Guarding the Cloud: Symmetric Encryption and Access Control for Untrusted Clouds

**Narasimhulu M1\*, Ajay Kishore G2, Mounika M3, Harsha Sri4 and Bhavana B5**

\* 1 Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh, India. Narasimhulu.cs@srit.ac.in

\*2 Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh, India.

204G1A0506@srit.ac.in

\*3 Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh, India

204G1A0561@srit.ac.in

\*4 Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, AndhraPradesh, India.

204G1A0536@srit.ac.in

\*5 Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh, India.

204G1A0522@srit.ac.in

***Abstract*—** The issue of safe data storage has emerged with the fast expansion of cloud environments, and both enterprises and end users must address it before sending their data online. Many alternatives have recently been put out that either use Attribute-Based Encryption (ABE) or Symmetric Searchable Encryption (SSE).SSE is a type of encryption that provides protection against both internal and external assaults. However, since everything is encrypted using a single key in an SSE scheme, cancelling access to a user would require downloading the entire encrypted database and re-encrypting it with a new key. On the other side, the issue of revocation can be resolved in an ABE system. However, because the suggested remedies are depending on the characteristics of the underlying ABE scheme, the revocation costs increase as the rules get more complicated. To this purpose, we build a hybrid encryption scheme based on ABE and SSE in such a manner that we use the greatest features of each of them by using these two cryptographic approaches that are well suited for cloud-based systems.

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

**1.INTRODUCTION:**

In cloud computing, people can quickly and easily do important things with their data, like saving, finding, and moving it. Bu there's a challenge making sure the data stays safe. This is because the data is stored with another company, and the biggest risks happen when data is not well protected. Cloud computing has developed so much over the last few years that it now has a significant impact on practically everyone's daily lives. Large enterprises and ordinary internet users alike now use the cloud on a daily basis. Many users are still hesitant to outsource their personal information, however, because cloud services are stored and managed by unreliable third parties, making the contents exposed to internal assaults.

To this purpose, both major industry actors and researchers have looked to the promising methods of symmetric searchable encryption and attribute-based encryption for solutions. Users encrypt their files locally before sending them to the Cloud Service Provider (CSP) in an SSE scheme. As a result, the CSP that does not have the encryption key is unable to obtain any useful data on the users' data.

The most intriguing aspect of SSE, though, is that it enables users to perform a direct keyword search on their encrypted data.

Sadly, SSE systems do not permit user revocation, which is a critical issue in cloud-based applications. So, removing a user is the same as downloading the whole database and encrypting it again with a new key.

ABE is a different method that works in cloud-based applications. All files in ABE schemes are encrypted using a master public key, however unlike conventional public key cryptosystems, the ciphertext produced is constrained by a policy. Additionally, each user has a special secret key linked to their qualities (such as their ID, age, organization, etc.). Therefore, a file can only be decrypted if and only if the user's characteristics match the policy associated with the ciphertext. However, it is not very effective to encrypt huge amounts of data using an asymmetric encryption algorithm.

**2. Literature Review**

**[1]** **A. Michalas, A. Bakas, H.-V. Dang, and A. Zalitko, ‘‘Access control in searchable encryption with the use of attribute-based encryption and SGX,’’ in Proc. ACM SIGSAC Conf. Cloud Comput. Secur. Workshop, 2019, p. 183**

Symmetric Searchable Encryption (SSE) is an encryption technique that allows users to search directly on their outsourced encrypted data while preserving the privacy of both the files and the queries. Unfortunately, majority of the SSE schemes allows users to either decrypt the whole ciphertext or nothing at all. In this paper, we propose a novel scheme based on traditional symmetric primitives, that allows data owners to bind parts of their ciphertexts with specific policies. Inspired by the concept of Attribute-Based Encryption (ABE) in the public setting, we design a scheme through which users can recover only certain parts of an encrypted document if and only if they retain a set of attributes that satisfy a policy. Our construction satisfies the important notion of forward privacy while at the same time supports the multi-client model by leveraging SGX functionality for the synchronization of users. To prove the correctness of our approach, we provide a detailed simulation-based security analysis coupled with an extensive experimental evaluation that shows the effectiveness of our scheme.

**[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy (SP).**

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

**[3] Y. Xu, W. Cui, and M. Peinado, ‘‘Controlled-channel attacks: Deterministic side channels for untrusted operating systems,’’ in Proc. IEEE Symp. Secur. Privacy (Oakland), May 2015, pp. 640–656.**

Multi-user oblivious storage allows users to access their shared data on the cloud while retaining access pattern obliviousness and data confidentiality simultaneously. Most secure and efficient oblivious storage systems focus on the utilization of the maximum network bandwidth in serving concurrent accesses via a trusted proxy. However, since the proxy executes a standard ORAM protocol over the network, the performance is capped by the network bandwidth and latency. Moreover, some important features such as access control and security against active adversaries have not been thoroughly explored in such proxy settings.

[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.**

Secure cloud storage is considered as one of the most important issues that both businesses and end-users take into account before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In this paper, we propose a hybrid encryption scheme that combines both SSE and ABE by utilizing the advantages of both these techniques. In contrast to many approaches, we design a revocation mechanism that is completely separated from the ABE scheme and solely based on the functionality offered by SGX.

**[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.**

Using dynamic Searchable Symmetric Encryption, a user with limited storage resources can securely outsource a database to an untrusted server, in such a way that the database can still be searched and updated efficiently. For these schemes, it would be desirable that updates do not reveal any information a priori about the modifications they carry out, and that deleted results remain inaccessible to the server a posteriori. If the first property, called forward privacy, has been the main motivation of recent works, the second one, backward privacy, has been overlooked.In this paper, we study for the first time the notion of backward privacy for searchable encryption. After giving formal definitions for different flavors of backward privacy, we present several schemes achieving both forward and backward privacy, with various efficiency trade-offs.Our constructions crucially rely on primitives such as constrained pseudo-random functions and puncturable encryption schemes.

Using these advanced cryptographic primitives allows for a fine-grained control of the power of the adversary, preventing her from evaluating functions on selected inputs, or decrypting specific ciphertexts. In turn, this high degree of control allows our SSE constructions to achieve the stronger forms of privacy outlined above. As an example, we present a framework to construct forward-private schemes from range-constrained pseudo-random functions.

**3. Problem Definition**

The increase of data breaches in the cloud computing puts all users at risk of business problems highlighting the need to improve security measures and also to mitigate the growing risk of threads faced by users in cloud

environment, pro-active measures are essential. The main goal is to create an advanced protection to user files by using different Encryption techniques like SSE and ABE at untrusted clouds.

**4.Proposed System Overview**

The proposed system works with hybrid, private or community cloud deployment models. The proposed system includes

# Encryption: The hybrid encryption system is used to encrypt the secret data in cloud

* The data will be encrypted using a public key before moving into cloud.

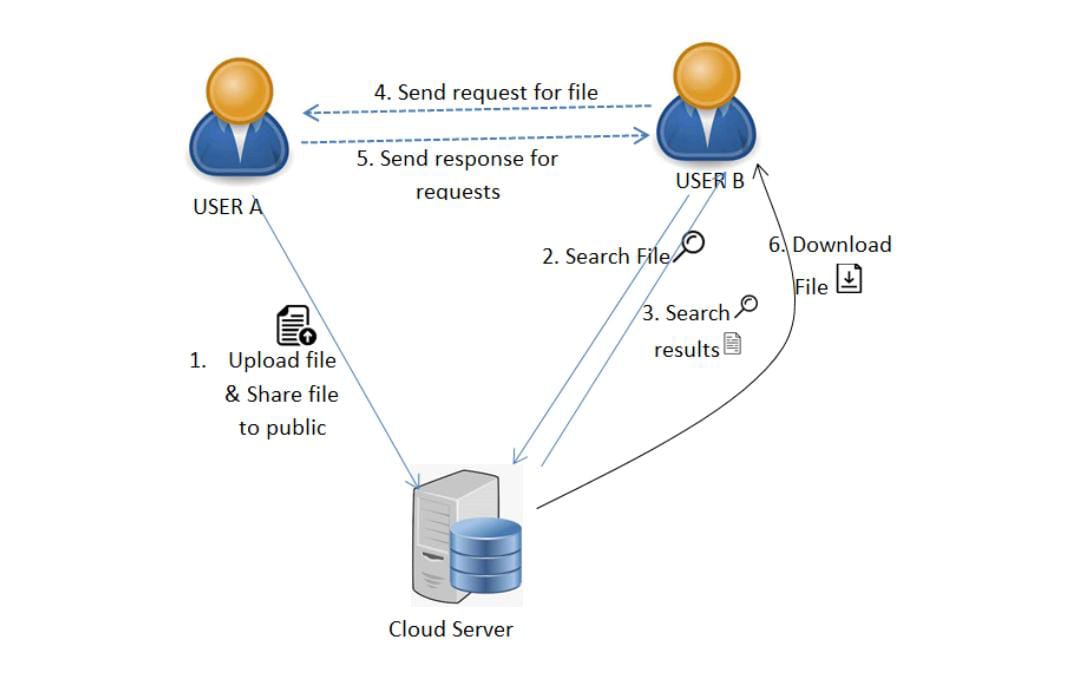
# After moving the encrypted data into the cloud, we have certain access that only particular people can access the cloud data information.

For an authenticated user, he/ she can use the cloud data information to read and modify. By using SSE Algorithm, if the user wants certain particular to be de crypted then the user can extract the particular block of code.

By using ABE Scheme, Not all people can access data only for the certain people the authentication will be given.

* These are the two cryptographic algorithms that we use.
* Here, the security will be strongly provided and also we can extract the particular code of data if we want.

**5. Methodology**

****

**User:**

**Register:** user can enter the details and he can register.

**Login:** user can login with his valid credentials. If user enter invalid credentials then its can be redirect into login page. If user enters valid credentials then it can be redirect into user home.

**Upload:** Here,User can upload the files.

While uploading the file it can be store into encrypted format and generate searchable keywords.

**View Files:** The user view the uploaded files and share files to other users.

**Search:** User can search for a file based on keywords. If file has been found send request to file uploaded user.

**View request:** In this user view the request from other users for their file then user can accept/Reject the request.

**Status:** The user view the file requested status, i.e. pending and Accepted**.**

**Download:** user can download the file if his request is accepted. Here Encryption file converted into decryption format(original File) can be Download.

**6.Result & Analysis**

**7. 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

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

**8. 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 oϕoς: 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