are: • Uploading • File Checking • Encryption • Downloading • Decryption	Phases causes execution time to increase in case uploaded file is large in size
Encryption	One algorithm BDNA	Folding method employed within DNA encryption generate key that is prone to collision
Key Size	1 key with 32 bits	Key size can be extended to 64 bits for increasing complexity
Execution time	It is a metric defining least time for key generation	Duplicate contents within file could cause high execution time during translation
Future Enhancement	Additional phases with duplicate content handling and collision detection	----

strategy is given in figure 1. The suggested mechanism includes phases.

These phases are explained as follows:

Phase 1: File Uploading

This is an initial phase where user selects the file to be uploaded on cloud. The file selected for upload could be media or text file. Media file consume excessive time while uploading so text file can be used for demonstration of propose system. Uploading of file uses is at server end and entire encryption process is deployed at client end.

Phase 2: File Checking

This phase involve checking of file against file already present at datacenter. In case file already present at datacenter then fresh file cannot be uploaded on cloud again. This save storage and replication problem at datacenter.

Phase 3: Encryption Process

This phase is critical and building block for the solution associated with collision. In this phase, folding is applied to check the collision and then chaining mechanism can be used to resolve the issues of collision. Using the hash based chaining mechanism, same location is capable of storing multiple data elements. In addition, randomization deployed for file data encryption causes complex key formation.

Phase 4: Downloading

This phase is performed at the client end. The downloading can be done at client that is subscribed to the cloud services. The downloading speed depends upon the internet service provider and file storage service that is provided be cloud service provider.

Phase 5: Decryption

This is last phase of the propose system. In this phase, decryption is performed using lookup table formed during encryption phase. Result can be presented in form of execution time, throughput and key size.

COMPARISON TABLE

Comparison of results obtained through different literature is presented through metric consideration as shown in table III

Table III: Metric comparison

Technique	Key Size	Execution time
RSA Encryption	10KB for file size of 1 MB	10ms
DES Encryption	12 KB for file size of 1 MB	12ms
DNA Encryption	9 KB for file size of 1 MB	11 ms
Hamming Codes	13 KB for file size of 1 MB	12 ms

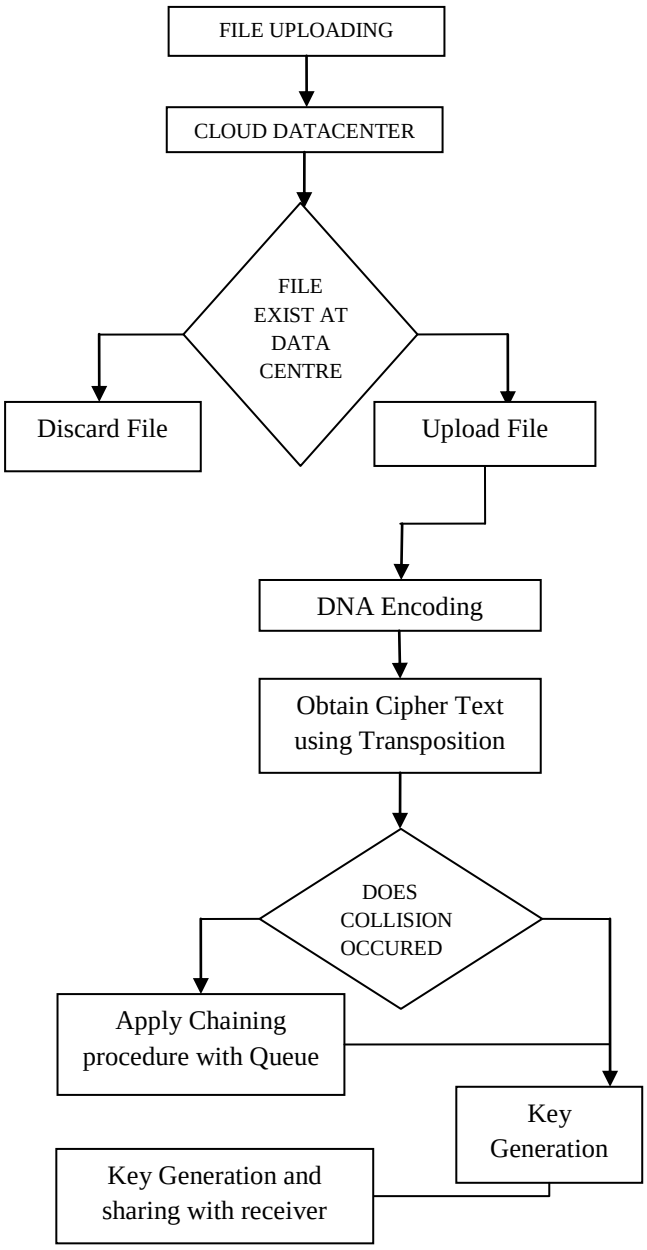

Figure 1: Flowchart for propose system using collision handling procedure

VI. CONCLUSION

Cloud computing provides shared resources so there is threat to security of users. In this paper the survey of various techniques used for maintaining security of cloud. The security threats distort the working of cloud system and harm the data of user so to resolve this problem many security handling mechanism is used. In this paper various algorithms that are used for handling security of cloud is studied. The advantages and disadvantage of each technique is listed and it is concluded that security mechanism utilised. In future, DNA encryption based mechanism with collision rectification for enhancing security within cloud system can be used. This may lead to enhance trust of users within cloud for storing sensitive data. Execution time and key size is critical in every security procedure. Key size is reduced to 10% of its original size using DNA encryption but collision increase execution time for encoding as well as decoding. This can be minimised considering chaining mechanism in future enhancement.

REFERENCES

1. Sohal M, Sharma S (2018) "BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing". J King Saud Univ - Comput Inf Sci. doi: 10.1016/j.jksuci.2018.09.024
2. Kudtarkar PP, Pagare JD, Ahire SR, Pawar TS (2015) Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment. 5:206–211.
3. Akhil KM, Kumar MP, Pushpa BR (2018)" Enhanced cloud data security using AES algorithm". Proc 2017 Int Conf Intell Comput Control I2C2 2017 2018-January:1–5 . doi:10.1109/I2C2.2017.8321820
4. Chase J, Niyato D, Wang P, Chaisiri S, Ko RKL (2019)" A Scalable Approach to Joint Cyber Insurance and Security-As-A-Service Provisioning in Cloud Computing". IEEE Trans Dependable Secure Comput 16:565–579 . doi: 10.1109/TDSC.2017.2703626
5. Shaukat K, Hassan MU (2017) Cloud computing security using encryption technique. Transylvanian Rev 25:74–82
6. Deshmukh R (2018) "Enhanced Privacy Preservation and Data Storage Security in Public Cloud." Helix 8:3726–3730 . doi: 10.29042/2018- 3726-3730
7. Esposito C, De Santis A, Tortora G, Chang H, Choo KKR (2018) Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput 5:31–37 . doi: 10.1109/MCC.2018.011791712
8. Jana B, Poray J, Mandal T, Kule M (2018) "A multilevel encryption technique in cloud security". Proc - 7th Int Conf Commun Syst Netw Technol CSNT 2017 220–224 . doi: 10.1109/CSNT.2017.8418541.
9. Meng Y, Qin T, Liu Y, He C (2018) "An Effective High Threating Alarm Mining Method for Cloud Security Management". IEEE Access 6:22634–22644 . doi: 10.1109/ACCESS.2018.2823724
10. Singh JP, Mamta, Kumar S (2015) Authentication and encryption in Cloud Computing. 2015 Int Conf Smart Technol Manag Comput Commun Control Energy Mater ICSTM 2015 - Proc 216–219 . doi: 10.1109/ICSTM.2015.7225417
11. Awad A, Matthews A, Qiao Y, Lee B (2018)" Chaotic Searchable Encryption for Mobile Cloud Storage". IEEE Trans Cloud Comput 6:440–452 . doi: 10.1109/TCC.2015.2511747

AUTHOR PROFILE

Jasmine Attri, Department of Comp. Engg. & Tech, Guru Nanak Dev University, Amritsar, India
Jasmine Attri is pursuing M.Tech (CSE) from Guru Nanak Dev University, Amritsar. Her research interests include Cloud Computing and Data Security.
She did her Bachelors of Engineering in Computer Science and Technology from Guru Nanak Dev University, Regional Campus Jalandhar, India.

Prabhpreet Kaur, Department of Comp. Engg. & Tech, Guru Nanak Dev University, Amritsar, India
Prabhpreet Kaur is an Assistant Professor in the Department of Computer Engineering and Technology at Guru Nanak Dev University, Amritsar. She is pursuing Ph. D. from Guru Nanak Dev University, Amritsar. Her research interests include Image Processing , Genetic Algorithm, machine learning and deep learning. she has had many research papers published in Scopus Index, Web of Science. More than 50 papers published in peer reviewed, journals and conferences.