International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A New Approach for Securely Sharing Data between Cloud Users with Dual Keys

Varsha K N[1], Prof Ganeshan M[2]

[1]Research Scholar, [2]Mentor and Program Coordinator,
[1,2]School of Computer Science and Information Technology,
Jain (Deemed to be University), Bangalore, Karnataka, India

ABSTRACT

In this project, we propose the Secure Data Sharing in Clouds (sedasc) methodology that provides data confidentiality and integrity; access control; data sharing (forwarding) without using compute-intensive re-encryption; insider threat security; and forward and backward access control. The Sedasc methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the Sedasc methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. We implement a working prototype of the Sedasc methodology and evaluate its performance based on the time consumed during various operations.

How to cite this paper: Varsha K N | Prof Ganeshan M "A New Approach for Securely Sharing Data between Cloud Users with Dual Keys" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.288-290, URL: www.ijtsrd.com/papers/ijtsrd49459.pdf

IJTSRD49459

1. INTRODUCTION

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on demand storage and computing services for customers. The data are usually encrypted before storing to the cloud. The access control, key management, encryption, and decryption processes are handled by the customers to ensure data security. A single key shared between all group members will result in the access of past data to a newly joining member. The SeDaSC methodology works with three entities as follows: 1) users; 2) a cryptographic server (CS); and 3) the cloud. The data are decrypted and sent back to the user. For a newly joining member, the two portions of the key are generated, and the user is added to the ACL.

2. LITERATURE SERVEY

"Distributing Data for Secure Database Services" Vignesh Ganapathy, Dilys Thomas, Dilys Thomas, Rajeev Motwani, Published In 2010

The advent of database services has resulted in privacy concerns on the part of the client storing data with third party database service providers. Previous approaches to enabling such a service have been based on data encryption, causing a large overhead in query processing. A distributed architecture for secure database services is proposed as a solution to this problem where data was stored at multiple sites. The distributed architecture provides both privacy as well as fault tolerance to the client. In this paper we provide algorithms for distributing data: our results include hardness of approximation results and hence a heuristic greedy hill climbing algorithm for the distribution problem partitioning the query at the client to queries for the various sites is done by a bottom-up state-based algorithm we provide. Finally, the results at the sites are integrated to obtain the answer at the client. We provide an experimental validation and performance study of our algorithms.

3. EXISTINGSYSTEM

The Secured BaaS architecture is tailored to cloud platforms and does not introduce any intermediary proxy or broker server between the client and the

cloud provider. Secured BaaS relates more closely to work using encryption to protect data managed by UN trusted databases. Main issue to address is that cryptographic techniques cannot be natively applied to standard DBaaS. Secured BaaS moves away from existing architectures that store just tenant data in the cloud database and save metadata in the client machine or split metadata between the cloud database and a trusted proxy.

3.1. Disadvantages of the existing system

- Even though they are using secure DBaaS means Distributing data among different providers and it give more secure, but its functions cannot be taking advantage of secret sharing outsourced to an untrusted cloud provider.
- It Cannot Store them in encrypted format.
- When considering scenarios where multiple clients can access the same database concurrently.

4. PROPOSEDSYSTEM

The proposed architecture is subject to the TPC-C standard benchmark for different numbers of clients and network latencies show that the performance of concurrent read and write operations not modifying the Secured BaaS database structure are comparable to that of unencrypted cloud Database. Even metadata confidentiality is guaranteed through encryption. This table uses one row for the database metadata, and one row for each table metadata. This encryption key is called a master key. Only trusted clients that already know the master key can decrypt the metadata and acquire information that is necessary to encrypt and decrypt tenant data. Each metadata can be retrieved by clients through an associated Id. This Id is computed by applying a

Message Authentication Code (MAC) function to the name of the object described by the corresponding row.

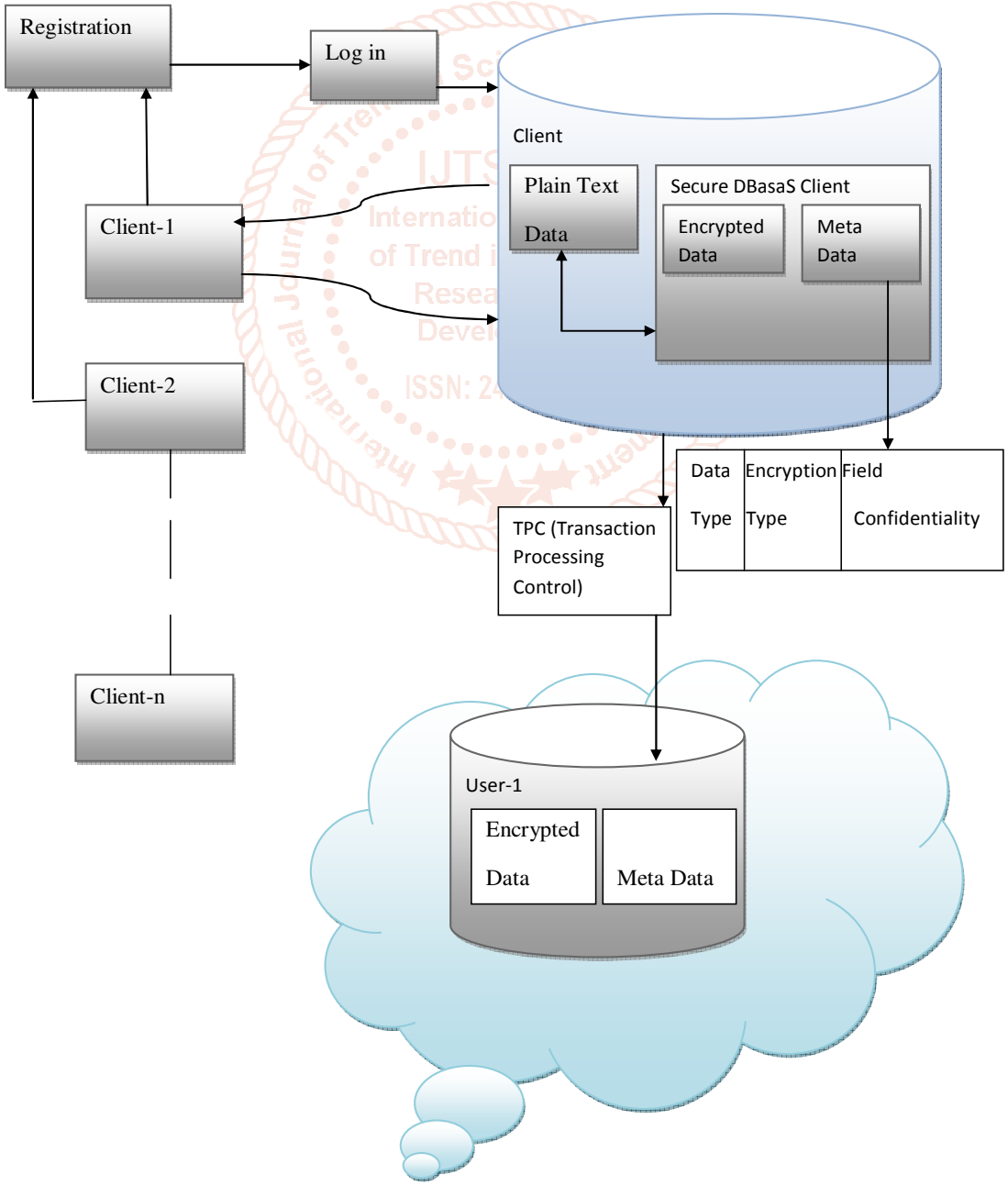

Fig 4.1

5. CONCLUSION

To conclude in this project, Open network, virtualization, monitoring, and security technologies to deploy multi-tier services (e.g., compute clusters) as machines on distributed infrastructures, combining both data center resources and remote cloud resources, according to allocation policies.

6. ACKNOWLEDGEMENT

I should convey my real tendency and obligation to Dr M N Nachappa and Prof. Ganeshan M undertaking facilitators for their effective steerage and consistent inspirations all through my assessment work. Their ideal bearing, absolute co-action and second discernment have made my work Gainful.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.

[3] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[4] J. Li, M. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.

[5] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6] H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, "Providing Database as a Service," Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.

[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of Computing, May 2009.

[8] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011.

[9] https://www.w3schools.com/js/

[10] https://ieeexplore.ieee.org/document/5071626