Cloud Reliability Enhancement Using Redundancy Analysis with Homomorphic Encryption Mechanism

Vikas Mangotra[1], Richa Dogra[2]
[1]*Dept. of CSE, GCET, Gurdaspur PTU Kapurthala, Punjab, India*
[2]*Dept. of CSE, GCET, Gurdaspur, Punjab, India*

Abstract- **Information security issue is a key bottleneck limiting the utilization of cloud computing advancing and applications. Cloud encourages its clients by giving virtual resources by means of web. As the field of cloud computing is spreading the new procedures are creating. This expansion in cloud computing condition likewise builds security challenges for cloud developers. Clients of cloud spare their information in the cloud consequently and the absence of security in cloud can lose the client's trust. In this paper, number of strategies on cloud computing security issues, for example, information encryption, access control, trustworthiness validation and different issues is reviewed, on this premise, some vital specialized issues of the cloud computing information security are discussed. In this paper, uses the method to remove the redundancy of data and compress of data and also reduce the size of data. after then using homomorphic encryption with pseudo random generator to increase the security of data. All the ways are used to remove redundancy of data, compress the size of data, less execution time of data, increase security and less consumption of energy.**

Index Terms- Homomorphic encryption, Reliability, Execution time, Redundancy, Pseudo random.

I. INTRODUCTION

Cloud computing has been imagined as the cutting edge worldview in computation. In the cloud computing condition, the two applications and resources are conveyed on request finished the Internet as administrations. [1]Cloud is an environment of the software and hardware resources in the server farms that give different administrations over the system or the Internet to fulfil client's prerequisites.

[2]Service based cloud computing is a critical type of the data framework in the Internet era, which receives new plan of action to give elite, ease computing and information administrations, supporting a wide range of data application. Alongside the fast advancement and utilization of this new system innovation, new security issues show up continually, and turn into a critical factor in limiting mechanical improvement. [3]Combined with the promotion of cloud computing, and the extending comprehension of cloud computing, the security issue has turned into the greatest worry in the utilizing cloud computing and the relocation to cloud computing. In the event that the bottleneck issue of cloud computing security can't be settled, cloud computing innovation is hard to complete the modern overhauling and application advancement. [4]

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 [5]Following cloud computing security examine in the academics group, a few specialists have started to focus on cloud computing security issues, however most by far of writing still stay in the examination of cloud computing organizations, administrations, applications and other related issues, and profundity inquire about on cloud computing security issues has not yet initiated, and the key security issues like information protection assurance identified with cloud computing are still absence of help of fundamental hypothesis and successful innovation. [6]

[7]Cloud computing can be considered as another computing model that can give benefits on request at a negligible cost. The three surely understood and usually utilized administration models in the cloud worldview are software as an administration (SaaS), platform as an administration (PaaS), and infrastructure as an administration (IaaS). In SaaS, software with the related information is conveyed by a cloud specialist co-op, and clients can utilize it through the web programs. In PaaS, a specialist co-op encourages administrations to the clients with an arrangement of programming programs that can comprehend the particular assignments.[8] In IaaS, the cloud specialist infrastructure encourages administrations to the clients with virtual machines and capacity to enhance their business abilities. In this paper we examine the security issues identified with cloud computing model. The primary objective is to think about various sorts of assaults and systems to secure the cloud display.[9]

In cloud computing situations, the typical data transmission and capacity mode is appeared in Figure 1:

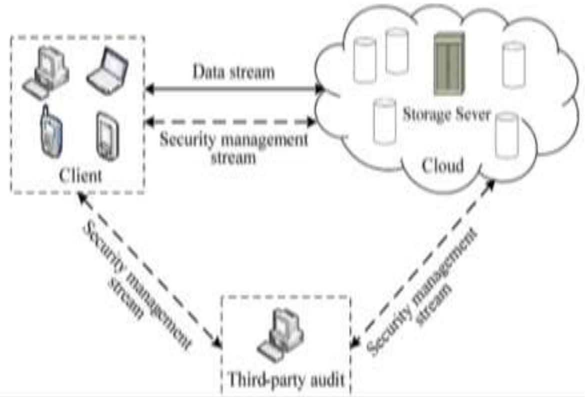

Data stream
Security management stream
Storage Sever
Cloud
Client
Security management stream
Security management stream
Third-party audit

Figure 1: Data storage structure of Cloud Computing[5]

The viable assurance of client protection data is the essential issue of cloud security. [2]From the above figure, we can see that cloud computing stores a substantial number of data records on the far off servers, and clients can lessen the weight of capacity and calculation, at that point appreciate the adaptable and productive administration brought by cloud computing. Be that as it may, the attributes of cloud stockpiling make clients' data looked with numerous security dangers, incorporates: (1) the customary security district parcel is invalid. In view of the cloud stockpiling administration must be adaptable, security limits and assurance gear can't be obviously characterized, which expands some trouble for the usage of particular insurance measures; (2) the cloud stockpiling transmits data through the system.[10] The administration intrusions, data obliteration, data stolen and altered caused by the pernicious assaults in the system represent an extreme test to the security of data correspondences, get to confirmation and classification; (3) from the client's view, the cloud stockpiling of data makes cloud computing specialist co-op acquires the data get to control, and the client's data is looked with protection security dangers. Individuals stress over that the touchy individual data will be exposure, abuse or missing by putting the data in cloud condition. [11]To understand the above issues, lately, analysts made a ton of research work in the data security get to control systems, data trustworthiness, confirmation, cipher text to recover and data encryption procedure of cloud computing condition.

A. Cloud Security Issues

[12]Organization utilizes different cloud benefits as IaaS, PaaS, SaaS and the models like open, private, crossover. These models and services have different cloud security issues. Each services show is related with a few issues. Security issues are considered in two perspectives first in the perspective of specialist co-op who guarantees that services gave by them ought to be secure and furthermore deals with the client's character administration. [13]Other view is client see that guarantees that administration that they are utilizing is sufficiently secure.

a) Multi-Tenancy- A cloud environment is build for reasons like sharing of resources, memory, storage and shared computing. Multi-tenancy gives proficient use of resources, keeping cost lower. [14]It infers sharing of computational resources, service storage and application with different occupants dwelling on same physical/consistent stage at supplier's premises. In this way it damages the secrecy of data and results in leakage of data and encryption and increment the likelihood of assaults.

b) Elasticity- Elasticity is characterized as how much a framework can adjust to workload changes by provisioning and unhinged resources in an autonomic way, with the end goal that the accessible resources coordinate the present request whenever as nearly as would be prudent.

Versatility suggests adaptability. [15]It says that customers can scale all over as required. This scaling empowers occupants to utilize an asset that is relegated beforehand to other inhabitant. However this may prompt secrecy issues. SaaS Software as a Service: Complete applications, adjustable inside points of confinement, understanding particular business needs, with centre around end-clients prerequisites PaaS Platform as a Services: No compelling reason to straightforwardly oversee OS, databases, and so on. Programming interfaces for building larger amount applications. [16]Pre-fabricated applications segments. IaaS Infrastructure as an administration: No compelling reason to buy or oversee physical data focus equipment (servers, storage, organizing, and so on.) oversee.

c) Insider assaults Cloud show is a multitenant based model that is under the supplier's single service area. [17]This is a risk that emerges inside the association. There are no contracting norms and suppliers for cloud representatives. So an outsider seller can without much of a stretch hack the data of one association and may degenerate or pitch that data to other association.

d) Outsider Attacks- This is the one of the major concerning issue in an association since it discharges the private data of an association in open. Clouds dislike a private system; they have a larger number of interfaces than private system. So programmers and aggressors have preferred standpoint of abusing the API, shortcoming and may complete an association breaking .These attacks are less hurtful than the insider attacks on the grounds that in the later we in some cases unfit to recognize the attack.[18]

e) Loss of control- Cloud utilizes transparent area locations by which it empowers associations to uninformed about the area of their administrations and data. Thus supplier can have their services from anyplace in the cloud. For this situation association may lose their data and perhaps they don't know about security instrument set up of the provider.[19]

f) Data Loss- As in cloud, there are different occupants, data honesty and wellbeing couldn't be given. Data loss can brings about money related, client check misfortune for an association. An essential case of this can be refreshing and erasure of data without having any reinforcement of that data. [20]

g) Network security- Network security is divided in following manner:

1. Man in middle attack:- In this attack, attacker makes a free association and speaks with the cloud client on its private system where all control is in the hand of assailant.
2. Distributed denial of service attack: - In DDOS attack, servers and systems are brought around an enormous measure of system activity and clients are denied the entrance to a specific Internet based Service.[20]
3. Port Scanning:- Port is a place from where data trade happens. Port examining is occurring when endorser designs the gathering. Port checking is done naturally when you design the web so this disregards the security concerns.
4. Malware Injection Attack Problem- In cloud computing, a considerable measure of data is exchanged between cloud supplier and shopper, there is a need of client confirmation and approval. At the point when the data is exchanged between cloud supplier and client, attacker can bring malicious code into it. Accordingly, the first client may need to hold up until the culmination of the activity that was noxiously presented.
5. Flooding Attack Problem In cloud, there is a no. of servers that speak with each other and exchange data. The solicitations is handled, the asked for occupations are verified to start with, yet this verification requires a considerable measure of CPU use, memory lastly because of these server is over-burden and it passes its offload to other server. By this the standard handling of framework is interfered, and the framework is overflowed.

B. Techniques to Secure data in Cloud

a) a)Authentication and Identity- Authentication of clients and even of imparting frameworks is performed by different strategies, yet the most well-known is cryptography. Validation of clients happens in different routes like as passwords that is known separately, as a security token, or in the shape a quantifiable amount like unique mark. One issue with utilizing conventional personality approaches in a cloud situation is confronted when the endeavour utilizes different cloud specialist organizations (CSPs). In such utilization case, synchronizing personality data with the venture isn't adaptable. Different issues emerge with customary personality approaches while relocating framework toward a cloud-based arrangement.

b) Data Encryption- If you are intending to store touchy data on a huge data store then you have to utilize data encryption strategies. Having passwords and firewalls is great, yet individuals can sidestep them to get to your data. At the point when data is encoded it is in a shape that can't be perused without an encryption key. The data is absolutely pointless to the gatecrasher. It is a method of interpretation of data into mystery code. On the off chance that you need to peruse the scrambled data, you ought to have the mystery key or secret key that is likewise called encryption key.

c) Information respectability and Privacy- Cloud computing gives data and resources to legitimate clients. Resources can be gotten to through web programs and can likewise be gotten to by malicious attacker. An advantageous answer for the issue of data trustworthiness is to give shared trust amongst supplier and client. Another arrangement can be giving legitimate validation, approval and bookkeeping controls so the way toward getting to data ought to experience different multi levels of checking to guarantee approved utilization of resources. Some secured get to systems ought to be given like RSA endorsements, SSH based passages.

d) Availability of Information- Non accessibility of data or data is a noteworthy issue with respect to cloud computing administrations. Service Level agreement is utilized to give the data about whether the system resources are accessible for clients or not. It is a trust bond amongst purchaser and supplier. An approach to give accessibility of resources is to have a reinforcement anticipate neighbourhood resources and for most critical data. This empowers the client to have the data about the resources even after their inaccessibility.

e) Secure Information Management- It is a system of data security for a gathering of data into focal store. It is involved specialists running on frameworks that are to be checked and afterward sends data to a server that is called "Security Console". The security comfort is overseen by administrator who is a person who surveys the data and takes activities in light of any cautions. As the cloud client base, reliance stack increment, the cloud security instruments to understand security issues additionally increment, this makes cloud security administration significantly more confounded. It is likewise considered as a Log Management. Data Security Management Maturity is another model of Information Security Management System.

f) Malware-injection attack solution- This arrangement makes a no. of customer virtual machines and stores every one of them in a focal stockpiling. It uses FAT (File Allocation Table) comprising of virtual working systems. The application that is controlled by a customer can be found in FAT table. Every one of the cases are overseen and planned by Hypervisor. IDT (Interrupt Descriptor Table) is utilized for trustworthiness checking.

g) Flooding Attack Solution- All the servers in cloud are considered as an armada of servers. One armada of server is considered for framework composes demands, one for memory administration and last one for centre calculation related occupations. Every one of the servers in armada can speak with each other. When one of the server is over-burden, another server is brought and utilized as a part of the place of that server and an another server that is called name server has all the record of current conditions of servers and will be utilized to refresh goals and states. Hypervisor can be utilized for overseeing jobs. Hypervisor additionally do the approval and confirmation of occupations. An approved client's demand can be distinguished by PID. RSA can likewise be utilized to scramble the PID.

C. Cloud Computing Security Standards

Measures for security characterize method and procedures for executing a security program. To keep up a safe situation, that gives protection and security some particular advances are performed by applying cloud related exercises by these benchmarks. An idea called "Protection in Depth" is utilized as a part of cloud to give security. This idea has layers of guard. Along these lines, on the off chance that one of the frameworks comes up short, covering method can be utilized to give security as it has no single purpose of failure. Customarily, endpoints have the method to look after security, where get to is controlled by client.

a) Security Assertion Markup Language (SAML)- SAML is fundamentally utilized as a part of business bargains for secure correspondence between online accomplices. It is a XML based standard utilized for verification, approval among the accomplices. SAML characterizes three parts: the central (a client), a specialist co-op (SP) and a personality supplier (IDP). SAML gives questions and reactions to indicate client properties approval and verification data in XML organize. The asking for party is an online webpage that gets security data.
b) Open Authentication (OAuth)- It is a strategy utilized for interfacing with secured data. It is essentially used to give data access to designers. Clients can give access to data to engineers and shoppers without sharing of their personality [3]. OAuth does not give any security without anyone else's input in reality it relies upon different conventions like SSL to give security.
c) OpenID- OpenID is a solitary sign-on (SSO) technique. It is a typical login process that enables client to login once and afterward utilize all the taking part frameworks [3]. It doesn't found on focal approval for verification of clients.
d) SSL/TLS- SSL/TLS is utilized to give secure correspondence over TCP/IP. TLS works in essentially three stages: In first stage, transaction is done between customers to distinguish which figures are utilized. In second stage, key trade calculation is utilized for verification. These key trade calculations are open key calculation. The last and third stage includes message encryption and figure encryption.

II. RESEARCH GAP

The techniques analysed worked on execution time reduction and safely storage if information over the cloud. The space conservation however is not considered. In other words there could be multiple keys which are generated for same information. In cloud cost is encountered on the basis of pay per use. This cost can be minimised by the use of space conservation mechanism. Redundancy handling mechanism along with homomorphic filtering can ensure efficient storage and space conservation mechanism. The Security of data is less.

III. PROBLEM DEFINATION

Cloud computing is the need of the hour and used heavily now days by almost every organization due to practically infinite resources provided by it. As the users of cloud increase so does the threats. malicious users can corrupt the data. Also cloud is vulnerable to attacks like DDOS. In order to tackle the issue space conservation and encryption could be a solution that is partially handled in existing literature using homomorphic encryption. Redundancy handling mechanism however is missing. Problems formulated from existing literature is listed as under

a) Encryption process becomes weekend through the application of redundancy and less security of data.
b) Space conservation mechanism is missing
c) Cost of storage and energy consumption enhanced greatly by the use of existing literature

IV. OBJECTIVES OF STUDY

Cloud security is of prime concern and enhancement procedure is suggested in the proposed literature. Introducing redundancy handling to minimise storage requirement and to enhance efficiency of homomorphic encryption. Cost associated with the overall system can be further reduced as storage requirement is minimised. And the consumption of energy is also reduced. The security of data is improved .

Parameter Consideration for optimization

A. Space Utilization

Equation used for this purpose

Space_Utilization=Task size/Total space

B. Execution time

This is the time required to execute entire task over the cloud

Execution_Time=Finish time - End time

C. Energy Consumption

Energy Consumed = Power Req. To Execute the Job / Total No. Of Jobs

D. Reliability

This parameter is obtained from the execution time observed in case of existing and proposed literature. Since reliability is a indirect metric hence it will be evaluated from the above two factors.

V. PROPOSED METHOLOGY

The methodology describes the steps to be followed in order to enhance the existing literature

```
Input: Cloudlets
Output: Space Utilized, Execution Time
Load the data from local client
File=load(Path)
Check for redundancy from within the file(SPECIAL DOMAIN)
For i=1:size(file)
End of for
For i=1:Word.length
End of for
Apply homorphic encryption on file
For i=1:length (final file)
Encrypted file= homophoric (final filei)
Apply Pseudo random number generator on Encrypted file
Generate Key and obtain Data.
End of for
```

VI. RESULTS

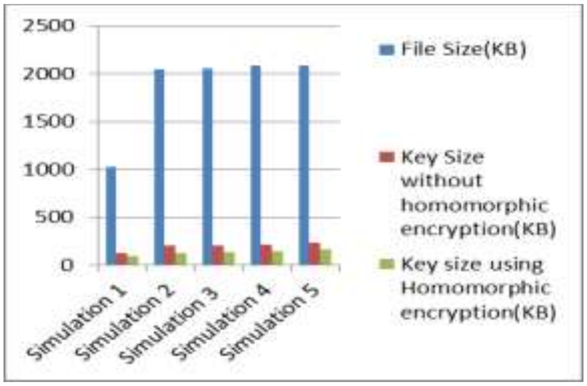
Because Since the size of the key is reduced hence storage space efficiency is achieved. Execution time is reduced considerably reduced by the use of said methodology and increase the security .these methods also reduce the consumption of energy. The results in terms of table and plots are given as follows:

The results in terms of table and plots are given as follows:

In terms of key size

Simulation	File Size(KB)	Key Size without homomorphic encryption(KB)	Key size using Homomorphic encryption(KB)
Simulation 1	1024	128	100
Simulation 2	2048	200	123
Simulation 3	2056	201	135
Simulation 4	2089	215	145
Simulation 5	2090	230	160

Table 1: Comparison in terms of key size

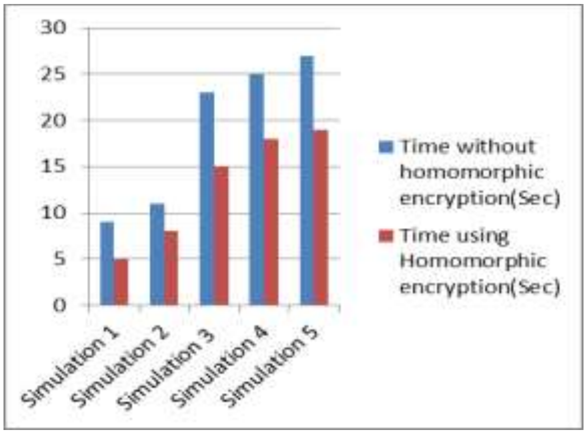


From the pot it is clear that key size is subsequently reduced by the use of homomorphic encryption.

In term of time consumed

Simulation	File Size(KB)	Time without homomorphic encryption(Sec)	Time using Homomorphic encryption(Sec)
Simulation 1	1024	9	5
Simulation 2	2048	11	8
Simulation 3	2056	23	15
Simulation 4	2089	25	18
Simulation 5	2090	27	19

Table 2: Comparison in terms of time consumed

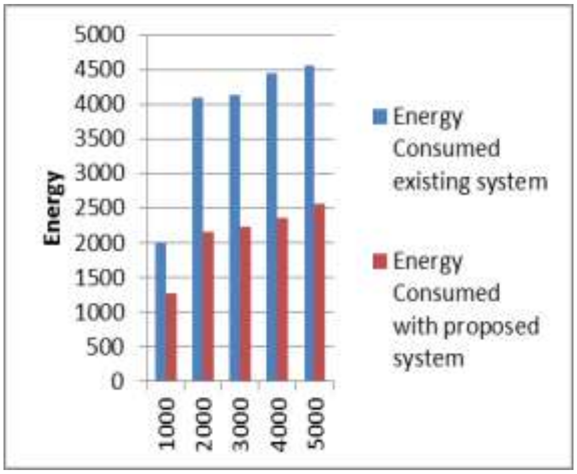


Time consumption also greatly reduced by the use of homomorphic encryption methodology.

Energy Consumption

Energy Consumed (Existing System)		Energy Consumed (Proposed System)
1	2000	1258
2	4096	2150
3	4135	2220
4	4450	2365
5	4565	2554

Table 3: Cloudlet Energy Consumed of existing and proposed system



Result shows improvement by the significant manner by the considered approach.

VII. CONCLUSION

This paper describes a portion of the cloud ideas and shows the cloud properties, like versatility, stage free, minimal effort, flexibility and unwavering quality. In this paper ,firstly to remove the redundancy of the data and any unauthentic thread. In spite of the fact that there are different security challenges in cloud computing however in this paper, we have talked about some of them and furthermore the systems to anticipate them, they can be utilized to keep up the protected correspondence and evacuate the security issues. The security of data is very high to use the homomorphic encryption with the pseudo random generator. This study is fundamentally done to consider every one of the issues like assaults, data misfortune and unauthenticated access to data and furthermore the strategies to evacuate those issues. The size of the data is compressed using spatial domain method and data consume less storage .The Execution time is less in this paper and the process consume less energy consumption. The surety of the processing od data is high using this methology.

REVIEW PAPER PUBLISHED

"Cloud reliability enhancement mechanisms: A Survey" Vikas Mangotra1 Richa Dogra2 Section: Survey Paper, Product Type: Isroset Journal Vol.6 , Issue.3 , pp.31-34, Jun-2018

REFERENCES

[1] D. M. X. Zhang, Z. Huo, Jie Ma, "Exploiting Data Deduplication to Accelerate Live Virtual Machine Migration," IEEE Int. Conf. Clust. Comput., pp. 88–97, 2010.

[2] R. Miguel, "HEDup: Secure Deduplication with Homomorphic Encryption," in 2015 IEEE International Conference on Networking, Architecture and Storage (NAS), 2015, pp. 215–223.

[3] "Error Characterization, Mitigation, and Recovery in Flash-Memory-Based Solid-State Drives," IEEE, vol. 105, no. 9, pp. 1666–1704, 2017.

[4] G. Zhu, X. Zhang, L. Wang, Y. Zhu, and X. Dong, "An Intelligent Data De-duplication Based Backup System," in 2012 15th International Conference on Network-Based Information Systems, 2012, pp. 771–776.

[5] Vikas Mangotra, Richa Dogra "Cloud reliability enhancement mechanisms: A Survey", International Journal of Scientific Research in Computer Science and Engineering Vol.6, Issue.3, pp.31-34 , June (2018)

[6] Y. Hua, X. Liu, and D. Feng, "Cost-Efficient Remote Backup Services for Enterprise Clouds," IEEE Trans. Ind. Informatics, vol. 12, no. 5, pp. 1650–1657, 2016.

[7] T. Knauth, "VeCycle : Recycling VM Checkpoints for Faster Migrations," pp. 210–221.

[8] T. Lu, M. Stuart, K. Tang, and X. He, "Clique Migration : Affinity Grouping of Virtual Machines for Inter-Cloud Live Migration," 2014.

[9] Y. Zhao and S. S. M. Chow, "Updatable Block-Level Message-Locked Encryption," ACM, pp. 449–460, 2017.

[10] L. Gupta, M. Samaka, R. Jain, A. Erbad, D. Bhamare, and H. A. Chan, "Fault and Performance Management in Multi-Cloud Based NFV using Shallow and Deep Predictive Structures," Springer, 2017.

[11] C.-N. Yang and J.-B. Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing," in 2013 International Symposium on Biometrics and Security Technologies, 2013, pp. 259–266.

[12] D. Chen, “Data Security and Privacy Protection Issues in Cloud Computing,” Int. Conf. Comput. Sci. Electron. Eng. Data, no. 973, pp. 647–651, 2012.

[13] J. I. A. You, Z. Zhong, G. Wang, B. O. Ai, and S. Member, “Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors,” IEEE Access, vol. 2, 2014.

[14] J. Aikat, N. Carolina, J. S. Chase, A. Juels, C. Tech, T. Ristenpart, and C. Tech, “Rethinking Security in the Era of Cloud Computing,” no. June, 2017.

[15] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, “Security transparency : the next frontier for security research in the cloud,” J. Cloud Comput., 2015.

[16] H. Hammami, H. Brahmi, and I. Brahmi, “A Security Approach for Data Migration in Cloud Computing Based on Human Genetics,” pp. 384–396, 2017.

[17] S. Rajput and A. C. Computing, “International Journal of Advanced Research in Computer Science and Software Engineering Live-VM Migration Policies, Attacks & Security – A Survey,” vol. 4, no. 2, pp. 366–373, 2014.

[18] S. Kaushik, “Cloud data security with hybrid symmetric encryption,” pp. 0–4, 2016.

[19] A. Ibrahim, H. Jin, A. A. Yassin, D. Zou, and P. Xu, “Towards Efficient Yet Privacy-Preserving Approximate Search in Cloud Computing,” IEEE Access, vol. 57, no. 2, 2014.

[20] K. Govinda and E. Sathiyamoorthy, “Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud,” Procedia Technol., vol. 4, pp. 495–499, 2012.