Privacy Protecting Data Replication and Secure Storage in the Cloud

S. Nithya
M.E(Assistant Professor)
Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode-638012.

K. A. Santhos Kumar, V. Sathyaroopa, D. Swathi
Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode-638012.

Abstract - Customers have access to a practical cloud storage choice with mobile cloud storage. In this research, we introduce a practical, safe, and privacy-preserving mobile cloud storage system that safeguards both the confidentiality and privacy of data, particularly the access pattern. As the central element of the suggested mobile cloud storage system, we explicitly offer an oblivious selection and update technique. The client can secretly download an encrypted data item from the cloud and update it with a new value thanks to OSU, which is based on onion additively homomorphic encryption with constant encryption layers. This drastically minimises the client's calculation and communication overheads. Due to its fine-grained data structure, minimal client-side processing, and constant connection overhead, our approach is very beneficial for cloud Storage scenarios. Moreover, by utilizing the "verification chunks" method. With our advancement, we fragment a file and copy the corrupted data across other cloud nodes. In order to ensure that even in the event of a successful attack, the attacker would not acquire any important information, each server retains a piece of a data file.

Index Terms—Mobile cloud storage, data security, fragmentation, malicious server.

I. INTRODUCTION

Mobile cloud storage allows for the storing of data in the cloud and remote access to that data via mobile devices cloud storage. Due to its appealing characteristics, Cloud storage is gaining popularity. Mobile cloud storage services are offered for corporate use by some major corporations, including Apple I Cloud, Drop box, Microsoft One Drive, and Google Drive[1]. Not everyone believes the cloud to be 100 percent trustworthy. As a result, the client can use encryption to protect data before uploading it to the cloud. In MSC-based applications, however, data will always be connected to particular information, such as location information in location-based services. In this instance, the data item being accessed leaks additional data to the cloud server. The cloud may determine the operation of the client and even the content of the encrypted data by using this access pattern information that has been hacked [3]. For instance, a cloud can find about 80% of search queries in a searchable encryption system by using a generic inference attack with access pattern leaks and the least amount of prior knowledge.
The "oblivious" system can protect both access patterns and data. "Oblivious storage," "oblivious random-access machine," and "oblivious transfer" are some examples (OT).In principle, these solutions enable a customer to access their outsourced data kept in a shaky cloud without identifying which things have been accessed or even the types of operations being asked for[1]. These technologies have been widely used in a variety of application scenarios because to the high level of privacy preservation, including searchable encryption, encrypted hidden volumes, cloud storage, multi-party computation, etc.

II. LITERATURE SURVEY

A.Software Protection and Simulation on Oblivious RAMs

One of the most difficulties in computer usage is software protection. Although there are numerous heuristics and improvised solutions for defence, the issue as a whole has not received the theoretical attention it requires and hereby it explains the software protection theoretically. It simplifies the challenge of software protection to the problem of efficient simulation on oblivious Memory. If the order in which a machine accesses

memory locations is equivalent for any two inputs with the same running time, the machine is unaware. An ignorant Turing machine, for instance, is one in which each computation results in the exact same movement of the heads on the tapes. As a result, it is unrelated to the real input. With the random-access machine model of computation, it demonstrates how to simulate an arbitrary RAM input online using a probabilistic oblivious RAM with a poly-logarithmic running-time slowing and this demonstrates a lower bound is a logarithmic slowing.

B.TWORAM: Efficient Oblivious RAM in Two Rounds with Applications to Searchable Encryption

It introduces TWORAM, an asymptotically effective oblivious RAM (ORAM) protocol that enables blind access (read and write) to a memory index in two rounds: In an encrypted query, the client creates and sends a request to the server. Gaining access to memory M, the server then sends back encrypted data containing the desired value. When compared to tree-based ORAM schemes like the path ORAM method developed by the cost of TWORAM is merely a multiplicative factor of security parameter greater. The interesting applications of TWORAM include a 4-round symmetric searchable encryption scheme where, in the worst case, the search is sublinear and the search pattern is kept secret. If the documents are kept in the memory M that is being accessed unaware, the access pattern can also be kept secret.

C. Remote Oblivious Storage: Making Oblivious RAM Practical

Because of cloud computing technologies, remote data storage has grown more appealing and advantageous. While data is protected by encryption, the access pattern to the data is not concealed. Accessing distant storage using an Oblivious RAM (ORAM), which demonstrates that all access patterns are hidden, is a natural option. Even though ORAM is asymptotically efficient, the best implementation currently available a significant amount of overhead: for every M items locally stored, it stores 4–6 times as many items remotely, makes round trips to the storage server for each request and periodically stops all the data requests to shuffle all storage (which is a lengthy process). It describes the oblivious storage (OS), a concept related to ORAM that more easily and properly reflects the security setting of remote storage. Then, suggests a brand-new ORAM/OS construction that addresses the issues with practicality that were just mentioned. It has a storage constant, achieves round trips to the storage server for each request, and permits requests to happen concurrently with shuffle without endangering security and includes a new flat main section and hierarchical shelter for server memory, a client-side index for quickly finding identifiers at the server, a new shelter serving requests simultaneously with the shuffle, and a data structure for quickly finding objects in a partially shuffled storage.

III. PROBLEM DEFINITION

In existing system, the cloud is not regarded entirely trusted. As a result, the client can use encryption techniques to protect data before uploading it to the cloud. Data that has been outsourced to the cloud must be protected. As mentioned above, illegal data access by other users and processes (whether intentional or unintentional) must be prevented because any weak entity can jeopardise the entire cloud. The security system needs to be considerably improved under these circumstances. Yet, data will always be connected to specific information in MSC-based applications, such as location data in location-based services. The type of data being accessed in this case gives the cloud server additional information.

IV. PROPOSED MODEL

In this study, we collectively approach the performance and security issues as a secure data replication issue. For better performance and security, we offer Detaching and Reproducing of Data in the Cloud, which judiciously divides user files into pieces and replicates them at key locations within the cloud [3].A file is broken into pieces based on provided user criteria so that no meaningful information is contained in any individual fragments. To strengthen data security, each cloud node has a unique fragment. Additionally, save your data on several servers so that if one of them is compromised or becomes unavailable in the future, the others will still allow you to retrieve your data. The second is to transfer the info to others in secure manner. So the user request to transmit the data from cloud to others mean the server generates a key for a specific file and supplied to the cloud user. The random function used to generate a key. The keys are shared by the sender and receiver. The receiver can securely retrieve data from the cloud by utlising the secret key.

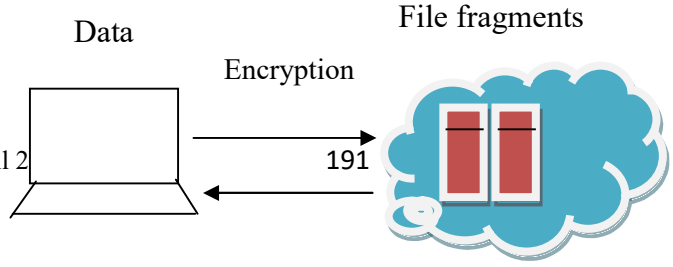

Fig.1. System Model

V. RESULTS AND DISCUSSION

Finally, using DotNet, we put the suggested mobile cloud storage technique to the test while simulating the cloud and the client, respectively. A file is divided into pieces based on specified user criteria so that no useful information is contained in any individual fragments. To strengthen data security, each cloud node has a unique fragment.

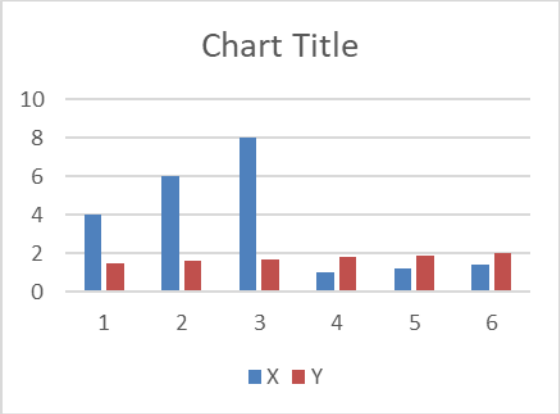

Fig.2. The client storage

The client storage need is shown in Fig. 2 together with variable stash parameters and the smallest effective item size. We can presume that the recommended mobile cloud storage system enables the client to access a much larger mobilecloud storage while using a modest quantity of local storage with high levels of privacy protection.

VI. CONCLUSION

In this research, we provide a mobile cloud storage solution that is effective, secure, and privacy-preserving. The recommended method might simultaneously protect data and access patterns. Compared to current plans. To further increase the effectiveness of the plan, we additionally consider temporal locality. The security and privacy analyses and proofs demonstrate that our plan successfully maintains data confidentiality and a high level of privacy. Finally, using a simulation environment, we fully estimate our construction and compare it to the other two oblivious storage schemes. The results reveal that our method is significantly efficient and has good performances.

ACKNOWLEDGEMENT

We would like to convey our thanks to our guide Ms.S.Nithya (Assistant Professor), Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode for guiding us to take this project.

REFERENCES

[1] M. S. Islam, M. Kantarcioglu, M. kuzu, "Accessing the pattern on searchable encryption: Ramification, attack and mitigation," in 19th Annual Network and Distributed System Security Symposium, NDSS 2012.

[2] Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[3] M.Kannan, R.Srinivasan and G.Neelakrishnan, "A Cascaded Multilevel H-Bridge Inverter for Electric Vehicles with Low Harmonic Distortion", International Journal of Advanced Engineering Research and Science, November 2014; 1(6): 48-52.\

[4] J. Kilian, "Founding cryptography on oblivious transfer," in Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, pp. 20–31.

[5] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[6] G.Neelakrishnan, M.Kannan, S.Selvaraju, K.Vijayraj, M.Balaji and D.Kalidass, "Transformer Less Boost DC-DC Converter with Photovoltaic Array", IOSR Journal of Engineering, October 2013; 3(10): 30-36.

[7] D. Boneh, D. Mazieres, and R. A. Popa, "Remote oblivious storage:Making oblivious Ram Practical," pp. 1–18, 2011.

[8] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[9] R.Baskar, R.Jayaprakash, M.Balaji, M.Kannan, A.Divya and G.Neelakrishnan, "Design of Nanoscale 3-T DRAM using FinFET", IOSR Journal of Electrical and Electronics Engineering, November-December 2013; 8(1):1-5.

[10] O. Goldreich and R. Ostrovsky, "Software protection and the simulation on oblivious Rams," ACM, vol. 43, no. 3, pp. 431–473.

[11] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[12] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised the private searches on public key encrypted data," in Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, March 18-20, 2009. Proceedings, 2009, pp. 196–214.

[13] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay"Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022

[14] T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Oblivious dynamic searchable encryption via distributed PIR and ORAM," IACR Cryptology Archive, vol. 2017, p. 1158, 2017.

[15] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[16] S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: an efficient oblivious RAM in two rounds with applications to the searchable encryption," in Advances in Cryptology ,36th Annual International Cryptology Conference, August 14-18, 2016, Proceedings, Part III, 2016, pp. 563–592.

[17] E. Blass, T. Mayberry, G. Noubir, and K. Onarlioglu, "Toward robust hidden volumes using the write-only oblivious RAM," in ACM SIGSAC Conference on the Computer and Communications Security,November 3-7, 2014, pp. 203–214.

[18] D. S. Roche, A. J. Aviv, S. G. Choi, and T. Mayberry, "Deterministic, stash-free write-only ORAM," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, October 30 - November 03, 2017, pp. 507–521.

[19] E. Stefanov and E. Shi, "Oblivistore: High performance oblivious cloud storage," in 2013, IEEE Symposium on Security and Privacy, pp. 253–267.