Implementation of Secure Encrypted Cloud in Perception of Data Security

Sunil Kumar[a] and Gaurav Aggarwal[b]

[a] Research Scholar, Department of CSE, Jagannath University, Bahadurgarh, Jhajjar (Haryana)

[b] Professor, Department of CSE, Jagannath University, Bahadurgarh, Jhajjar (Haryana)

Abstract: In today's digital age, the growing dependency on cloud storage has brought data security to the forefront of technological concerns. This paper explores the implementation of secure encrypted cloud systems to enhance data confidentiality, integrity, and user trust. Cloud computing, while offering scalable and cost-effective data management, poses critical risks due to potential data breaches, unauthorized access, and privacy violations. The implementation of end-to-end encryption, homomorphic encryption, and robust key management techniques are examined as core strategies to safeguard data. Furthermore, the study delves into the perception of users regarding cloud security, highlighting the correlation between security mechanisms and user adoption. By integrating advanced encryption methods with transparent security protocols, a secure cloud environment can be established that aligns with user expectations and regulatory standards. The findings emphasize that encryption not only protects data but also significantly influences user confidence in cloud technologies.

Keywords: - Cloud computing, Cryptography, Encryption, Decryption, Cipher Text, DES.

Introduction:

Cloud computing Security has been considered a basic issue. Information in cloud require to be collected in form of encryption. In order to limit user access of secret information the proxy and brokerage services must be used. Users need to make analyses of several aspects of resource before deploying a exacting resource to cloud which are as follow:

1. Choose the resource that requires shifting to cloud & make analyses of its sensitivity to challenges.
2. Taking cloud service models in account as IaaS, PaaS, & SaaS. Models need customer to be accountable for protection at several levels of service.
3. The different Cloud to be used for example private, public, community or hybrid should be considered.
4. Making understanding of cloud service provider system. Considering information storage & out of cloud & its transfer into.
5. The risk in cloud deployment basically is based on service models and different kind of cloud.

CLOUD COMPUTING SECURITY

Because information is communicated via Internet, data security is must in cloud. Following are known to be key mechanisms to keep the data safe and protected.

a) Auditing
b) Access Control
c) Authorization
d) Authentication

Every service model may consider the security mechanism which has been operating in case of above stated areas.

The third parties provide information and system management for cloud computing as of cloud privacy is major issue. To deliver important information in the direction of cloud service provider becomes a big problem. Violation could make loss of user or occupation .thus the venders give security.In the background of cloud data is transferred rapidly over internet therefore safety of data is always kept in mind. Several customers' data may be affected because they are using the infected cloud for distribution of data. Integrity of data consists of situations when some human errors are made, while feeding data. Errors could take place during information is transferred from one system to another. Sometime errors occur due to hardware malfunctions such as crashing hard drives. Authentication is the most essential procedure to ensure the cloud data in a secured manner. However, strong user authentication is the main requirement for cloud computing that reduces the unauthorized user access of data on cloud. Data security is a more important issue of cloud computing. Thus, the need to ensure the safety of information that being exchanged between the users and the cloud became more significant. Many security and authentication techniques have been proposed to secure the exchanged data. These techniques aim to keep the authentication, privacy and reliability levels of data. Here in this survey paper, I have presented security algorithms in cloud computing. Database and web contents are hosted on cloud server and accessed via network connection. So there are the chances of attacking or hacking of data during transmission. Web programming is made using client side script and server side script. Cloud server based hosting has

been provided to host web services. These services are made available to user on requirement via Internet. Cloud server hosting services has been supplied with the integration of multiple connected servers. There are different type of attacks which are performed to attack or hack the sensitive data during it transmission. In modern cloud hosting multiple physical machine are connected for cloud based hosting. This cloud host supports web hosting as well as email hosting. The net banking is one of the examples of session based login. Session is generated when user logins. Such session distinguish user from another user. The session hijacking attack in such system would make the un authentic user capable to manipulate or destroy confidential information of user. It has been seen there is time limit of particular session. But some time attacker could attack during this time. Session get generated when user login in to cloud. Intruder captures access & ability to do anything. He could access information like authorized user Hacker could steal authorized user log in by capturing his session ID. There are different techniques which are proposed to secure cloud services such as RSA, AES, DES, FLOW FISH, MD5, Multiplicative inverse etc. But these encryption have their own limitations.

Security is biggest problem of cloud computing. Many Research paper discuss about cloud and its advantage and disadvantage. In my Literature review I found security is major key point. From the Literature Review I found Holomorphic encryption is the more secure encryption scheme. In this scheme cloud server can perform any algebraic operation on cipher data. From literature Review I found that Chosen Cipher text attack is major problem.

Multiplicative Holomorphic Encryption

In Multiplicative Holomorphic encryption Multiplication of encrypted cipher text is same as Multiplication of original plain text. This property allows you to apply Multiplication on encrypted data without knowing original data.

RSA and Elgamal cryptosystems realize the properties of the multiplicative Holomorphic encryption. The client sends the pair (C1, C2) to the Cloud server and server performs the calculations requested by the client and sends the encrypted result (C1 × C2) to the client.

If the attacker intercepts two ciphers C1 et C2, which are encrypted with the same private key, so they are able to decrypt all messages exchanged between the server and the client. Because the Holomorphic encryption is multiplicative, i.e. the product of the ciphers equals the cipher of the product.

The basic RSA algorithm and Paillier Cryptosystem is vulnerable to chosen cipher text attack (CCA).CCA is defined as an attack in which adversary chooses a number of cipher text and is given the corresponding plaintext, decrypted with the target's private key. Thus the adversary could select a plaintext, encrypt it with the target's public key and then be able to get plaintext back by having it decrypted by private key. So attacker will know the entire data in-between client and cloud server.

Proposed System:

To prevent cipher data from CCA (chosen cipher text attack) I propose Proxy Re-Encryption algorithm with paillier and RSA Cryptosystem. In Holomorphic encryption scheme data was encrypted by the private key and public key was kept with client only. We again pass that data in proxy re-encryption algorithm and get every time random key generated cipher data. If attacker gets that key ones then they need to decrypt that data twice with two different keys. If once attacker gets the plaintext than he is not able to get every plaintext between client and server. So this system provides more security than existing system.

Key generation:

1. Choose two large prime numbers p and q randomly and independently of each other such that gcd (pq ,(p-1)(q-1))=1.
2. Compute n=pq and λ=lcm (p-1, q-1).
3. select random integer g where g Є Z*n2
4. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: μ=(L(a λ mod n2))-1 mod n, where function is defined as L(u)=u-1/n.
5. The public (encryption) key is. (n,g)
6. The private (decryption) key is (λ, μ)

Encryption:

Enc (m, pk)

1. Let m be a message to be encrypted where m Є Zn.
2. Select random where r Є Zn*.
3. Compute ciphertext as: c=gm . rn mod n2.

Proxy Re-Encryption(c)

1. Compute Private and Public key.(Rsk,Rpk).
2. Re Encrypt Ciphertext generated by Paillier algorithm and send Public key (Rpk) to cloud server.

Decryption: Dec(c,sk)

1. Ciphertext c Є Zn2*.

2. Compute message: m=L(c λ mod n2)/ L (g λ mod n2). Mod n

The Need for Improvement in Cloud Security

There is a requirement for development in cloud security dependent on the reactions underneath, were 72% of respondents said Yes and just 28% say No who are of the conviction that no need of progress.

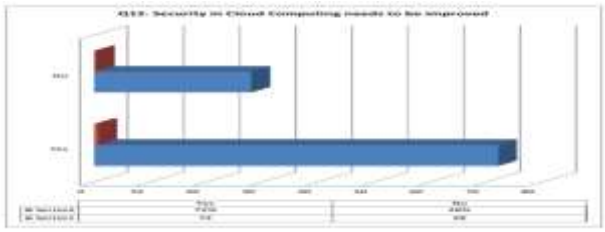


Figure: Improvement in Cloud Security (Q12)

The Issue of Adherence to Data Security Control

On the Issue of Adherence to Data Security Control as concurred in Services Level Agreements (SLA) the reactions from respondents is that 16% said Yes, 49% said No and 35% of the respondent addressed Maybe, that is to say they don't know on whether the Cloud Service Provider comply to such understanding rigorously or not.

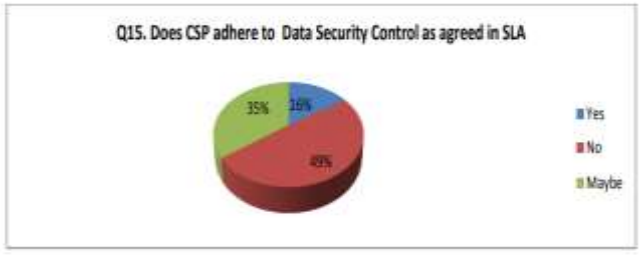


Figure: CSP adherence to Data Security Control as agreed in SLA (Q15)

Cloud Service Providers (CSP) Perspective and Users Perspective

On the security worries with respect to relationship from Cloud Service Providers (CSP) Perspective and Users Perspective, both the suppliers and clients are having related worries as far as Data and Information Storage. Most particular the protection and security issues, so reactions are introduced after investigation of the Question from the Survey structure which shows 62% of the reacted consider there is solid direct relationship from the two players and 38% are of the assessment of in a roundabout way related as displayed in the figure beneath

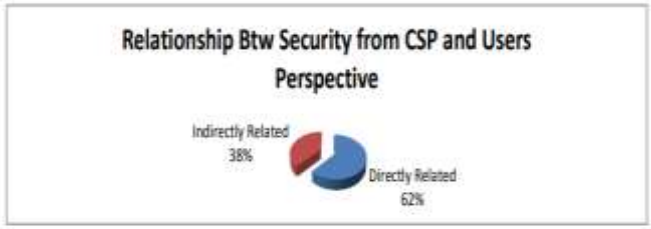
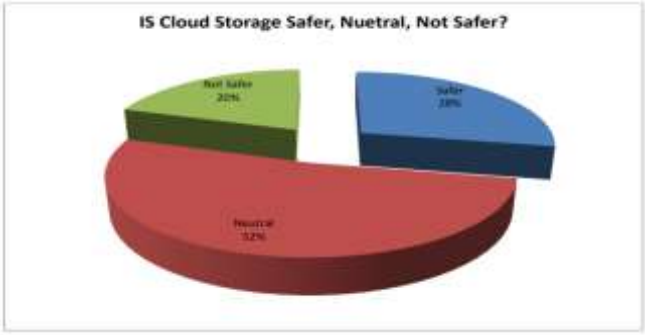


Figure : Relationship between Security from CSP and Users Perspective

Safeness of Cloud Computing

Besides, as talked about in the past section, on the legitimacy of data that is put away in the cloud computing climate is more secure or not more secure and climate there is a requirement for further developed security in the cloud computing security for the most part to support clients in receiving the technology and surprisingly complete relocation to accomplish a portion of the utilization and advantage got from the cloud technology. Reactions are given as 28% accept whatever that is put away in cloud is more secure, 20% think the data isn't protected and about 52% are nonpartisan because of the affectability and nature of the whole Cloud Architecture.



The need for Improvement in General Security of Cloud Computing

On the requirement for cloud computing general security to be further developed dependent on the poll overview 73% of the respondent said there is a need to work on the security to empower client's appropriation and execution of cloud computing technology, just 27% of the respondents consider the security is typical. Which dependent on the scientists assessment are the little clients who are as of now utilizing the cloud computing technology for data stockpiling.

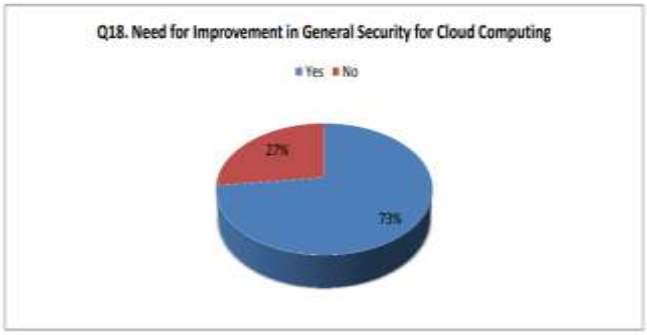


Figure: The need for improvement in General Security of Cloud Computing (Q18)

Conclusions:

In this paper I have use Homomorphic encryption technique to provide security on cloud. Homomorphic encryption is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. In this paper I have proposed RSA and Paillier algorithm for homomorphic encryption using proxy-Re-encryption algorithm that prevents cipher data from Chosen Cipher text Attack (CCA). So, this system is more secure than existing system. In future we can optimize more efficiency of the system by reducing size of the key and we can also check proxy Re-Encryption method for other Homomorphic Encryption Scheme.

In this work, another the capacity and recovery with access control has been proposed and executed utilizing spatio-

worldly limitations for giving dynamic and got cooperation in cloud. This gives dynamic and got joint effort and reasonable access control arrangements utilizing new spatio-fleeting imperatives to improve the security adequately. The presentation investigation shows that this proposed work demonstrates that the proposed calculation gives more security and burns-through less energy than the current frameworks.

References:

1. A. Bhardwaj, V. K. Singh, Vanraj, and Y. Narayan, "Analyzing BigData with Hadoop cluster in HDInsight azure Cloud," 12th IEEE Int. Conf. Electron. Energy, Environ.
2. Aaron Zimba, Chen Hongsong, Wang Zhaoshun(2021) An Integrated State Transition-Boolean Logic Model for Security Analysis in Cloud Computing 2016 First IEEE International Conference on Computer Communication and Internet
3. AL-MuseelemWaleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.
4. Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil (2015) Cloud Computing – A market Perspective and Research Directions I.J. Information Technology and Computer Science, 2018
5. Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil (2023) Cloud Computing – A market Perspective and Research Directions I.J. Information Technology and Computer Science, 2023
6. Babitha. M. P, K.R. RemeshBabu, "Secure Cloud Storage Using AES Encryption", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), ©2016 IEEE.
7. BurhanUl Islam Khan, Rashidah F. Olanrewaju, AsifaMehraj Baba(2019) Secure-Split-Merge Data Distribution in Cloud Infrastructure, IEEE Conference on Open Systems (ICOS), August 24-26, 2015
8. Dharma P. Agrawa(2023) – "Recent Advances in Mobile Cloud Computing", Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 5895817, 1 page.
9. G.M.Nasira, Thangamani(2016) Securing Cloud Database By Data Fusing Technique (DFT) Using Cloud Storage Controller (CSC), 2017 IEEE International Conference on Advances in Computer Applications (ICACA)
10. Jianghong Wei, Wenfen Liu, Xuexian Hu(2018) Secure Data Sharing in Cloud Computing Using
11. Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791.
12. Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2022, pg.786 – 791.
13. MajedAlsanea 2022 "Factors Affecting the Adoption of Cloud Computing in Saudi Arabia"s Government Sector"
14. Manpreet Kaur, Hardeep Singh (2015) A review of cloud computing security issues International Journal of Advances in Engineering and Technology, June, 2018.
15. ManpreetKaur, Hardeep Singh (2023) A review of cloud computing security issues International Journal of Advances in Engineering and Technology, June, 2015.
16. Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2018.
17. P. R. Merla and Y. Liang, "Data analysis using hadoop MapReduce environment," Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017, vol. 2018–Janua, pp. 4783–4785, 2018.
18. Raj Kumar(2022) Research on Cloud Computing Security Threats using Data Transmission International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015 ISSN: 2277 128X
19. Raj Kumar(2024) Research on Cloud Computing Security Threats using Data Transmission International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015 ISSN: 2277 128X
20. SakshiChhabra, Ashutosh Kumar Singh(2016) Dynamic Data Leakage Detection model based approach for Map Reduce Computational Security in Cloud,
21. Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. Kailash D. Kharat,(2017) "Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques"