A control mechanism over data access and download request without loss of security and efficiency

Md Kalesha Vali Mastan PG Scholar, Aditya Engineering College, Surampalem, India
Mr Phani Sridhar Addepalli Associate Professor, Aditya Engineering College, Surampalem, India

ABSTRACT

Due to the low cost and efficiency of the services, which are offered in an open network to protect data security and service user privacy, data sharing and storage has become an increasingly popular concept for business data and banking over the past year. This confidential data was compromised by the encryption technology used to protect it. However, the necessity for data management cannot be identified by mere encrypting data. However, a strong access control over download requests should be taken into account to prevent Economic Denial of Sustainability (EDoS) assaults from being launched to impede users' access to service. In the present research, we take into account dual access control in relation to cloud-based storage, in the sense that we considered control mechanisms that both data access and download requests without any security misuse and efficiency. In this work, two dual access control systems are planned, each of which is for a distinct planned context. Also briefly covered are the systems' security and analysis.

Keywords: *Cloud based data storage and sharing, storage service, ABE algorithms, data security*

1] INTRODUCTION:

All firms today, including those in social media, finance, healthcare, and many more, use cloud services to store and manage their company data because they offer powerful computing capabilities at a lower cost. The main drawbacks of adopting cloud services are DATA SECURITTY and ACCESS since data is stored on external cloud servers, away from the user's hands, where it might be accessed and used inappropriately by malevolent users or internal cloud employees. Data encryption technology was developed to address the aforementioned problems and prevent malicious hackers or internal cloud employees from accessing the data. However, this raises the issue of storing decryption keys with all users with whom the data owner wishes to exchange data. To solve this issue, KPABE (key policy attribute based encryption) was developed. With KPABE, data owners only need to design a policy that includes all sharing user information before encrypting data. When decrypting the data, KPABE checks to see if the file accessing username is present in the access policy; if it is, access will be granted; otherwise, access will be denied. The fundamental drawback

of KPABE is that users must share their keys, which increases the cost of delivering keys over a network and makes them vulnerable to hacking. CP-ABE (cypher policy attribute based encryption), which embeds keys inside encrypted data so they don't have to be sent directly, is introduced as a solution to this issue. Data security and access issues were resolved in the CP-ABE algorithm, but the issue of data downloading persisted because the cloud will permit N users to download data, and malicious users may send a large number of download requests that could cause the cloud server to crash or result in significant costs for the data owner. The author of this paper has introduced the "DUAL ACCESS CONTROL" data sharing concept to address the aforementioned problem. This concept only permits legitimate or authorised users to download data, preventing N users from doing so and preventing DENIAL of SERVICE attacks by ignoring N users' downloads.

Indian Automobile Industry over the years:

2] LITERATUREREVIEW

The creators of this employ the Charm framework to quickly prototype cryptosystems. They implemented over 40 cryptographic techniques utilising this framework. Finally, it can be recharged without charge. Their user base grew to be very active. [1]. With the use of a privacy-preserving multi-authority attribute-based encryption (PPMA-ABE) system, several authorities can be used to obtain a user's private key without disclosing their attributes. [2] The keyword search feature of OABE for cloud storage can greatly lower the calculation costs for customers who want to access encrypted data. [3] As it only distributes sensitive data at a coarse-grained level, attribute-based encryption is utilised for fine-grained access control of encrypted data. important aspect of policy [4] Here, the authors discuss an asymmetric encryption technique in relation to symmetric and week encryption schemes. [5] Encrypted data can be kept private with the CP-ABE technique even if the server is unreliable and is protected from collusion attempts. Secret sharing techniques [6] make it possible for some predetermined groups of parties to piece together a specific secret. key distribution system that makes it possible for each group of participants to produce a secret key [7] a protocol that combines SSE and ABE so that the benefits of each scheme are utilised and it is secured from user revocation issues for both internal and external assaults, as well as decryption through the CP-ABE scheme. [8] a process Verifiable safe secret sharing is not possible with TMACS. It benefits from the master key's ability to be shared while maintaining security and system-level resiliency. [9] Methodology for attributing malicious clients involved in FRC assaults. It aims to undermine the long-term financial feasibility of using the cloud and suggests an attribution approach that succeeds in difficult attack circumstances. [10]

3] OBJECTIVE

The two ABE algorithms, kp-ABE and cp-ABE, are known to have failed due to several drawbacks, thus we used a novel idea called Dual Access Control that only permits authorised or legitimate users to download data. Here, we employ a single strategy known as the Dual Access Control concept. The My SQL database and TOMCAT web application were used in the system approach development for this investigation. SQL database I use: The database management system is free source. Information about plugins is kept there, separated into tables, and connected using keys. Website for TOMCAT: It is a web application that is used to launch and manage web applications programmatically or interactively.

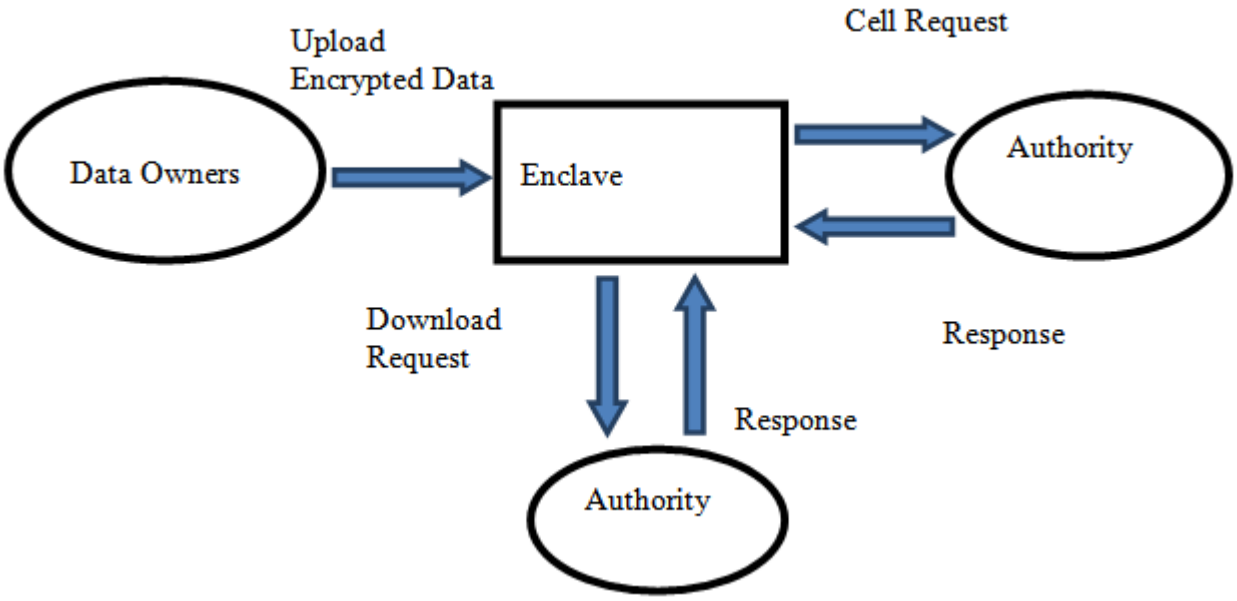


Figure 1: Architecture diagram

4] METHODOLOGY

The KP-ABE algorithm is used in the inquiry, and a web application is used as the user interface.

Dual Access Control (4.1) The following actions are taken

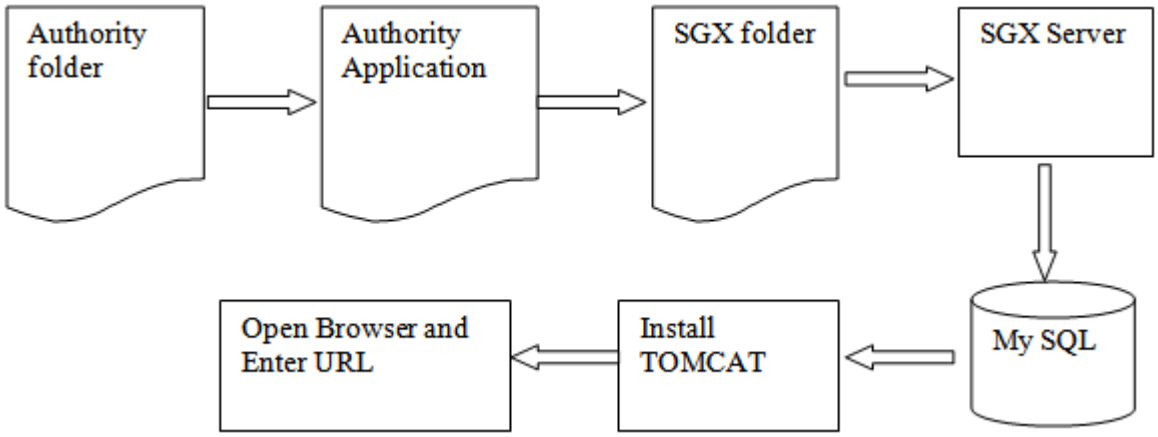
Step 1: Launch the Authority application by clicking the Authority folder.

Step 2: To launch SGX Server, click on the SGX folder.

Step 3: Open the MYSQL console and paste the database creation content.

Step 4: Complete tomcat installation by adding the "Dual-Access" folder to the TOMCAT webapp directory.

Step 5: After starting the Tomcat server, open a browser and type http://localhost:8080/DualAccess into the address bar to access the below home page.



Here, we compare the run times that are required for each step of the basic and improved systems, yielding findings for both the computing cost and the communication cost.

Computational cost:

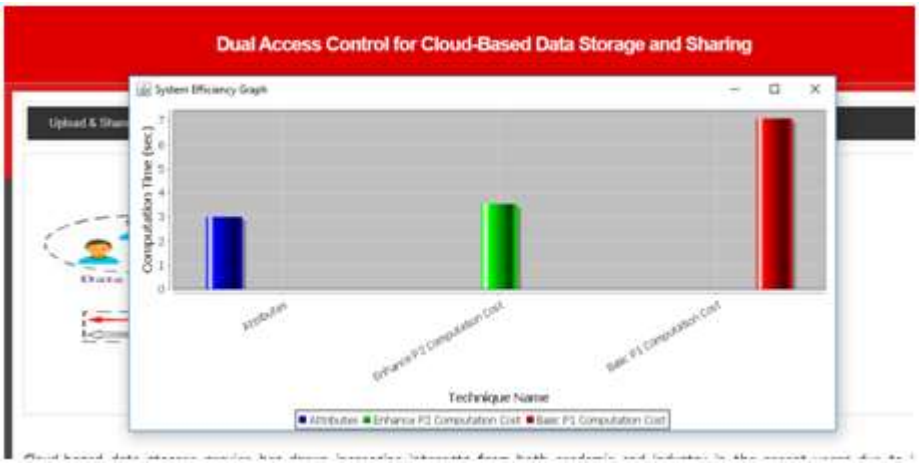
It is the duration of each simulation time step. Calculate the simulation execution-time budget for your real-time target machine to obtain an idea of how long it will take your model to run on real-time hardware. The parameter initialization of Σ 1 (resp. Σ 2) is identical to that of Σ 0 5 for the computational expenses of both encryption and decryption of Σ 1 (resp. Σ2)

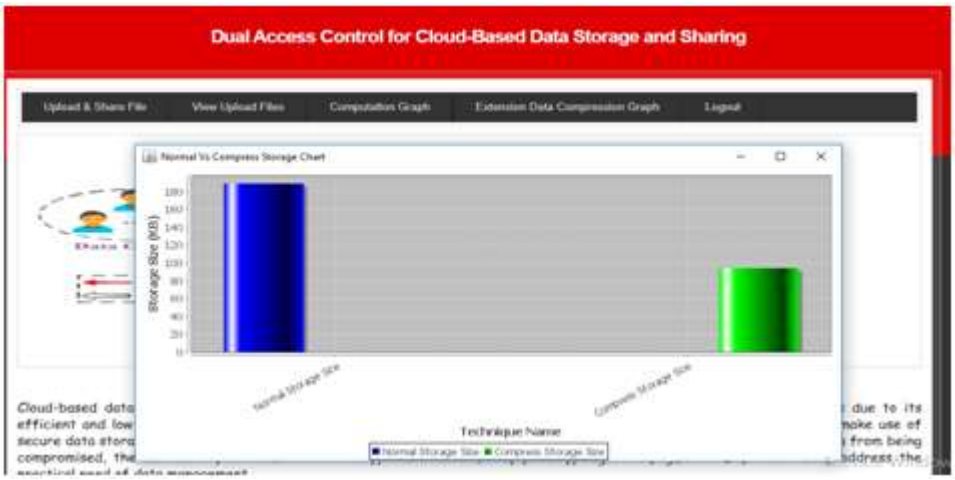
5] Communication cost:

The total communication costs of all the tasks that make up an algorithm make up the communication cost of that algorithm. We'll concentrate on the communication cost as a tool to gauge an algorithm's effectiveness. Only the communication costs utilized for access control during download requests are taken into account in this. The communication cost for a download request is proven to be lower in our suggested approach. Particularly, the ciphertext.

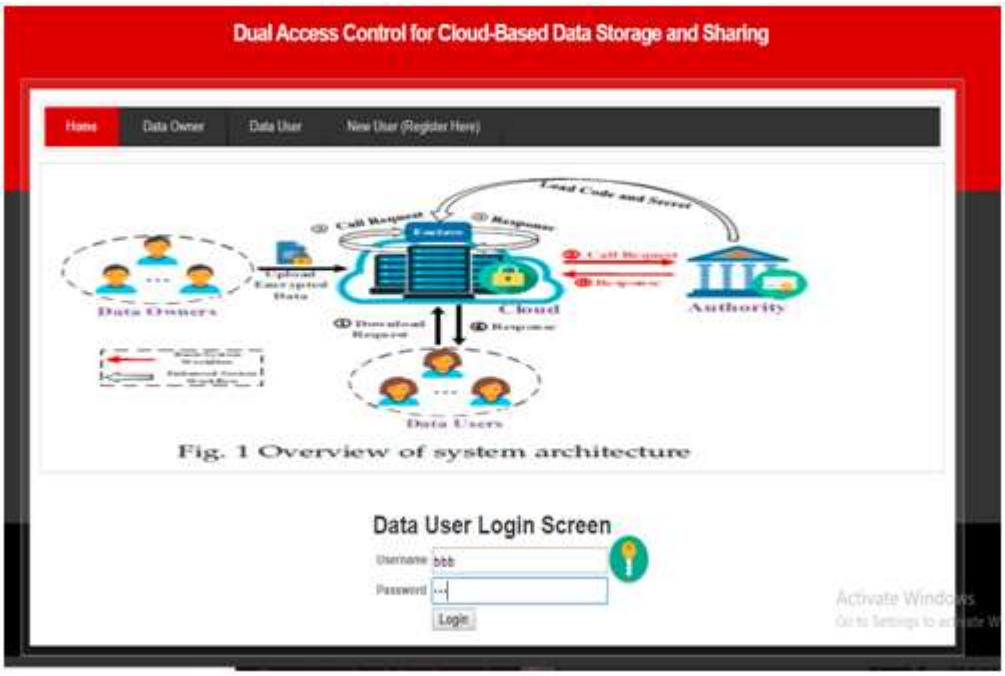
The x-axis in the graph above shows the basic P1 scheme and the enhanced P2 scheme. The basic P1 system generates keys for all users, so its computation time will be greater, but the enhanced P2 strategy will only generate keys for authorised users, so its computation time will be smaller.

Storage Size:





The x-axis in the graph above shows the basic P1 scheme and the enhanced P2 scheme. The basic P1 system generates keys for all users, which increases computation time. The enhanced P2 strategy, however, will only generate keys for authorised users, which decreases computation time.



Login Page

6] CONCLUSION

We draw the conclusion that there is a persistent issue with data security and access in cloud-based data sharing, and as a result, malicious users or internal cloud employees can misuse and get unauthorized access to the data. Both ABE algorithms—cipher text-based CP-ABE and key-based KP-ABE—are employed to solve this issue, but they both still have drawbacks and issues, and the secret data placed into the system cannot be recovered. Dual Access Control is a notion of data sharing that we created to address these difficulties. It only permits legitimate, authorised users to download data and guards against denial-of-service attacks by disregarding downloads from N people.

7] REFERENCES:

1. AUTO HINDUSTAN TIMES. (2021, 11 13). *Aim to make Indian automobile sector no. 1 inworld:NitinGadkari*.RetrievedfromAutoHindustanTimes:https://auto.hindustantimes.com/auto/news/aim-to-make-indian-automobile-sector-no-1-in-world-nitin-gadkari-41636774799243.html
2. Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: *a framework for rapidly prototyping cryptosystems*. Journal of Cryptographic Engineering, 3(2):111–128, 2013.
3. IttaiAnati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.
4. Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.
5. Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
6. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.
7. Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
8. Ben Fisch, DhinakaranVinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.
9. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.
10. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.
11. Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.
12. Christofer Hoff. Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of sustainability). http://www.rationalsurvivability.com/blog/?p=66.

13. Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.
14. Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel R software guard extensions: Epid provisioning and attestation services. White Paper, 1:1–10, 2016.
15. Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.
16. Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing, 10(5):715–725, 2017.
17. Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Full verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2017.2710190, 2017.
18. Wei Li, KaipingXue, Yingjie Xue, and Jianan Hong. Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on parallel and distributed systems, 27(5):1484–1496, 2016.
19. Ben Lynn et al. The pairing-based cryptography library. Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.
20. Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, VedvyasShanbhogue, and Uday R. Savagaonkar. Innovative instructions and software model for isolated execution. In HASP@ISCA 2013, page 10, 2013.
21. Antonis Michalas. The lord of the shares: combining attributebased encryption and searchable encryption and searchable encryption for flexible data sharing. In SAC 2019, pages 146–155, 2019.