Privacy Security in Cloud Computing

Pooja Kanjalkar[1] Prajkta Thakre[2] Namrata Patil[3] Shriechha Kumre[4] Dhruva Kothari[5]
[1,2,3,4,5]Department of Computer Science and Engineering
[1,2,3,4,5]GCOEN, Nagpur, India

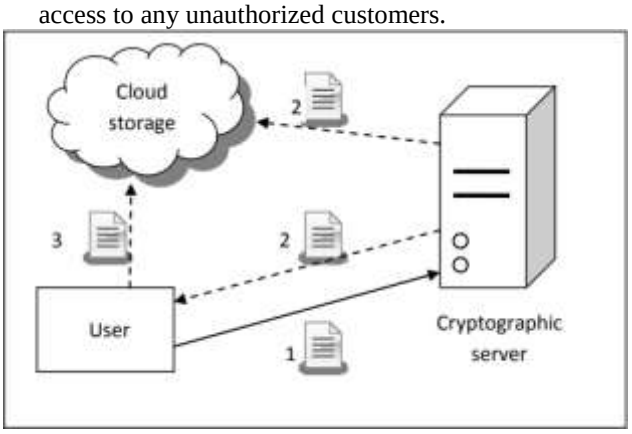
Abstract— Cloud computing is the on-call for availability of computer machine resources, especially facts garage (cloud garage) and computing power, without direct lively control through the consumer Cloud computing can make life easier and businesses extra agile. To address the problem of cloud garage that isn't absolutely depended on. However, they can also pose a major problem when it comes to data security. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose a solution for this data leakage and data loss like problems that provides: 1) security to confidential information 2) authentication 3) data uploading within organization with security; 4) insider threat security; and 5) forward and backward access control. To tackle the issue of cloud storage that is not completely trusted. To enhance the performance of cloud server in phrases of garage new steady facts self-destructing machine in cloud computing is used. In this machine MD5 algorithm is used for encryption and decryption reason. Encryption and decryption for the reason of attaining's the facts in cloud we use the encryption and decryption techniques. Generating the keys and certification an approach customers are said to shop their id personally because it operations as a device to confirm the consumer whenever once they login to the machine.

Keywords: Access Control, Cloud Computing, Key Generation, Authentication, Verification, Security

I. INTRODUCTION

Cloud computing offers a bendy and handy manner for facts sharing, which brings numerous blessings for each society and individuals. But there exists a herbal resistance for customers to at once outsource the shared facts to the cloud server since the facts often contain valuable statistics. Thus, it is vital to area cryptographically stronger get entry to manage the shared facts. Identity-primarily based totally encryption is a promising cryptographical primitive to build practical facts sharing machine. However, getting entry to manage isn't static. That is, whilst some consumer's authorization is expired, there should be a mechanism that could take away him/her from the machine. One of the broadly used alternatives to steady facts is to encrypt facts using cryptography which offers a wide range of techniques to encrypt facts and ensure their privateness and confidentiality. Encrypting facts before uploading them to the cloud assures privateness from the cloud provider company well. Cryptographic techniques contain key control, encryption, and decryption approach. Key control looks after key era for all of the customers which include the brand new customers that could be part of later. If all of the individuals of a set use an unmarried key, the customers want to be extra cautious with key control. So, whilst a brand new consumer is added, the institution generates a new key, re-encrypts the facts, and distributes the keys once more to all of the individuals. Apart from this, there's constantly a risk from malicious legal customers withinside the institution who can also additionally attempt to get entry and tamper with the facts. In the case of an unmarried symmetric key, if customers of the institution maintain the complete key, it could show to be a serious risk if any of the legal customers flip malicious. Though facts are encrypted, it is thus vital to cope with key control efficiently to offer steady facts sharing in the cloud garage. The cryptographic server looks after getting entry to manage, key era, encryption, and decryption approach. Access manage offers all of the statistics approximately the customers which include their rights, permissions, becoming a member of date, etc. Key era entails producing an unmarried symmetric key that's used to encrypt the facts. This secret is then cut up into key stocks for every consumer withinside the institution. The cloud offers garage offerings to the customers. The facts document is encrypted through the cryptographic server and uploaded to the cloud. Whenever the consumer requests get entry to this facts document, the cryptographic server or the recipient consumer downloads the encrypted document from the cloud validates this consumer, decrypts the facts, and sends it again to the consumer primarily based totally on the consumer rights.

- Any consumer with inside the institution can shop and percentage facts files with others through the cloud.
- The encryption complexity and length of ciphertexts are impartial with the wide variety of revoked customers in the machine.
- User revocation may be accomplished without updating the non-public keys of the final customers.
- It offers the offerings as a low upkeep value and excessive best offerings.
- Save the facts of the investment.
- Maintain the facts as a sensitive facts without having access to any unauthorized customers.



II. REVIEW OF LITERATURE

Cloud computing is rapidly emerging due to the provisioning of elastic, bendy, and on-call for garage and computing offerings for customers. Organizations with low finances can now make use of excessive computing and garage offerings without heavily investing in infrastructure and upkeep. However, the loss of management over facts and computation increases many protection concerns for businesses, thwarting

the wide adaptability of the general public cloud. The lack of manage over facts and the garage platform also motivates cloud customers to maintain the get entry to manage over facts (man or woman facts and the facts shared amongst a set of customers thru the general public cloud) Moreover, the privateness and confidentiality of the facts is likewise advocated to be cared for through the customers. The confidentiality control through a customer guarantees that the cloud does now no longer analyzes any statistics approximately the customer facts. Cryptography is used as a typical device to offer confidentiality and privateness offerings to the facts. The facts are usually encrypted before storing them in the cloud. The get entry to manage, key control, encryption, and decryption approaches are handled through the customers to ensure facts protection. However, whilst the facts are to be shared amongst a set, the cryptographic offerings want to be bendy sufficient to cope with distinctive customers, exercising the get entry to manage, and control the keys in a powerful way to safeguard facts confidentiality. The facts managing amongst a set has sure extra traits rather than -celebration verbal exchange or the facts managing to belong to an unmarried consumer. The existing, departing, and newly becoming a member of institution individuals can show to be an insider risk of violating facts confidentiality, and privateness. Insider threats can show to be extra devastating because of the reality that they're normally released through dependent-on entities. Due to the reality that human beings accept as true with insider entities, the research community focuses extra on outsider attackers. Nevertheless, more than one protection problem can get up because of distinctive customers in a set. Literature takes a look at what is made in this paper.

III. System Overview

The user registers himself at the server and then login with a valid username and password into the system. After login, the user requests keys to the cryptographic server. The user/owner encrypts the files using the keys and uploads these files to a cloud server. The authentication key will send to their registered email id with that key user first login the site user id and password that was created during registration and then use that key to upload the file on the server once the file upload action complete that file will be in encrypted form even server cannot open that file and when user wants to view their shared data they can download the specific file using the same key that provided to them during uploading that specific file and then they can download that file the goal is to provide security to organization who works in team. different groups created user needs to register themselves according to their group name and can access or upload file within group itself. If new user enter into to group he or she can not access previously uploaded files this will tackle with malicious insider.

IV. Algorithm

A. Algorithm 1

Input:
F, the ACL, the SKA, the 256-bit hash function H_f Compute:
$R = \{0, 1\}^{256}$

$K = H_f(R)$
$C = \text{SKA}(F, K)$
for each user i in the ACL, do
$Ki = \{0, 1\}256$
$K_i = K \oplus K_i$
Add K_i' for user i in the ACL
Send K_i' for user i end for delete (K) delete (K_i')
return C to the owner or upload to the cloud.
K_i' serves as the user portion of the key and is used to compute K when needed.

B. Algorithm 2: Decryption Algorithm

Input: C, the ACL, the SKA Compute:
Get K_i' from the requesting user
Get C from the requesting user or download from the cloud
Retrieve K_i from the ACL
If K_i does not exist in the ACL, then return the access denied message to the user else
$K = K_i \oplus K_i'$
$F = \text{SKA}(C, K)$ send F to the user
end if
delete (K) delete (K_i').

V. Verification of Properties

The homes which might be validated are the following.

- A legitimate consumer withinside the institution cannot cause the technology of a legitimate K by pretending to be another consumer and contributing a random Ki.
- A legitimate consumer withinside the institution ends in the technology of a legitimate K through contributing a legitimate.
- A malicious consumer outside the institution, if somehow gets get right of entry to the encrypted record, can not cause its decryption.
- Password ought to contain capital small letter and quantity min period eight-character.

VI. Results

Fig. 1: Homepage

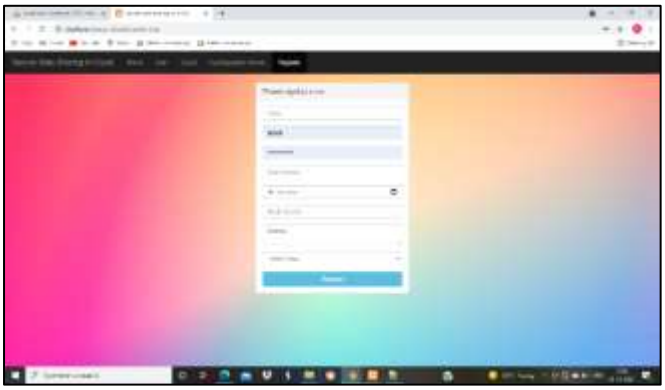


Fig. 2: Registration page

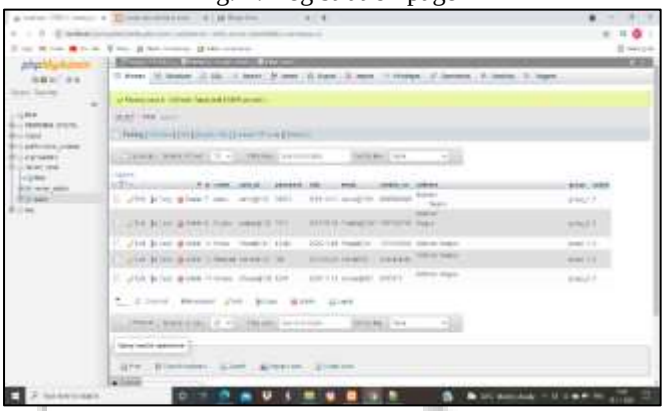


Fig. 3: Database Structure

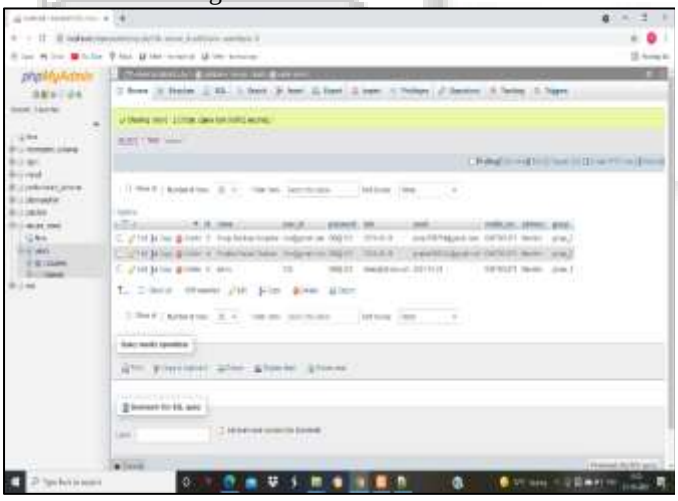


Fig. 4: Database table named secure cloud in mysql

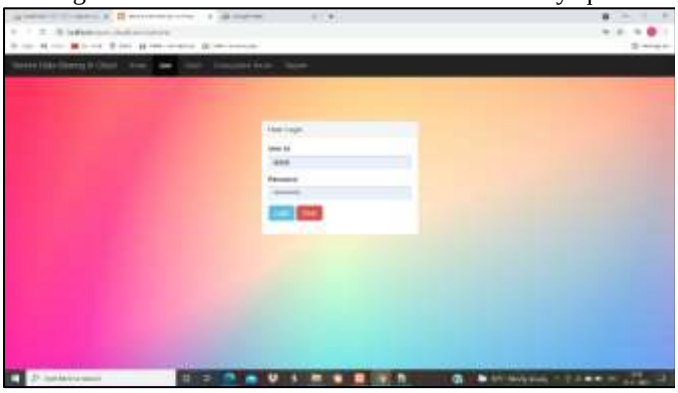


Fig. 5: Cryptographic server login page

Fig. 6: Cryptographic server

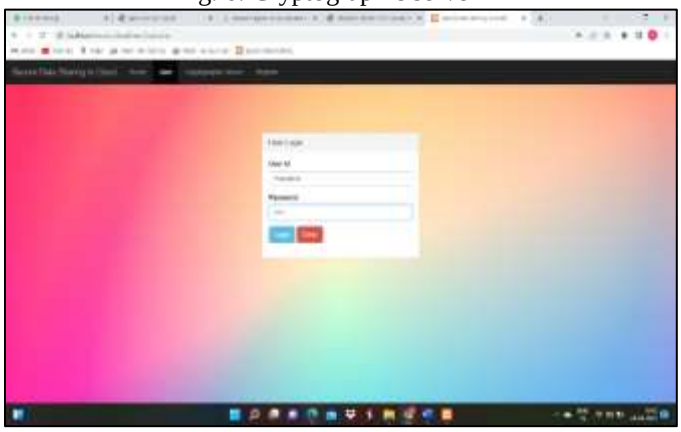


Fig. 7: User login

Fig. 8: User Information

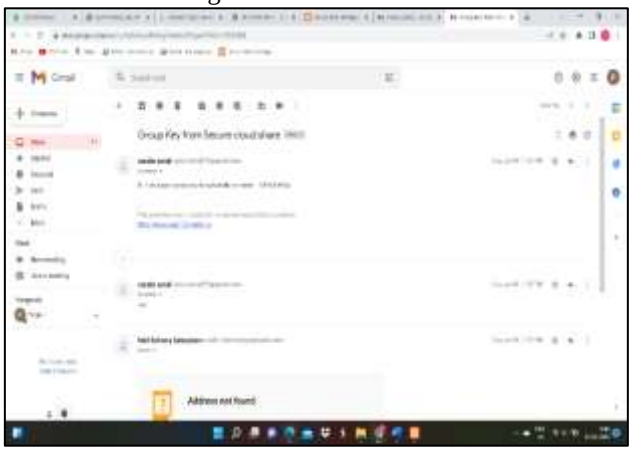


Fig. 9: Group Key Received

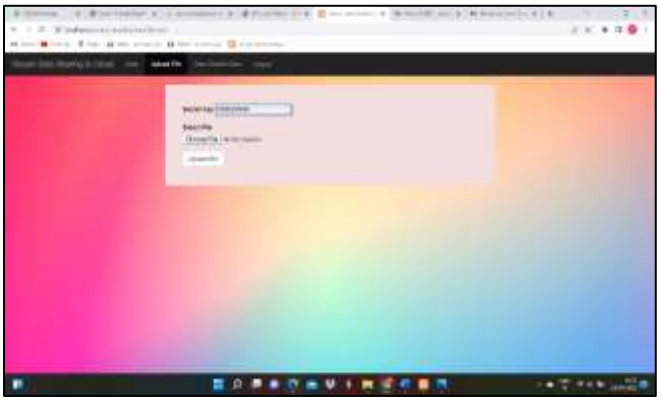


Fig. 10: File Upload

Fig. 11: Dashboard

VII. CONCLUSION

How to guard consumers' personal information in disbursed cloud garage is a hard task. To proportion the private record from one consumer to another consumer is most hard the usage of the cloud computing. To offer greater steady to the information the usage of one of a kind schemes. We studied one-of-a-kind Cloud Computing principles like cellular cloud computing, integrity and ahead protection, social cloud computing, framework, resource allocation, information protection, privateness, and dynamic, IoT, and load balancing schemes. While concerning the protection of information we analyze one-of-a-kind issues such as low protection, excessive computational complexity, privateness/public record sharing, and improper usage of assets. There are distinctive scheduling techniques utilized in more than one federated information center. Aggregate key presents a greater steady in sending records between sender and receiver. Forward protection encryption and re-encryption strategies are used to offer excessive protection for personal information. It gives demonstrates and reproduction of big-scale disbursed computing, together with information centers. Virtual Machines (VMs) and Physical Machines (PMs) consume greater power. This is the limitation, because of this, the fee for record switch is increased. In addition enhancement to triumph over intruder's assaults on personal information, offers greater protection and greater sharing of files, efficaciously usage of assets, and decreasing the electricity consumption.

REFERENCES

[1] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 1431–1441, Jul. 2014.

[2] K. Alhamazani *et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*, DOI: 10.1007/s00607-014-0398-5, 2014, to be published.

[3] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Gen. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul. 2013.

[4] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inf. Sci.*, vol. 258, pp. 371–386, Feb. 2014.

[5] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.

[6] D. Chen *et al.*, "Fast and scalable multi-way analysis of massive neural data," *IEEE Trans. Comput.*, DOI: 10.1109/TC.2013.2295806, 2014, to be published.

[7] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band, "Incremental proxy re-encryption scheme for mobile cloud computing environment," *J. Supercomput.*, vol. 68, no. 2, pp. 624–651, May 2014.

[8] Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in *Proc. IEEE 11th Int. Conf. TrustCom*, 2012, pp. 295–302.

[9] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud," in *Proc. 7th ACM Symp. Inf. , Comput. Commun. Security*, 2012, pp. 87–88.

[10] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in *Proc. 6th USENIX Security Symp. Focusing Appl. Cryptography*, 1996, p. 8.

[11] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–2119, Sep. 2013.

[12] Y. Chen, J. D. Tygar, and W. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in *Proc. IEEE INFOCOM*, pp. 1952–1960.

[13] T. Murata, "Petri Nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[14] L. Moura and N. Bjrner, "Satisfiability modulo theories: An appetizer," in *Proc. Formal Methods, Found. Appl.*, vol. 5902, *Lecture Notes in Computer Science*, 2009, pp. 23–36.

[15] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A methodology for OSPF routing protocol verification," in *Proc. 12th Int. Conf. ScalCom*, Changzhou, China, Dec. 2012, pp. 1–5.

[16] Mazhar Ali (S'14) is presently working toward the Ph.D. diploma in the Department of Electrical and Computer Engineering, College of Engineering, North Dakota State University, Fargo, ND, USA. He is presently with the Department of Computer Science, COMSATS Institute

of Information Technology, Abbottabad, Pakistan. His foremost regions of studies pastimes encompass code-based cryptography and protection in cloud computing.

[17] Samee U. Khan (S'02–M'07–SM'12) obtained the Ph.D. diploma in pc technological know-how from University of Texas, Arlington, USA. He is presently an Associate Professor of electrical and pc engineering with the Department of Electrical and Computer Engineering, College of Engineering, North Dakota State University, Fargo, ND, USA. His studies pastimes encompass topics such as sustainable computing, social networking, and reliability.

[18] Athanasios V. Vasilakos (M'00–SM'eleven) obtained the Ph.D. diploma in pc engineering from the University of Patras, Patras, Greece. He is presently a Professor with the Department of Computer Science, College of Computer Science and Engineering, Kuwait University, Safat, Kuwait. His studies pastimes encompass robustness, protection, pc networks, and disbursed systems.

[19] Keqin Li (M'90–SM'96–F'15) is a Distinguished Professor with the Department of Computer Science, School of Science and Engineering, State University of New York, New Paltz, NY, USA. His studies pastimes mainly encompass the regions of layout and evaluation of algorithms, parallel and disbursed computing, and pc networking.

[20] Revathi Dhamotharan is currently working toward the M.S. degree in electrical and computer engineering in the Department of Electrical and Computer Engineering, College of Engineering, North Dakota State University, Fargo, ND, USA. Her research interests include cryptography and security.

[21] Eraj Khan received the Ph.D. degree in communication security from Lancaster University, Lancaster, U.K. He is currently with the Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, Pakistan. His main areas of research interests include code-based cryptography and security in cloud computing.

[22] Albert Y. Zomaya (F'04) is currently the Chair Professor of high-performance computing with the School of Information Technologies, The University of Sydney, Sydney, Australia.

[23] Mr. Zomaya is a Fellow of The Institution of Engineering and Technology and of the American Association for the Advancement of Science.

