DIVISION & REPLICATION OF DATA IN CLOUD ENVIRONMENT FOR INCREASE PERFORMANCE & SECURITY

Mr. TANVEER AHMAD
Department of Computer Science and Engineering
Farah Institute of Technology, Chevella,
R.R. District –Telengana,
India - 501503
tanveer0587@gmail.com,

K SOMANATHA RAO
Department of Computer Science and Engineering
Farah Institute of Technology, Chevella,
R.R. District –Telengana,
India - 501503
visitsomanatha@gmail.com

ABSTRACT:

Outsourcing facts to a 3rd-celebration managing control, as is achieved in cloud computing, offers rise to security issues. The statistics compromise may additionally arise due to attacks by other customers and nodes within the cloud. Therefore, high safety features are required to guard statistics within the cloud.

However, the hired safety method need to also don't forget the optimization of the facts retrieval time. In or work, we suggest department and replication of records in the area cloud for optimal overall performance and safety (DROPS) that collectively techniques the safety and performance troubles.

In my work, we fragments a file into fragments, & reflect the fragmented statistics over the cloud nodes. Each of the nodes stores most effective a unmarried fragment of a particular statistics document that ensures that even in case of a a success assault, no significant information is found out to the attacker. also, the cloud nodes storing the file fragments will be seperated with certain distance through graph Tcoloring to prevent an attacker to identify the places of the fragments.

Furthermore, the DROPS method does no longer depend on the traditional cryptographic techniques for the statistics security; thereby relieving the machine of computationally high-priced methodologies. We show that the possibility to discover and compromise all of the nodes storing the fragments of a single record is extremely low. We additionally examine the overall performance of the DROPS methodology with 10 different schemes. The better level of protection with mild performance overhead changed into found.

Keywords: *Authentication, key management, Privacy, Rabin cryptosystem, smart card, wireless sensor networks*

I INTRODUCTION

Outsourcing facts to a 3rd-celebration managing control, as is achieved in cloud computing, offers rise to security issues. The statistics compromise may additionally arise due to attacks by other customers and nodes within the cloud. Therefore, high safety features are required to guard statistics within the cloud.

However, the hired safety method need to also don't forget the optimization of the facts retrieval time. In or work, we suggest department and replication of records in the area cloud for optimal overall performance and safety (DROPS) that collectively techniques the safety and performance troubles.

In the my wprk , we fragments a file into fragments, & reflect the fragmented statistics over the cloud nodes. Each of the nodes stores most effective a unmarried fragment of a particular statistics document that ensures that even in case of a a success assault, no significant information is found out to the attacker. Also, the cloud nodes storing the file fragments will be seperated with certain distance through graph Tcoloring to prevent an attacker to identify the places of the fragments.

Furthermore, the DROPS method does no longer depend on the traditional cryptographic techniques for the statistics security; thereby relieving the machine of computationally high-priced methodologies. We show that the possibility to discover and compromise all of the nodes storing the fragments of a single record is extremely low. We additionally examine the overall performance of the DROPS methodology with 10 different schemes. The better level of protection with mild performance overhead changed into found.

II. LITERATURE SURVEY

In the last decade, various security mechanisms [7], have been proposed to prevent unauthorized access to the sensor data in transit. Li et al. proposed a signcryption scheme to protect the information flow between a sensor and an entity outside the WSN, which fulfills confidentiality, integrity, authentication, and non-repudiation in one step. However, bilinear pairing is used in the scheme, which makes it unsuitable (because of its high computation and processing overheads) for regular SNs.

Astorga et al. proposed the Ladon security protocol which provides E2E authentication and key establishment mechanism for resource-constrained devices. To prevent potential eavesdroppers from tracking users' access patterns, they also presented a privacy-enhanced Laden protocol by integrating the original protocol with the PrivaKERB user privacy framework for Kerberos [7]. In these protocols, the long keys need to be securely stored and may be compromised.

In 2014, Turkanovic et al. proposed a lightweight 2FA protocol based on hash function for WSNs, which is claimed to be energy efficient and secure. However, Amin and Biswas [9] showed that the protocol of Turkanovic et al. [10] has several security weaknesses, including offline identity guessing attack, offline password guessing attack, impersonation attack, etc. To address these security deficiencies, they proposed a 2FA protocol for multi-gateway WSN. Independently, Farash et al. Also revealed that the protocol of Turkanovic et al. is susceptible to smart card loss attacks (SSLA), impersonation attack, session key disclosure, et al. and proposed an improved 2FA protocol. In the same year.

III SYSTEM ANALYSIS

EXISTING SYSTEM

The data migration to the cloud is accomplished through the Iris document system. A gateway utility is designed and employed within the business enterprise that guarantees the integrity and freshness of the records the use of a Merkle tree. The record blocks, MAC codes, and model numbers are saved at numerous levels of the tree. The proposed technique in [10] closely depends at the user0s employed scheme for data confidentiality. Moreover, the probable quantity of loss in case of data tempering due to intrusion or get admission to via different VMs cannot be reduced.

- Our proposed approach does no longer depend upon the traditional cryptographic techniques for facts safety. Moreover, the DROPS technique does not store the complete file on a unmarried node to avoid compromise of all the facts in case of a hit attack at the node.
- The authors in [11] approached the virtualized and multi-tenancy associated troubles in the cloud garage with the aid of utilizing the consolidated garage and native get right of entry to control. The Dike authorization architecture is proposed that mixes the local get entry to manage and the tenant call space isolation. The proposed machine is designed and works for item primarily based document systems. However f essential facts in case of flawed sanitization & malicious VM is not handled. The DROPS methodology handles the leakage of crucial records by using fragmenting statistics report and the use of a couple of nodes to keep a single record.

✓ The use of a relied on 0.33 birthday celebration for providing safety offerings in the cloud is advocated in [22]. The authors used the general public key infrastructure (PKI) to beautify the extent of trust inside the authentication, integrity, and confidentiality of information and the communication between the involved events. The keys are generated and managed through the certification authorities. At the user stage, using mood proof devices, consisting of smart cards become proposed for the storage of the keys. Similarly, Tang et al. Have utilized the public key cryptography and depended on third party for offering statistics security in cloud environments [20]. However, the authors in [20] have now not used the PKI infrastructure to lessen the overheads.

Drawbacks of The Existing system

1) There is not any Data Fragmentations to hold statistics in relaxed manner.

2) The information outsourced to a public cloud isn't always secured because of lack of Cloud Security.

PROPOSED SYSTEM

✓ In the proposed model, the device collectively processes the issue of security and overall performance as a secure statistics replication hassle. The system provides Division & Replication of Data in Cloud Environment for Increase Performance & Security that judicially fragments consumer files into portions & replicates them at several places inside the cloud. The department of a record into fragments is finished based totally on a given consumer criteria such that the individual fragments do no longer include any meaningful information and Each of the cloud nodes contains a distinct fragment to boom the information protection.

A a hit attack on a unmarried node must no longer reveal the places of different fragments inside the cloud. To maintain security form an attacker about the locations of the record fragments & to in addition enhance the security, we pick out the nodes in a manner that they may be not adjacent & are at sure distance from every different. The node separation is ensured by the way of the T-coloring.

Attack on node must no longer reveal the places of different fragments inside the cloud. To maintain security form an attacker about the locations of the record fragments & to in addition enhance the security, we pick out the nodes in a manner that they may be not adjacent & are at sure distance from every different. The node separation is ensured by the way of the T-colorings.

To enhance facts retrieval time, the nodes are decided on based totally at the centrality measures that make certain an stepped forward get right of entry to time. To further our model enhance the retrieval time of the fragments, also replicate fragments in the cloud nodes that generate the very best study write requests. The choice of the nodes is finished in two levels. In the primary segment, the nodes are decided on for the initial placement of the fragments primarily based at the centrality measures. In the second section, the nodes are selected for replication. The working of the DROPS technique is shown as a high-stage paintings go with the flow in this machine.

✓ **Advantages**

1) A a hit attack on a node may put the facts confidentiality or integrity, or both at danger.

2) The system proposes not to keep the entire file at a single node. The DROPS methodology fragments the document and uses the cloud for replication. The fragments are disbursed such that no node in a cloud holds more than a single fragment, in order that even a a success attack on the node leaks no big information.

IV IMPLEMENTATION Data Owner Module

● In this module, the facts owner uploads their statistics in the cloud server. For the security motive the records owner encrypts the data report's blocks and then shop within the cloud. The facts proprietor can check the replication of the report's blocks over Corresponding cloud server. The Data owner may have capable of manipulating the encrypted facts file's blocks and the data owner can test the cloud facts in addition to the replication of the precise record's blocks and additionally he can create far off person with admire to registered cloud servers. The statistics owner also exams facts integrity proof on which the block is modified by way of the attacker.

Cloud Server Module

- The cloud carrier issuer manages a cloud to provide information garage service. Data owners encrypt their facts document's blocks and shop them inside the cloud for sharing with Remote User. To get entry to the shared statistics document's blocks, records clients download encrypted records document's blocks of their hobby from the cloud after which decrypt them.

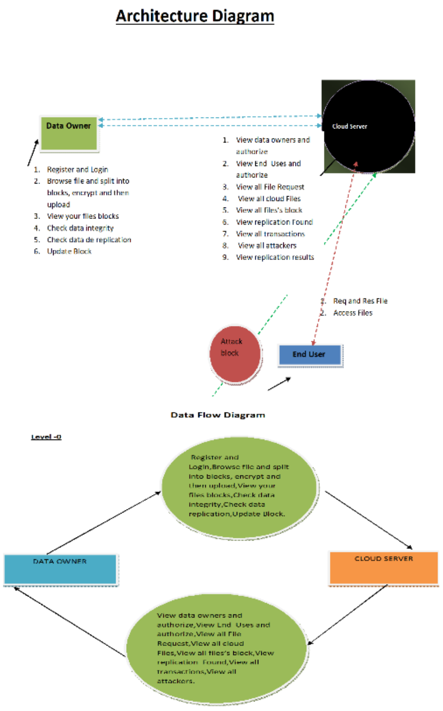
- **End User**
- In this module, remote user logs in through the use of his person call and password. After he will request for secrete key of required file's blocks from cloud servers, and get the secrete key. After getting secrete key he is attempting to download record's blocks by coming into record's blocks name and secrete key from cloud server.

Data Encryption and Decryption

- All the criminal users in the device can freely query any involved encrypted and decrypted information. Upon receiving the facts from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by way of the use of its secret keys from exclusive Users. Only the attributes the person possesses satisfy the get entry to structure provided in the ciphertext and the consumer can get the content key.
- **Attacker Module** The consumer who attacks or modifies the block content material called attacker. The attacker may additionally the user who tries to get right of entry to the report contents by wrong mystery key from the cloud server.

V SYSTEM DESIGN

SYSTEM ARCHITECTURE:


Architecture Diagram
Data Owner
Cloud Server
1. Register and Login
2. Browse file and split into blocks, encrypt and then upload
3. View your files blocks
4. Check data integrity
5. Check data de replication
6. Update Block
1. View data owners and authorize
2. View End Uses and authorize
3. View all File Request
4. View all cloud Files
5. View all Files's block
6. View replication Found
7. View all transactions
8. View all attackers
9. View replication results
1. Req and Res File
2. Access Files
Attack block
End User
Data Flow Diagram
Level -0
Register and Login,Browse file and split into blocks, encrypt and then upload,View your files blocks,Check data integrity,Check data replication,Update Block.
DATA OWNER
CLOUD SERVER
View data owners and authorize,View End Uses and authorize,View all File Request,View all cloud Files,View all files's block,View replication Found,View all transactions,View all attackers.

DATA FLOW DIAGRAM:

Figure 2: System Architecture

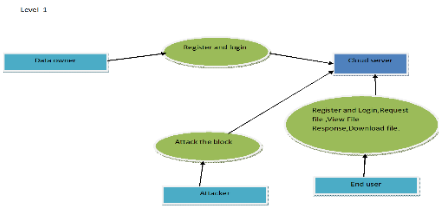


Figure 3: Data flow diagram

VI CONCLUSION

We proposed the DROPS technique, a cloud storage security scheme that collectively offers with the security and performance in phrases of retrieval time. The data file changed into fragmented and the fragments are dispersed over multiple nodes. The nodes had been separated through T-coloring. The fragmentation and dispersal ensured that no significant statistics become available with the aid of an adversary in case of a successful assault. No node within the cloud, stored greater than a unmarried fragment of the equal file. The overall performance of the DROPS methodology was in comparison with full-scale replication strategies. The consequences of the simulations discovered that the simultaneous focus on the security and overall performance, resulted in improved safety stage of records followed via a slight performance drop. Currently with the DROPS technique, a user has to down load the file, update the contents, and upload it again. It is strategic to develop an automated update mechanism which can pick out and update the desired fragments handiest. The aforesaid destiny work will save the time and sources applied in downloading, updating, and importing the file again. Moreover, the consequences of TCP incast over the DROPS technique want to be studied this is relevant to dispensed information garage and get right of entry to.

VII REFERENCES

[1] S. Hong et al., "SNAIL: An IP-based remote sensor organize way to deal with the web of things", IEEE Wireless Commune., vol. 17, no. 6, pp. 34-42, Dec. 2010.

[2] R. Roman, "Key Management Systems for Sensor Networks in the Context of the Internet of Things", Computers and Electrical Eng., vol. 37, no. 2, pp. 147-159, Mar. 2011.

[3] J. Granjal, E. Monteiro, J. S. Silva, "Security in the joining of lowpower remote sensor systems with the web: A review", Ad Hoc Netw., vol. 24, pp. 264-287, Jan. 2015.

[4] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, K. Leung, "An overview on the IETF convention suite for the Internet of Things: Standards difficulties and openings", IEEE Wireless Commun., vol. 20, no. 6, pp. 91-98, Dec. 2013.

[5] 6LoWPAN Working Group, http://tools.ietf.org/wg/6lowpan/

[6] ROLL Working Group, http://tools.ietf.org/wg/roll/.

[7] R. Roman and J. Lopez, "Incorporating remote sensor systems and the Internet: A security investigation," Internet Res., vol. 19, no. 2, pp. 246– 259,2009.

[8] J. Astorga, E. Jacob, N. Toledo, et al. "Improving secure access to sensor information with client protection bolster," Computer Networks, vol. 64, pp. 159-179, 2014.

[9] J. Qi, X. Hu, Y. Mama, et al. "A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme," IEEE Access 3 (2015): 718-724.

[10] Z. Fu et. al, "Accomplishing Efficient Cloud Search Services: Multi-watchword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1,pp.190-200, 2015.

[11] Z. Fu et. al, "Empowering Semantic Search dependent on Conceptual Graphs over Encrypted Outsourced Data," IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2016.2622697

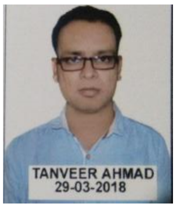
[12] H. Li, D. Liu, Y. Dai, et al. "Building accessible encryption of versatile cloud systems: when QoE meets QoP," IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, 2015.

[13] D. He, S. Zeadally, N. Kumar, J.- H. Lee, "Unknown confirmation for remote body region systems with provable security," IEEE Systems Journal, DOI: 10.1109/JSYST.2016.2544805, 2016.

[14] D. He, S. Zeadally. "Confirmation convention for surrounding helped living framework," IEEE Communications Magazine, vol. 35, no. 1, pp. 71-77, 2015.

[15] K. T. Nguyena, M. Laurentb, N. Oualha, "Review on secure correspondence conventions for the Internet of Things", Elsevier Ad Hoc Networks, vol. 32, pp. 17-31, September 2015.

AUTHORS



Mr Tanveer Ahmad Graduated in B.Tech [CSE] from Royal Institute of Technology & Science JNTU Hyd. He is Studying Master's Degree in M.Tech [CSE] in Farah Institute of Technology JNT University, Hyderabad. Data Mining, Cloud Computing, Information security are his interesting research areas

K.Somanatha rao *Graduated in B.Tech [CSE] from JNTU Hyd. He received Master's Degree in M.Tech [CSE] from JNT University, Hyderabad. His research interests include Information Security, Data Mining and Network Security. She has published research papers in various National, International Conferences,*

Proceedings and Journals. At present he is working as Assistant Professor in CSE Department in Farah Institute of Technology, Chevella, R.R. Dist Telangana State, India.