PAPER NAME

R paper.pdf

WORD COUNT

2263 Words

CHARACTER COUNT

12062 Characters

PAGE COUNT

7 Pages

FILE SIZE

1017.8KB

SUBMISSION DATE

Jan 31, 2024 11:37 AM GMT+5:30

REPORT DATE

Jan 31, 2024 11:37 AM GMT+5:30

19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 11% Internet database
- Crossref database
- 14% Submitted Works database
- 13% Publications database
- Crossref Posted Content database

Excluded from Similarity Report

- Bibliographic material

Safe Sharing: Access Control for Cloud Stored Data

Abstract-

With the swift development of cloud settings, the problem of safe data storage has surfaced, and before transmitting any data online, businesses and end users alike need to solve it. Lately, a lot of substitutes have been released that either employ Symmetric Searchable Encryption (SSE) or Attribute-Based Encryption (ABE). SSE encryption offers defense against attacks from the inside as well as the outside. But in an SSE system, everything is encrypted with a single key, therefore in order to remove a user's access, the entire encrypted database must be downloaded and then encrypted again with a new key. Conversely, revocation is a problem that can be solved in an ABE system. However, as the rules get more complex, the cost of revocation rises because the recommended remedies depend on the features of the underlying ABE scheme. To do this, we combine the best aspects of both ABE and SSE cryptography techniques to create a hybrid encryption method that is ideal for cloud-based systems.

Keywords: - Encryption, Untrusted parties, Access Control, Symmetric Searchable Encryption (SSE), Attribute-Based Encryption (ABE)

I. Introduction

People may rapidly and simply execute crucial tasks with their data in cloud computing, such as locating, transferring, and conserving it. However, maintaining the security of the data is a challenge. This is due to the fact that the data is kept by a different organization, and poorly protected data carries the highest risks.

The last several years have seen such rapid development in cloud computing that almost everyone's everyday life is now significantly impacted by it. The cloud is currently used on a daily basis by both large corporations and regular internet users. However, because cloud services are maintained and held by dubious third parties, leaving the contents vulnerable to internal attacks, many users are still reluctant to outsource their personal information.

Major players in the business as well as researchers have looked at attribute-based and symmetric searchable encryption as potential solutions for this reason. In an SSE system, users encrypt their files locally before transferring them to the Cloud Service Provider (CSP). Consequently, the CSP lacking the encryption key is unable to acquire any meaningful information regarding the users' data.The ability to do a direct keyword search on encrypted data is the most exciting feature of SSE, though. Unfortunately, user revocation is not supported by SSE systems, which is a major problem for cloud-based apps. Thus, eliminating a user corresponds to downloading the entire database and re-encrypting it using a fresh key.An alternative approach that functions in cloud-based applications is ABE. A master public key is used to encrypt every file in ABE schemes; however, in contrast to traditional public key cryptosystems, the ciphertext that is generated is limited by a policy. Every user also has a unique secret key associated with their attributes (ID, age, organization, etc.). As a result, a file can only be unlocked if and when the user's attributes align with the ciphertext's policy. However, utilizing an asymmetric encryption technique to encrypt large volumes of data is not very successful.

II. Literature survey

A. Michalas and A. Bakas presented a novel technique that enables data owners to link specific policies to specific areas of their cipher texts. The scheme is based on existing symmetric primitives. They combined an in-depth simulation-based security study with an experimental evaluation that demonstrates our scheme's efficacy to demonstrate the accuracy of our methodology[1]. A. Sharma claims in the J. Bethencourt study that

using a trusted server to store data and handle access control is the only way to enforce such regulations. In their system, a party encrypting data establishes a policy for who can decrypt, and attributes are used to characterize a user's credentials. Consequently, techniques like role-based access control (RBAC) [2] are used. The safe and effective oblivious storage systems described in the paper by Y. XU and W. Cui concentrate on making use of all available network bandwidth to provide concurrent access through a reliable proxy. However, the performance is limited by the network's latency and bandwidth because the proxy uses the network to carry out a common ORAM protocol. Furthermore, in such proxy environments, several crucial elements like access control and security against active adversaries have not been well investigated [3]. The study by R. Dowsley shows how to create a hybrid encryption scheme that combines SSE and ABE while taking advantage of their respective benefits. Unlike many other methods, we build a revocation process that is based only on SGX's capability and is totally independent of the ABE scheme [4].The concept of backward privacy for searchable encryption is examined for the first time in the study by R. Bost and B.Minaud. Following the theoretical definitions of several flavors of backward privacy, we propose multiple strategies with varied efficiency trade-offs that achieve both forward and backward privacy. Importantly, our constructs depend on primitives like puncturable encryption schemes and limited pseudo-random functions[5].

Problem Definition:

Due to the rise in data breaches in cloud computing, all users are vulnerable to business issues. Proactive approaches are crucial in mitigating the increasing danger of threads that users encounter in cloud environments, while also emphasizing the need for improved security controls. The major objective is to use various encryption algorithms, such as SSE and ABE, at untrusted clouds to create advanced protection for user assets.[6]

III. Proposed System:

The proposed approach is compatible with deployment models for private, communal, or hybrid clouds. The suggested framework consists of the sensitive data in the cloud is encrypted using a hybrid encryption approach. Before the data is transferred to the cloud, it will be encrypted with a public key. We have specific access that only specific individuals can access the cloud data information after moving the encrypted data there.

An authorized user has the ability to view and edit cloud data information. A user can extract a certain block of code using the SSE Algorithm and use it to decrypt a particular file. Not all users of the ABE Scheme will be able to access data; authentication will only be granted to specific users.

IV. Block Diagram:

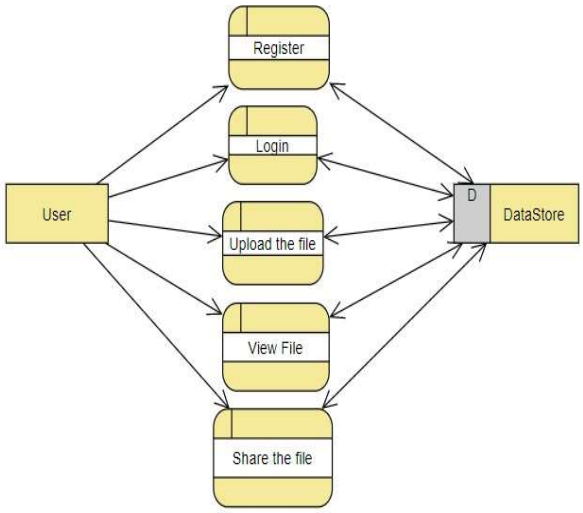

Fig 1: Block Diagram

The user will first register using his email address and password in the diagram. Following page login, he or she will upload a file and be able to view it or retrieve it by using a term as a key. By employing that keyword, the user can so share the file with others. The credentials are crucial for the system in the main.

Architecture

The flow diagram that follows provides an explanation of how the system operates. The steps that make up the overall process are as follows.

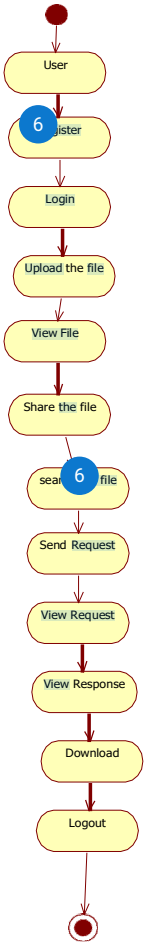

Fig 2: Flow Diagram

V. System Implementation:

Modules:

The methodology consists of a set of steps that must be followed in a specific order for the process to be completed. Since the waterfall model is used in the methodology, the suggested system meets the requirements by creating planning in a way that ensures steps are completed in a methodical manner.

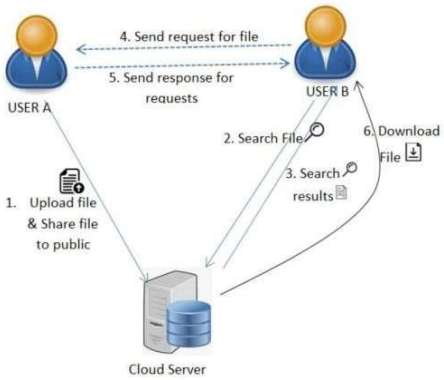

Fig 3: Architecture

• **Register:** After entering his information, the user can register.
• **Login:** Using legitimate credentials, the user can log in. The user may be redirected to the login page if they provide invalid credentials. The user may be sent to their home if they submit proper credentials.
• **Upload:** The user may upload files here.
• The file can be generated with searchable keywords and stored in an encrypted format during the upload process.
• **View Files:** The user can share files with other users and view files that have been submitted.
• **Search:** Using keywords, users can look for files. Send a request to the file uploaded user if the file has been located.
• **View request:** This feature allows the user to see requests made by other users for their files, which they can either accept or reject.
• **Status:** The feature allows the user to check the requested file's pending and accepted states.
• **Download:** Should the user's request be approved, he can get the file. The original encryption file, which has been transformed into a decryption format, can be downloaded here.

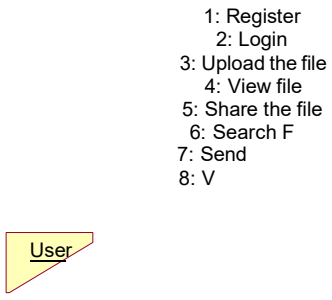

Fig 4: Use Case Diagram

VI. Results and Discussion

The user will be the only source of dependency for the proposed system. Given that we are using a webpage to demonstrate how the system functions. The outputs from the first to the last step, or from the registration stage to the file retrieval or sharing stage, are displayed in the photos below. Users can only share their files with other users if the keyword matches the index number. Users can only grant access to other users to other files if they request it; only the user can determine whether to grant access.

Home : this is the intial page of the project

5 ig 5 : Home Page

User Registration:

Fig 6: Registration page

User login :

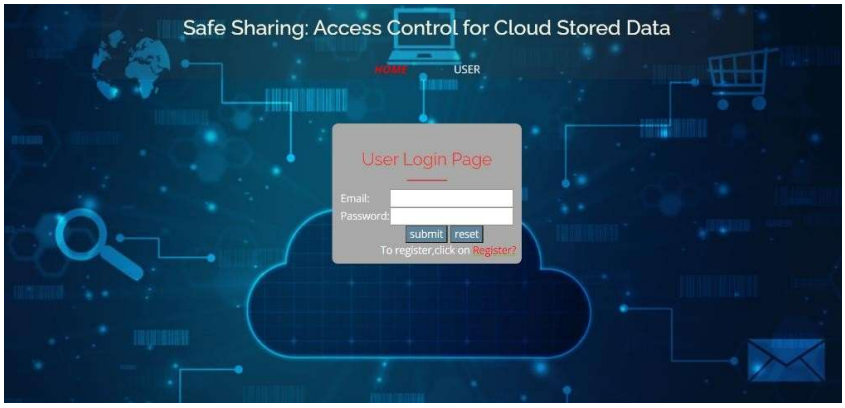

Fig 7: Login Page

User Files Upload:

Fig 8: User Uploading Files

View Files:

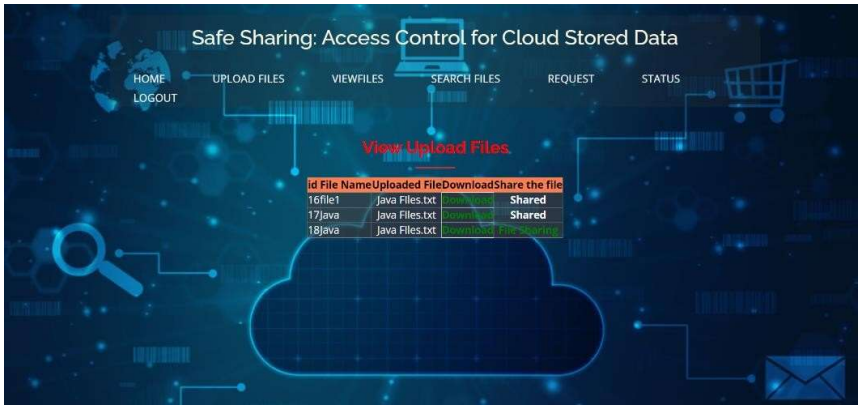

Fig 9: User Viewing Files

Search Files:

Fig 10: User Searching Files

Request Files:

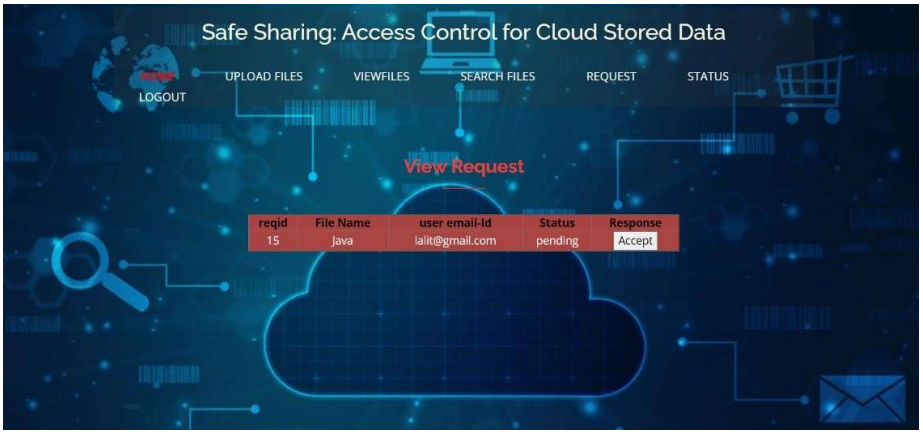

Fig 11: Request Acceptance

Status:

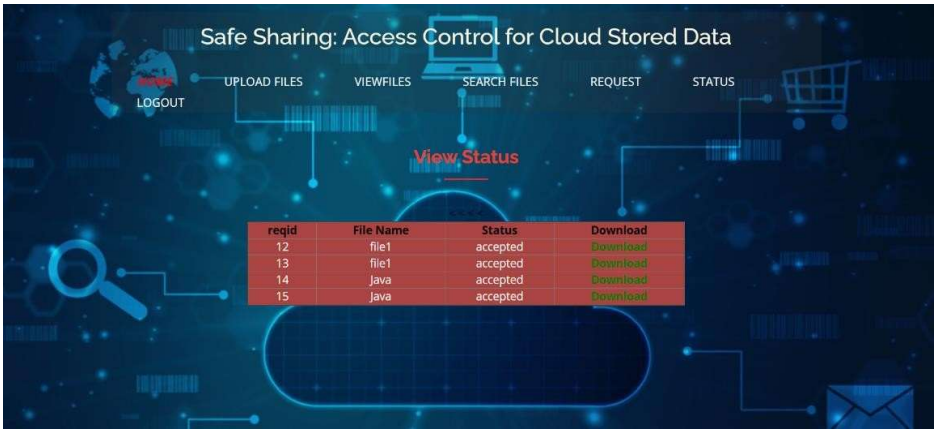

Fig 12: Status of the Page

VII. Conclusion

In this paper, we proposed ABE. Our construction allows a data owner to share her data in a privacy-preserving way and manage the access rights of the rest of the users.

VIII. Future Scope: In future we can implement to More security and provide Email Authentication.

IX. References

[1] S. Agrawal and M. Chase, ‘‘FAME: Fast attribute-based message encryption,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2017, pp. 665–682.

[2] G. Amjad, S. Kamara, and T. Moataz, ‘‘Forward and backward private searchable encryption with SGX,’’ in Proc. 12th Eur. Workshop Syst. Secur. (EuroSec). New York, NY, USA: Association for Computing Machinery, 2019.

[3] A. Bakas and A. Michalas, ‘‘Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX,’’ in Security and Privacy in Communication Networks, S. Chen, K.-K. R. Choo, X. Fu, W. Lou, and A. Mohaisen, Eds. Cham, Switzerland: Springer, 2019, pp. 472–486.

[4] A. Bakas and A. Michalas, ‘‘Multi-client symmetric searchable encryption with forward privacy,’’ Cryptol. ePrint Arch., Tampere Univ., Tampere, Finland, Tech. Rep. 2019/813, 2019. [Online]. Available: https://eprint.iacr.org/2019/813

[5] A. Bakas and A. Michalas, ‘‘Power range: Forward private multi-client symmetric searchable encryption with range queries support,’’ in Proc. IEEE Symp. Comput. Commun. (ISCC), Jul. 2020, pp. 1–7.

[6] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy (SP). Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[7] A. Boldyreva, V. Goyal, and V. Kumar, ‘‘Identity-based encryption with efficient revocation,’’ in Proc. 15th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2008, pp. 417–426.

[8] D. Boneh, X. Boyen, and E.-J. Goh, ‘‘Hierarchical identity based encryption with constant size ciphertext,’’ in Advances in Cryptology—EUROCRYPT, R. Cramer, Ed. Berlin, Germany: Springer, 2005, pp. 440–456.

[9] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ‘‘Public key encryption with keyword search,’’ in Proc. Int. Conf. Appl. Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506–522.
[10] R. Bost, ‘‘σ οφος: Forward secure searchable encryption,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 1143–1154.
[11] R. Bost, B. Minaud, and O. Ohrimenko, ‘‘Forward and backward private searchable encryption from constrained cryptographic primitives,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2017, pp. 1465–1482.
[12] V. Boyko, ‘‘On the security properties of OAEP as an all-or-nothing transform,’’ in Advances Cryptolology— CRYPTO, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 503–518,
[13] V. Costan and S. Devadas, ‘‘Intel SGX explained,’’ Cryptol. ePrint Arch., Intel, Mountain View, CA, USA, Tech. Rep. 2016/086, 2016.
[14] R. Dowsley, A. Michalas, M. Nagel, and N. Paladi, ‘‘A survey on design and implementation of protected searchable data in the cloud,’’ Comput. Sci. Rev., vol. 26, pp. 17–30, Nov. 2017.
[15] M. Etemad, A. Küpçü, C. Papamanthou, and D. Evans, ‘‘Efficient dynamic searchable encryption with forward privacy,’’ Proc. Privacy Enhancing Technol., vol. 2018, no. 1, pp. 5–20, Jan. 2018.
[16] B. Fisch, D. Vinayagamurthy, D. Boneh, and S. Gorbunov, ‘‘IRON: Functional encryption using Intel SGX,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), Oct. 2017, pp. 765–782.
[17] B. Fuhry, R. Bahmani, F. Brasser, F. Hahn, F. Kerschbaum, and A.-R. Sadeghi, ‘‘HardIDX: Practical and secure index with SGX,’’ in Data and Applications Security and Privacy, G. Livraga and S. Zhu, Eds. Cham, Switzerland: Springer, 2017, pp. 386–408,
[18] S. Lee, M. Shih, P. Gera, T. Kim, H. Kim, and M. Peinado, ‘‘Inferring fine-grained control flow inside SGX enclaves with branch shadowing,’’ in Proc. 26th USENIX Secur. Symp., Victoria, BC, Canada, Aug. 2017, pp. 557–574.
[19] J. K. Liu, T. H. Yuen, P. Zhang, and K. Liang, ‘‘Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list,’’ in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. Cham, Switzerland: Springer, Jul. 2018, pp. 516–534.
[20] A. Michalas, ‘‘The lord of the shares: Combining attribute-based encryption and searchable encryption for flexible data sharing,’’ in Proc. 34th ACM/SIGAPP Symp. Appl. Comput., New York, NY, USA, Apr. 2019, pp. 146–155.
[21] A. Michalas, ‘‘Text files from Gutenberg database,’’ Tampere Univ., Tampere, Finland, Tech. Rep., Aug. 2019. [Online]. Available: https://zenodo.org/record/3360392#.X7fuas0zaUk

19% Overall Similarity

Top sources found in the following databases:

- 11% Internet database
- Crossref database
- 14% Submitted Works database
- 13% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	**trepo.tuni.fi** Internet	8%
2	**SASTRA University on 2022-07-12** Submitted works	4%
3	**Brent Waters. "Ciphertext-Policy Attribute-Based Encryption", 2007 IEE...** Crossref	1%
4	**Alexandros Bakas, Hai-Van Dang, Antonis Michalas, Alexandr Zalitko. "...** Crossref	1%
5	**Universite Saint Joseph on 2023-10-09** Submitted works	<1%
6	**VIT University on 2017-04-25** Submitted works	<1%
7	**SASTRA University on 2022-07-14** Submitted works	<1%
8	**link.springer.com** Internet	<1%

9	Qinlong Huang, Yixian Yang, Wei Yue, Yue He. "Secure Data Group Shar... Crossref	<1%
10	archive.org Internet	<1%
11	springerprofessional.de Internet	<1%