**Safe Sharing: Access Control for Cloud Stored Data**

Narasimhulu Malavathula,1, a) Ajay Kishore Gattu,Mounika Meenuga, Harsha Sri Talanki, Bhavana Bommineni2,3,4,5 b)

*1Assistant Professor, Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, India.*

*2,3,4,5 Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology*

*a)*[*narasimhulu.cse@srit.ac.in*](mailto:narasimhulu.cse@srit.ac.in)*,*

*b)*[*204g1a0506@srit.ac.in*](mailto:204g1a0506@srit.ac.in)

*c)*[*204g1a0561@srit.ac.in*](mailto:204g1a0561@srit.ac.in)

*d)*[*204g1a0536@srit.ac.in*](mailto:204g1a0536@srit.ac.in)

*e)*[*204g1a0522@srit.ac.in*](mailto:204g1a0522@srit.ac.in)

**Abstract.** The rapid expansion of cloud environments has brought about a significant challenge to secure data storage. This is a critical consideration for every user when decided to move the data online. To address this challenge, various solutions have been proposed, with two prominent approaches being Searchable Symmetric Encryption and Attribute-Based Encryption. SSE offers protection against both external and internal threats. It allows for efficient search capabilities while maintaining the confidentiality of the data. In an SSE technique, all data is usually encrypted using a single key. The entire encrypted database would need to be downloaded and re-encrypted with a new key if a user was to be revoked. Conversely, though, ABE offers a more granular approach to access control by encrypting data based on attributes and policies. This means that different users or groups can be granted different levels of access to the data based on their attributes.

**Keywords: Encryption, Cryptography, Access Control, Searchable Symmetric Encryption (SSE), Attribute-Based Encryption(ABE)**

# 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 because the information is maintained 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. Many individuals are yet reluctant to delegate their personal data due to the fact that cloud services are hosted and overseen by dubious third parties, rendering the data vulnerable to internal breaches.

Major players in the business as well as researchers have looked at attribute-based and symmetric searchable encryption as potential solutions for this reason. Before transmitting their files to the Cloud Service Provider (CSP), individuals participating in SSE employ local encryption. Consequently, the CSP, lacking the encryption key, is unable to access any pertinent details regarding the user 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 download the complete database and again encrypting it using a new key.

An alternative approach that functions in applications that utilize cloud technology is ABE. A master public key is employed to encrypt all files in ABE schemes; nevertheless, in contrast to traditional public key cryptosystems, which use the ciphertext that is generated is limited by a policy. Every user also has a secret key which is unique and associated with the user’s attributes. As a result a file can be unlocked only if and when the characteristics possessed by the user align with the ciphertext's policy. However, encrypting vast amounts of data with an asymmetric encryption method is not particularly effective.

**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 a security study that employs simulation-based methods and includes an experimental evaluation is conducted to showcase the effectiveness of our scheme, thereby demonstrating the precision of our methodology[1].

A. Sharma claims in J. Bethencourt study that using a reliable server for data storage and access control is the only way to enforce such regulations. In their system, a party encrypting data create 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]

The primary objective of this study is to emphasize and give attention to an encryption scheme called efficient revocable Ciphertext-Policy Attribute-Based Encryption. This particular encryption scheme is designed to allow the revocation of access to encrypted data based on specific attributes associated with the intended recipient. This means that if a user's attributes change, they can be revoked access to the encrypted data, ensuring security and privacy. The scheme focuses on enhancing the efficiency of the revocation process, ensuring that it can be done in a timely and effective manner. By utilizing this encryption scheme, organizations and individuals can have more control over who can access their encrypted data, enhancing overall data security. [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 flavours 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

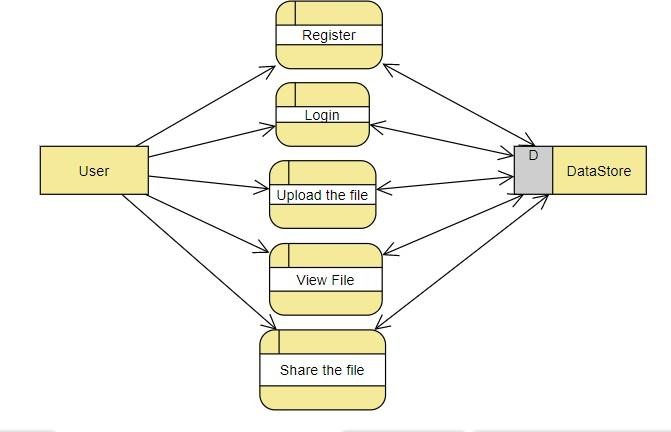
Due to the rise in data breaches in cloud computing, all users are vulnerable to business issues. Proactive approaches are crucial in mitigating the increasing danger of threads that users encounter in cloud environments, while also emphasizing the need for improved security controls. The major objective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

# 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.

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.

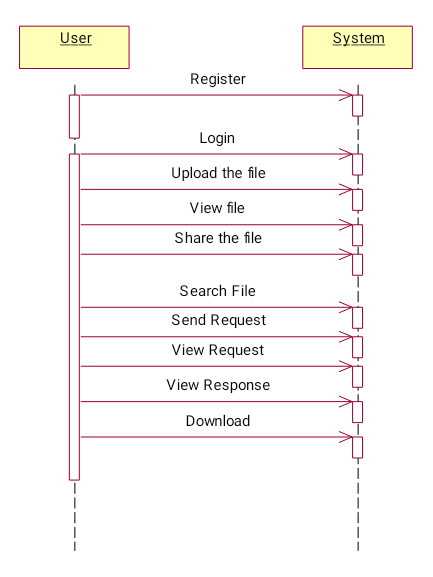
# BLOCK DIAGRAM



**FIGURE 1: Block Diagram**

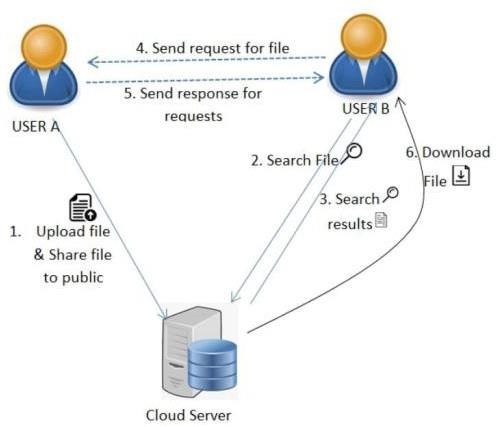
The user will first register using his email address and password in the diagram. Following page login, he or she will upload a file and be able to view it or retrieve it by using a term as a key. By employing that keyword, the user can so share the file with others. The credentials are crucial for the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

**FIGURE 2: Flow Diagram**.

**SYSTEM IMPLEMENTATION**

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.

**FIGURE 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

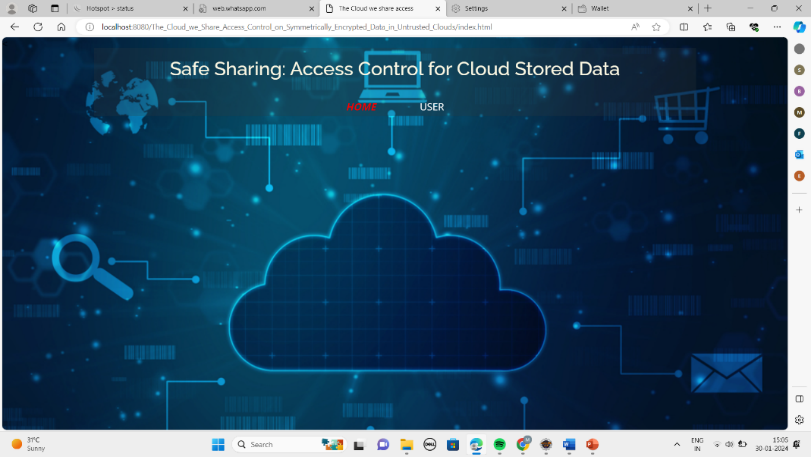
**FIGURE 4: Use Case Diagram**

**EFFICIENCY OF ALGORITHMS**

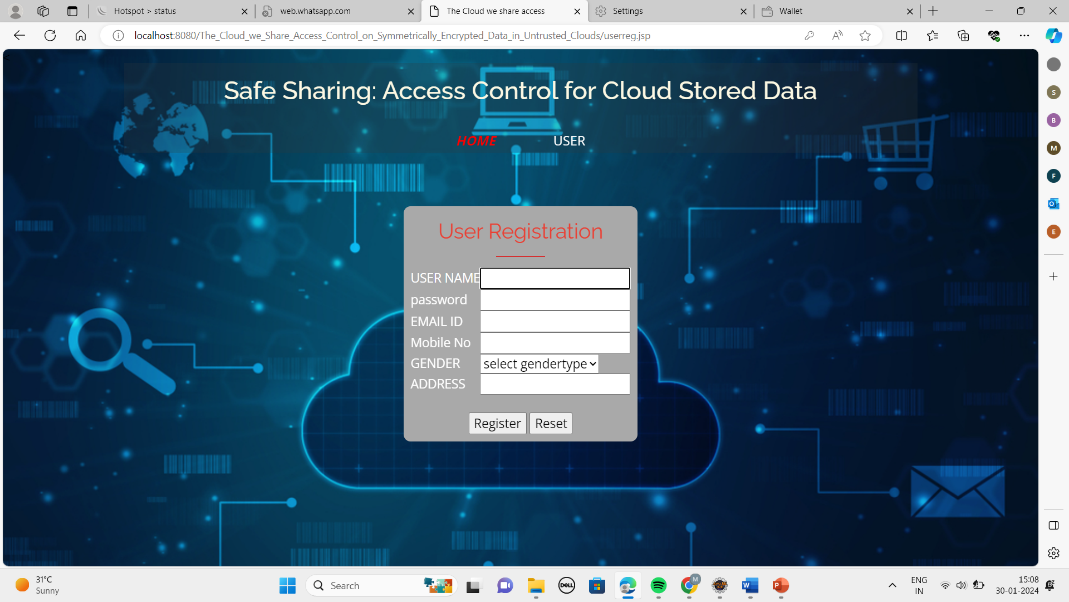
It's difficult to provide an exact percentage of the security offered by Attribute-Based Encryption (ABE) and Symmetric Searchable Encryption (SSE) as it is reliable on various factors such as the strength of encryption algorithms, key management practices, and implementation details. However, both ABE and SSE can provide a high level of security, typically well above 90% when implemented correctly and used in appropriate scenarios.

**RESULTS & DISCUSSION**

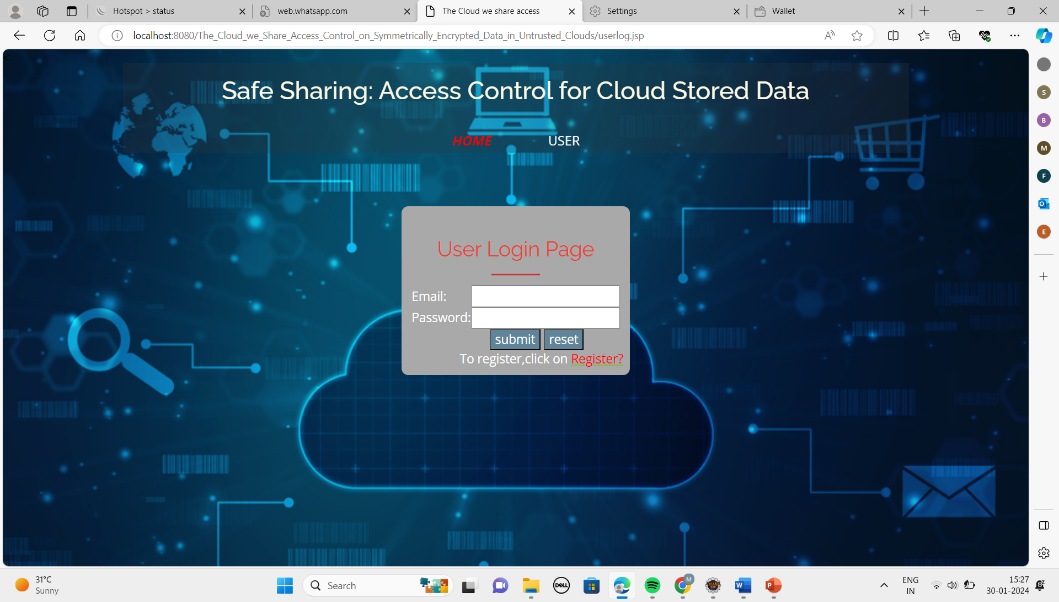
The user will be the only source of dependency for the proposed system. Given that we are using a webpage to demonstrate how the system functions. The outputs from the registration stage to the file retrieval and sharing stage are displayed in the images below. Users can only share their files with other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

*Home : this is the intial page of the project*

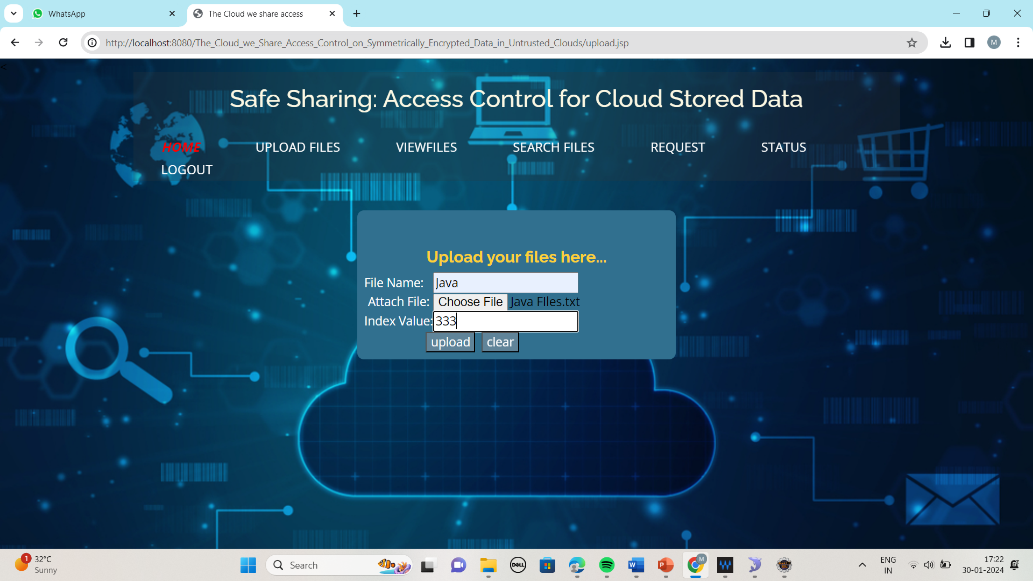
**FIGURE 5: Home Page**

*User Registration*:

**FIGURE 6: Registration Page**

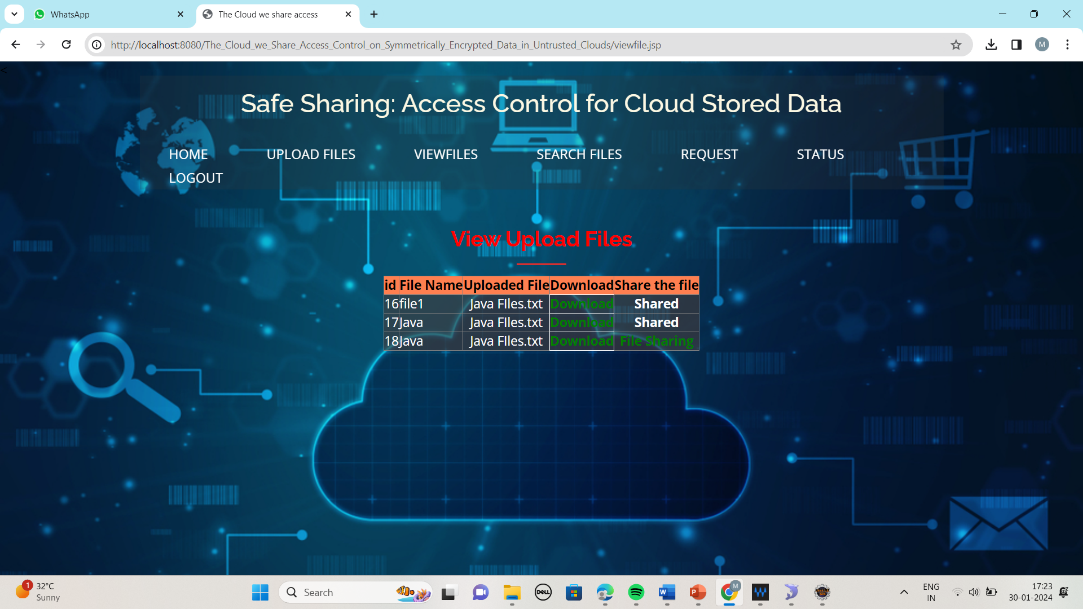
*User login*

**FIGURE 7: Login Page**

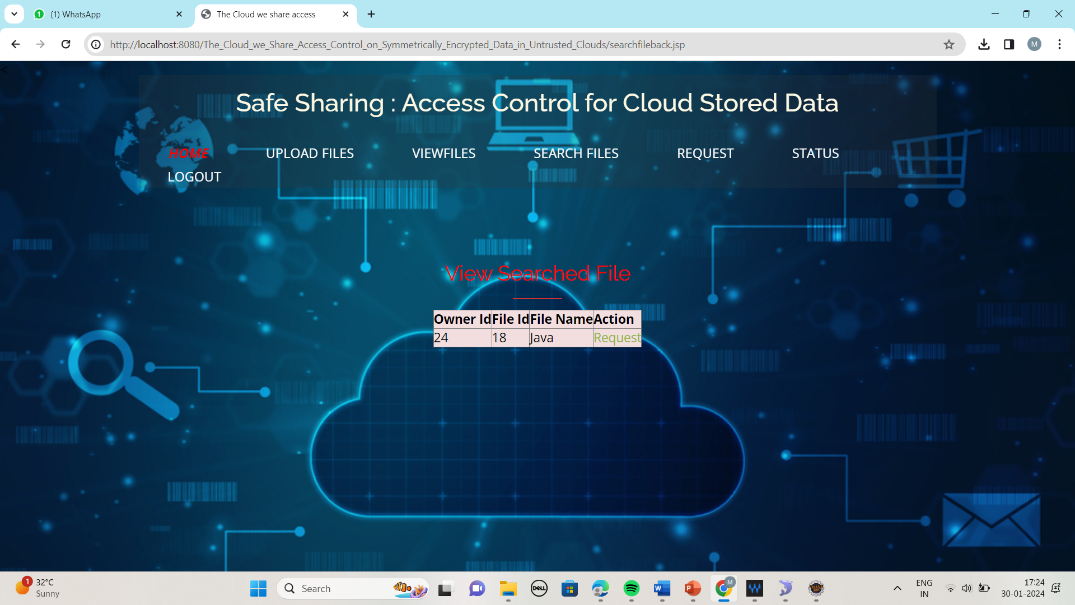
*User Files Upload*

**FIGURE 8: User Uploading Files**

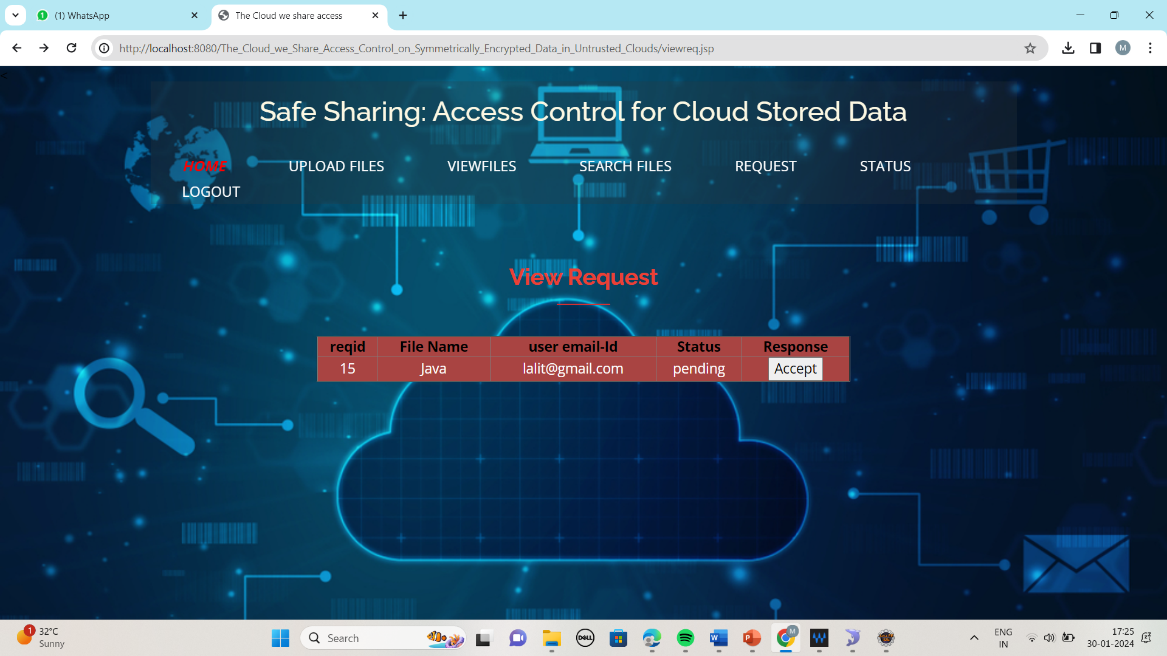
*View Files*



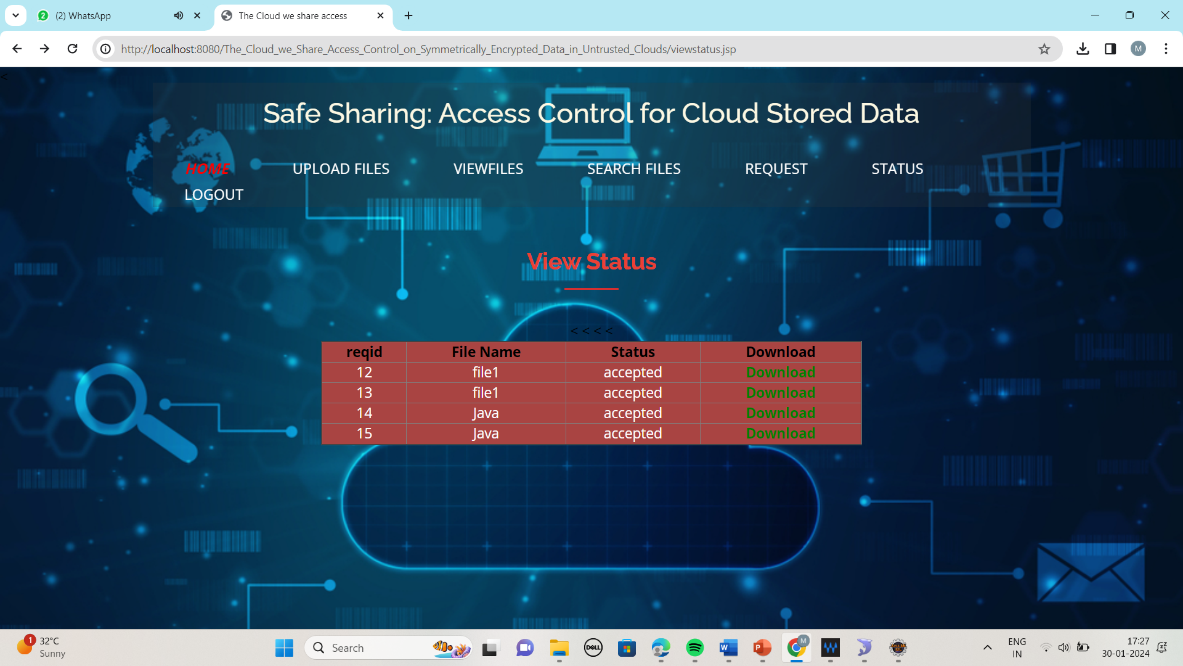
**FIGURE 9: User Viewing Files**

*Search Files*

**FIGURE 10: User Searching Files**

*Request Files*

**FIGURE 11: Request Acceptance**

*Status*

**FIGURE 12: Status of the Page**

**CONCLUSION**

Our project combines the strengths of both Symmetric Searchable Encryption (SSE) and Attribute-Based Encryption (ABE) to ensure secure data storage in cloud environments. SSE provides efficient search capabilities and protection against attacks, while ABE offers fine grained access control based on attributes and policies. By combining these two techniques, we aim to create a web application that meets the diverse security needs of our users

**FUTURE SCOPE**

In future we can implement to more security and provide two step authentication.

**REFERENCES**

**[1].** 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.

**[2].** 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.

**[3].** 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.

**[4].** 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.

**[5].** 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

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

**[7].** 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.

**[8].** 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

**[9].** 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.

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

**[11].** 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

**[12].** ringer, 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

**[13].** 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,

**[14].** R. Bost, ‘‘σ oϕoς: Forward secure searchable encryption,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 1143–1154.

**[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]** 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.

**[18]** 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.

**[19]** A. Michalas, ‘‘Text files from Gutenberg database,’’ Tampere Univ., Tampere, Finland, Tech. Rep., Aug. 2019. [Online]. Available: https://zenodo.org/record/3360392#.X7fuas0zaUk