JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

TRENDS IN CLOUD COMPUTING: ANALYSIS AND SOLUTION

KIRAN KUMARI

DEEPAK

1. 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 centers 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. 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. In today's era cloud computing becomes the hottest topic due to its ability to reduce the cost associated with computing. Cloud computing provides the on demand services like storage, servers, resources etc. to the users without physically acquiring them and the payment is according to pay per use. Since cloud provides the storage, reduces the managing cost and time for organization to the user but security and confidentiality becomes the one of the biggest obstacle in front of us. The major problem with cloud environment is, the number of user is uploading their data on cloud storage so sometimes due to lack of security there may be chances of loss of confidentiality. To overcome these obstacles a third party is required to prevent data, data encryption, and integrity and control unauthorized access for data storage to the cloud.

With the rapid development of hardware and software cloud computing brings the revolution in the business industry(Yu, 2012). It provides resources like computational power, storage, computation platform ad applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Salesforce, Microsoft etc. Cloud computing

features included resource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. Even though, to control the infrastructure of clouds there is no need of knowledge or expertise, it is abstract to the user. (Mills, Znati and Melhem, 2014). Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it.

1.1 Security issues in cloud Computing

In cloud environment usual data transmission occurs between client and server using third party. So the confidentiality of your data becomes the primary problem. (Chen *et al.*, 2015). The system which interconnects a cloud must be secure and the migration from physical machine to virtual machine must be safe. Information security includes encoding the information and additionally guaranteeing that suitable strategies are implemented for information sharing(Lakshmi, 2013). Cloud security isn't to be mistaken for "cloud-based" security benefit over the conventional danger. This security administration can be upgraded with the distributed computing, ensuring against DDOS, Trojan, Virus and Spam and so on more viably than any other time in recent memory(Buyya, Yeo and Venugopal, 2008).

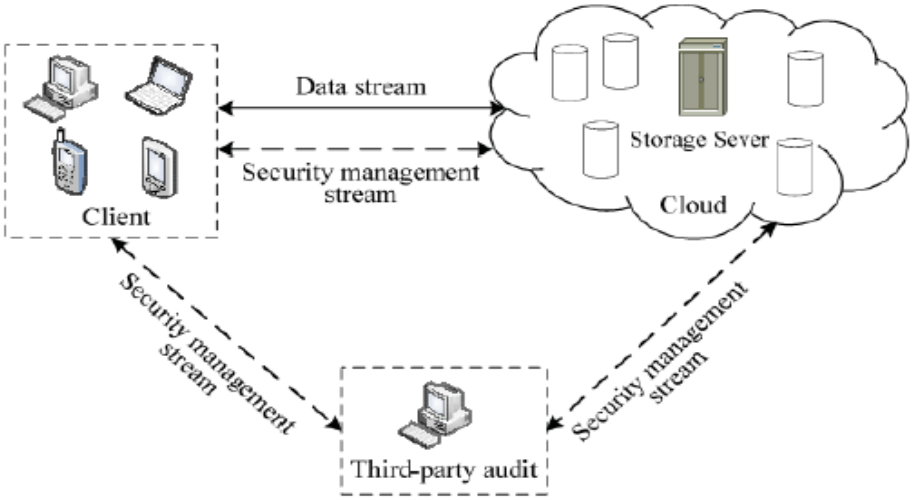

Figure 1: Data storage structure of Cloud Computing

However, the qualities of distributed storage make clients' information looked with numerous security dangers, incorporates: (1) the conventional security district parcel is invalid. On account of the distributed storage benefit must be adaptable, security limits and assurance hardware can't be unmistakably characterized, which builds some trouble for the usage of particular assurance measures; (Xiao, Song and Chen, 2013)(2) the distributed storage transmits information through the system. The benefit interferences, information devastation, data stolen furthermore, altered caused by the noxious assaults in the organize represent a serious test to the security of information correspondences, get to confirmation and classification; (Wajid *et al.*, 2015)(3) from the client's view, the distributed storage of information makes distributed computing specialist co-op gets the information get to control, and the client's information is looked with protection security dangers. Individuals stress over that the touchy individual information will be exposure, abuse or missing by putting the information in cloud condition(Xie *et al.*, 2015). To tackle the above issues, as of late, scientists made a parcel of research work in the information security to control systems, information respectability, confirmation, cipher text to recover and information encryption system of cloud figuring condition(Ardagna *et al.*, 2014).

There are lots of security issues with cloud computing because of technologies utilization including networks, operating systems, databases, resource scheduling, virtualization, load balancing, transaction management, memory management and concurrency control. For example, the network should be secure on cloud so that migration of VM to PM should be secure.(Armbrust *et al.*, 2010). Data security not only involves encrypting the data but also gives surety of appropriate policies. Cloud computing suffers from some various security concerns which are given below.

- Server & application access
- Transmission of data
- Secure VM
- Secure Network

- Security of Data
- Privacy of data
- Correctness of Data
- Location of data
- Availability of data
- Segregation of Data

1.2 Cloud Security Challenges

Some of the cloud security challenges that come in front of users are given below:

a. Authentication: The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost.
b. Access Control: To give access to only legalized users some control policies are used. These services must be adjustable, well planned, and their allocation is overseeing conveniently(Saha, Pal and Pattnaik, 2016).
c. Policy Integration: There are many cloud providers they use their own policies and approaches. Some of them are Amazon, Google who provides services to end users.
d. Service Management: In this different cloud providers such as Amazon, Google, comprise together to provide services to meet their customers need.
e. Trust Management: The trust management approach must be developed so that trust remains between both parties such as user and provide.

Cloud security is hampered by the threats which are common in cloud system. These threats are mitigated using the techniques described through the table 1

Type of Threats	Mitigation technique
VM level Threat	IDS and IPS
Abuse and nefarious	Credit card fraud monitoring and coordination.
Loss Of Governance	No proper strategy available for handling this attack
Xml Signature Element Wrapping	Utilization of digital certificate
Browser Security	XML encryption and SOAP encryption
Cloud Malware Injection Attack	Authenticity check
Flooding Attacks	Intrusion detection system is used
Isolation Failure	Authentication and access control
Data Loss Or Leakage	Encrypting and protecting integrity of data
Account Or Service Hijacking	Multifactor authentication techniques

Table 1: Types of threats and mitigation strategies.

In addition threats could lead to security problems if not tackled at early stage. The security problems could hamper the overall working of the cloud. User data may be corrupted due to the application of attacks. Various attacks along with mitigation strategies are listed in the table 2.

Type of attack	Mitigation technique	Advantage	Disadvantage
Denial Of Services	Clustering based mechanism	Reduce functionality of hijackers	Time consumed more
Authentication Attacks	Access Control	Unauthorized access control	Only utilized for frequent targets
Man in the middle attack	Block Level Parity attack	Gives better prevention	Space is more consumed
DNS attack	IP address validation	Had better performance	Rerouting processing are inadequate
Network stiffing	Encryption algorithms is used	Data is secured	Much Complex
Cross site Scripting	Validating Input	Sensitive data can be secured	Violation of user credential may occur
Cookie Poisoning	Regular cookie cleanup	Removed unauthorized accessed	Must be improved for large data
Distributed Denial of service	Deadline oriented techniques	Early detection of intruder	Used more space
SQL Injection Attack	Special character elimination using buffer allocation	Eliminate intruder	More information can not be added
Side Channel Attack	Nearest Neighbor mechanism	Secured channel using nearest neighbor	Server proxy can be hacked

Table 2: Attacks and mitigation strategies

2. 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 2018) proposed a DNA based symmetric key algorithm for providing security in cloud. Cloud security services includes 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. 2015) 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. 2018) 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 datacenter 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. 2019) 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 honeypot data so accuracy can be further enhanced.

(Shaukat and Hassan 2017) proposed an encryption strategy for cloud security that monitor the cloud server and maintain the SLA. It enhanced the availability and security of data centers. 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 handled multiple user at a time so security of cloud must be improved.

(Deshmukh 2018)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 datacenter

and also privacy preservation in public cloud. It does not considered cloud data storage that are significantly enhanced.

(Esposito et al. 2018)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. 2018)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. 2018)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. 2015) 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 datacenter. This technique provides more security.

(Awad et al. 2018)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.

Reference	Technique used	Advantage	Disadvantge
(Kudtarkar et al. 2015)	Multiple cloud storage with encryption	This technique is efficient and increases the advisory of users.	it is not implemented on live storage cloud server.
(Akhil et al. 2018)	AES based cloud security	It ensures the correctness of data and handle large amount of data. It also avoids intruder access into the cloud datacenter 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. 2019)	Cyber insurance provisioning and security	It gives increased allocation and attack detection.	It worked on honeypot data so accuracy can be further enhanced.
(Shaukat and Hassan 2017)	Encryption strategy	It enhanced the availability and security of data centers. 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 2018)	Three level protection technique	It provides more secure cloud datacenter and also privacy preservation in public cloud.	It does not considered cloud data storage that are significantly enhanced.
(Esposito et al. 2018)	Block chain based access control	The accuracy of system increased	These security strategies become critical as more and more users interact with the cloud.
(Jana et al. 2018)	Memory replication mechanism	In case of failure sensitive information can be recovered from other replicated images.	Storage space was heavily used in this approach.

(Meng et al. 2018)	Hierarchal framework	It analyzes the data in clusters and the accuracy of cluster is increased.	Storage space utilized is more.
(Singh et al. 2015)	Elliptic Curve Digital Signature Algorithm (ECDSA)	It enhances the storage and retrieval of data in cloud datacenter. This technique provides more security.	It must be optimized so that transmission process fastened.
(Awad et al. 2018)	chaos based encryption strategy	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.

Table 1: Comparative analysis of different literature corresponding to security

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.

3. Base Paper Description

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.

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

FEATURE	QUANTITY AND DESCRIPTION	PROBLEM
Number of phases	5 • 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	----

Table 2: Parametric comparison with essential and absent features

4. Progress So Far

Currently we have created a review paper and also implemented proposed system within the netbeans.

5. Methodology of propose work

The methodology 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 strategy is given in figure 1. The suggested mechanism includes phases. These phases are explained as follows

Phase 1: File Uploading

This is a 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.

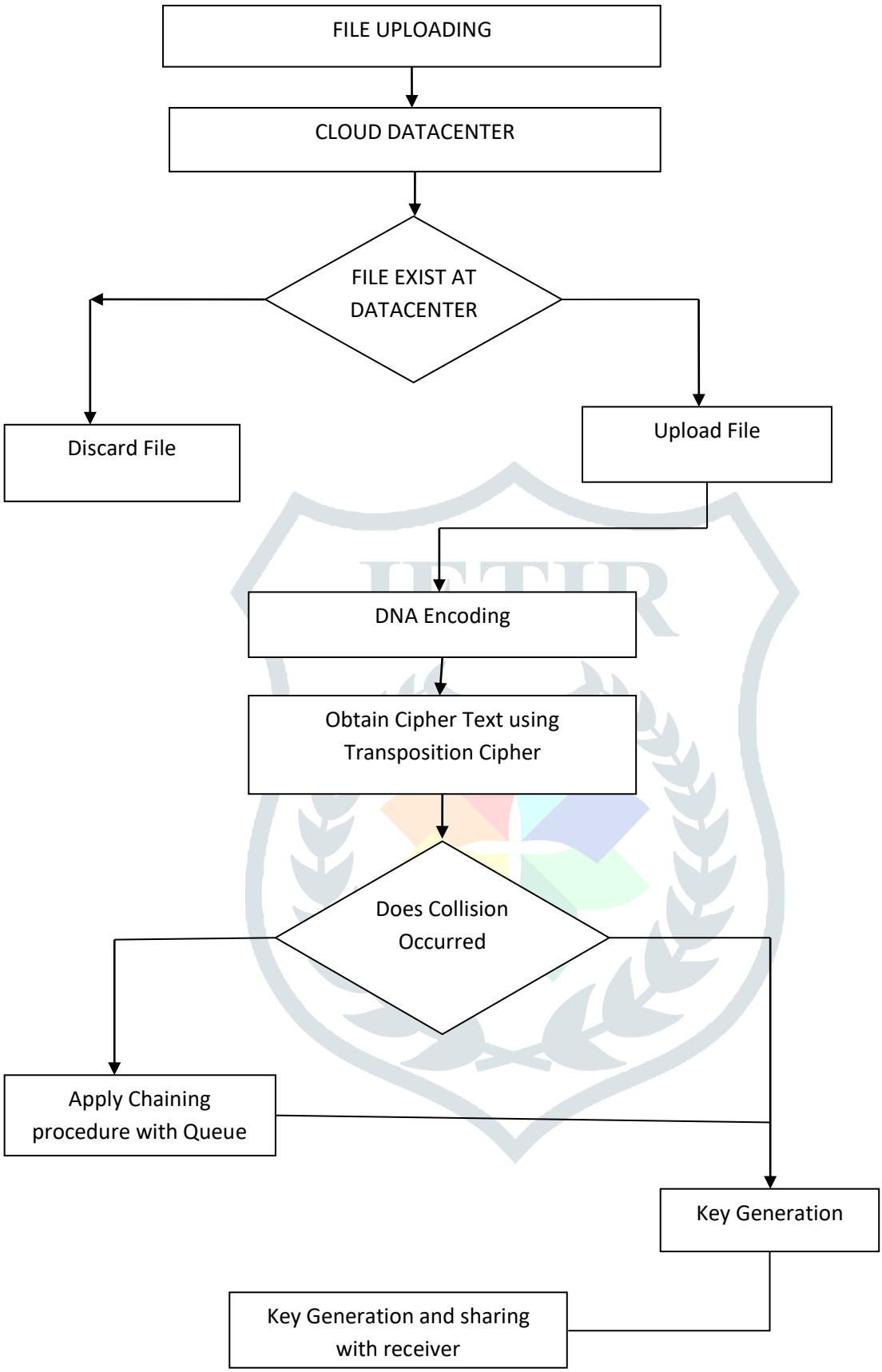

Figure 1: Flowchart for propose system using collision handling procedure

6. 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.

References

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

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

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 Secur Comput 16:565–579.doi: 10.1109/TDSC.2017.2703626

Deshmukh R (2018) Enhanced Privacy Preservation and Data Storage Security in Public Cloud. Helix 8:3726–3730 . doi: 10.29042/2018-3726-3730

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

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

Kudtarkar PP, Pagare JD, Ahire SR, Pawar TS (2015) Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment. 5:206–211

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

Shaukat K, Hassan MU (2017) Cloud computing security using encryption technique. Transylvanian Rev 25:74–82

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

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