

Research Paper

ATTRIBUTE-BASED SEARCHABLE ENCRYPTION WITH FORWARD SECURITY FOR CLOUD-ASSISTED IOT

D. KRSHINA VENI¹, GURRAM SHIRISHA², POSHABOINA VYSHNAVI³,
ASARAPALLY MOHAN VENKATA SAI⁴, G. MAHESH⁵

¹Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

^{2, 3, 4, 5} B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

ABSTRACT— Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) is one of the most suitable encryption mechanisms in cloud environments for its fine-grained access structure and keyword retrieval capability over the ciphertext. However, in the CP-ABSE schemes, guaranteeing the forward security of the outsourced cloud data and securely deleting those no longer needed data without relying on the cloud are challenging problems. To handle such challenges, we propose a Puncturable CP-ABSE (Pun-CP-ABSE) scheme that achieves self-controlled data deletion with a fine-grained access structure under the searchable mechanism. The data

owner punctures the trapdoor to accomplish the data deletion. Then, the deletion process does not need to communicate with a trusted third party and can guarantee forward security. After the punctuation, the cloud server can no longer search for the corresponding ciphertext. Furthermore, we prove the Pun-CP-ABSE scheme is secure against the Chosen-Plaintext Attack (CPA) and Chosen-Keyword Attack (CKA). We have also implemented the Pun-CP-ABSE scheme to show its efficiency and feasibility.

Index Terms – Attribute-Based Encryption (ABE), Searchable Encryption (SE), Forward Security, Cloud-Assisted Internet of Things

(IoT), Fine-Grained Access Control, Secure Data Sharing, Ciphertext Retrieval, Cloud Storage Security, Data Privacy, Cryptographic Access Control, Encrypted Keyword Search, Secure Cloud Computing.

I. INTRODUCTION

The pervasive adoption of Internet of Things (IoT) technology has propelled the widespread integration of IoT devices into various facets of individuals' daily lives, such as smart homes, intelligent healthcare, smart industries, intelligent transportation, and other fields. The extensive employment of IoT devices brings a tremendous volume of data. The analysis and prediction of massive IoT data can contribute to developing high-quality health treatment, disaster prediction, service improvement, and efficient management. However, IoT devices' storage and processing capabilities are very limited. Therefore, the cloud-assisted IoT technology has emerged, which takes advantage of cloud service's powerful computing and storage resources at a lower cost. Furthermore, the encryption-before-outsourcing method has been used in the semi-honest cloud environment to guarantee the security of the outsourced data generated by IoT devices. However, this method hinders the searchability of the encrypted data. The

Searchable Encryption (SE) ingeniously achieves the retrieve function over ciphertext. Furthermore, efficient access control over tremendous amounts of encrypted data in the cloud is another tricky problem. Fortunately, Ciphertext- Policy Attribute-Based Searchable Encryption (CP-ABSE) effectively solves this issue with three features, ie., the one-to many encryption method, fine-grained access policy and searchability, which allows the data owner to manage, search, and decrypt the ciphertext efficiently.

The data collected by IoT devices is encrypted as ciphertexts with corresponding indexes before uploading the to the cloud. Whenever the data owner accesses the data, he sends the trapdoor to the cloud server. Then, the cloud server returns the search result if the attributes in the trapdoor satisfy the access structure and the keyword matches the indexes.

However, CP-ABSE implemented in cloud-based IoT environments still suffers from security problems. For example, some sensitive data after access or when no longer needed should be securely deleted from the cloud reliably and flexibly. If the data is deleted by the cloud, the cloud may back up the sensitive data for profit. Therefore, implementing secure data deletion without

relying on the cloud and ensuring that deleted data no longer appears is a challenging problem.

The best solution for this problem is regularly updating the trapdoor to withdraw the search ability for ciphertexts. This way, data deletion was successfully achieved without depending on the cloud.

To the best of our knowledge, the data deletion was widely studied previously, and several corresponding data deletion schemes were proposed. For example, Green and Miers first proposed Puncturable Encryption (PE) to achieve data deletion in public key encryption. In their work, the ciphertext contains a set of labels, and data deletion is performed by puncturing the secret key with a specific negative label. If the negative label could match labels in the ciphertext, then the secret key would lose the decryption capability. Phuong et al. first proposed a puncturable ABE (Pun-ABE) to implement data deletion in the ABE system. Sun et al. first combined Searchable Symmetric Encryption (SSE) with PE to propose a Pun-SSE scheme. In their scheme, puncture method was applied to achieve data deletion in the SSE system. After the puncturation, the cloud could not retrieve the deleted data.

However, the problem of data deletion has yet to be solved in the CP-ABSE scheme. To handle this problem,

we combine PE with CP-ABE and add a search function to propose a new searchable encryption mechanism, Pun-CP-ABSE, which achieves forward secure data deletion in CP-ABSE. In our scheme, the data owner generates two kinds of trapdoors named general trapdoor and puncturable trapdoor, respectively, for searching and securely deleting the outsourced data. The general trapdoor possesses the attributes to achieve access control. The puncturable trapdoor is generated by the original secret key of PE that can achieve fine-grained data deletion executed by the puncture algorithm. After the puncturable trapdoor is punctured with specific tags, the cloud server will lose searchability toward the ciphertext, which contains the same tags as in the puncturable trapdoor. The main contributions of the Pun-CPABSE are presented as follows:

- 1) We combine PE with CP-ABE to propose a Pun-CPABSE scheme that achieves precisely, permanently, fine-grandly, and self-controlled data deletion in a searchable CP-ABE mechanism. In our scheme, the data deletion process does not relay to trusted third parties such that the communication

overhead could be omitted. And the forward security is guaranteed at the same time.

2) The Pun-CP-ABSE scheme achieves fine-grained access control over the ciphertext with a keyword search, which enables the data owner to retrieve the ciphertext corresponding to the keywords if his attributes match the access structure.

3) We prove that the Pun-CP-ABSE scheme is secure under the Chosen-Plaintext Attack (CPA) and Chosen Keyword Attack (CKA). Furthermore, we present the efficiency and practicability of the Pun-CP-ABSE scheme by implementing simulations.

II. RELATED WORK

A. Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure

The exponential growth of the Internet of Things (IoT) technologies requires high data security. Here, data security is very critical as all IoT devices transfer data over the Internet. The fine-grained access control provided by the ciphertext policy attribute-based encryption (CP-ABE) technique can be considered as a potential solution to this issue. However, most of the CP-ABE schemes use bilinear pairing operations for its internal working, which is expensive for any resource constraint device. An elliptic

curve cryptography (ECC) based CP-ABE scheme can be well suited for resource constraint IoT framework because ECC takes less computational time. This article proposes a novel CP-ABE technique based on ECC to achieve fine-grained access control over data or resources. The proposed technique includes multiple attribute authorities to manage attributes and key generation, which can reduce the work overhead of having a single authority in traditional CP-ABE systems. In addition, the proposed scheme outsources the decryption process to a user assistant entity to reduce the decryption overhead of the end-users. To prove the efficiency of the proposed scheme, both formal security analysis and performance comparisons are presented in this article. The result and findings prove the effectiveness of the proposed scheme over some well-known schemes.

B. Extracting spatial information of IoT device events for smart home safety monitoring

Smart home IoT devices have been widely deployed and connected to many home networks for various applications such as intelligent home automation, connected healthcare, and security surveillance. The network traffic traces generated by IoT devices have enabled recent research

advances in smart home network measurement. However, due to the cloud-based communication model of smart home IoT devices and the lack of traffic data collected at the cloud end, little effort has been devoted to extracting the spatial information of IoT device events to determine where a device event is triggered. In this paper, we examine why extracting IoT device events' spatial information is challenging by analyzing the communication model of the smart home IoT system. We propose a system named IoT Duet for determining whether a device event is triggered locally or remotely by utilizing the fact that the controlling devices such as smartphones and tablets always communicate with cloud servers with relatively stable domain name information when issuing commands from the home network. We further show the importance of extracting spatial information of IoT device events by exploring its applications in smart home safety monitoring.

C. Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system

The cloud-assisted mobile electronic health (e-health) system facilitates e-health data sharing between healthcare providers and patients, but also raises the security and

privacy concerns of e-health data. Although Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been a promising technique to achieve fine-grained access control over encrypted e-health data, it still incurs high encryption and decryption burdens on mobile users such as smartphones and sensors. In addition, malicious cloud servers may conduct incorrect operations due to various interest incentives (e.g., leaking sensitive information to illegal users, saving computation and storage costs). To solve the above issues, in this paper we first propose an Outsourced CP-ABE (OABE) with verifiable encryption scheme by splitting secret keys corresponding to an attribute set and using the short signature, which not only reduces the encryption and decryption complexities of mobile users but also guarantees that cloud servers correctly perform encryption operations. Then, we extend OABE to construct outsourced CP-ABE with verifiable decryption (OABE+) by utilizing the verifiable tag mechanism, which guarantees that cloud servers correctly conduct the ciphertext transformation. Formal security analysis proves that our schemes are selectively secure against unauthorized accesses and malicious operations. Extensive experiments using various real-world datasets

demonstrate that our schemes are efficient and feasible in real applications.

III. PROPOSED METHODOLOGY

We propose a Puncturable CP-ABSE (PunCP-ABSE) scheme that achieves self-controlled data deletion with a fine-grained access structure under the searchable mechanism.

The data owner punctures the trapdoor to accomplish the data deletion. Then, the deletion process does not need to communicate with a trusted third party and can guarantee forward security.

After the punctuation, the cloud server can no longer search for the corresponding cipher text. We prove that the Pun-CP-ABSE scheme is secure under the Chosen-Plaintext Attack (CPA) and Chosen Keyword Attack (CKA). Furthermore, we present the efficiency and practicability of the Pun-CP-ABSE scheme by implementing simulations.

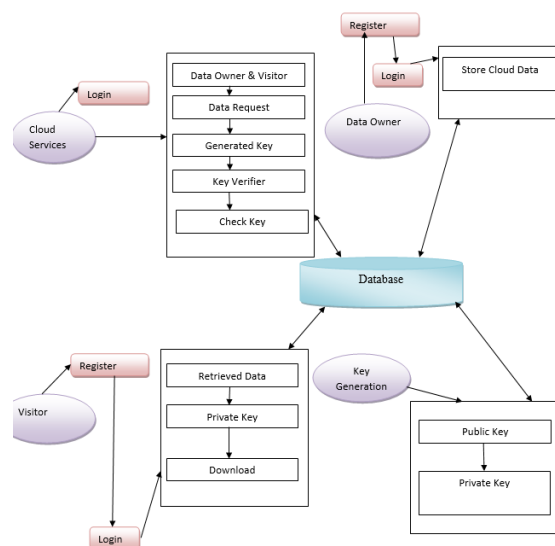
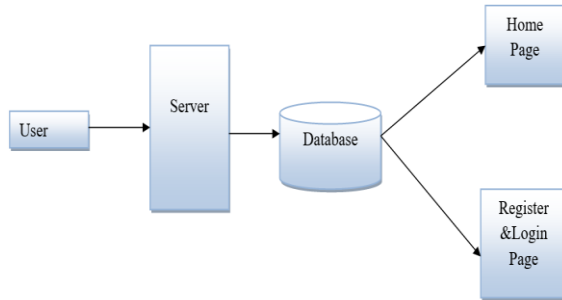


Fig. 1: System Overview

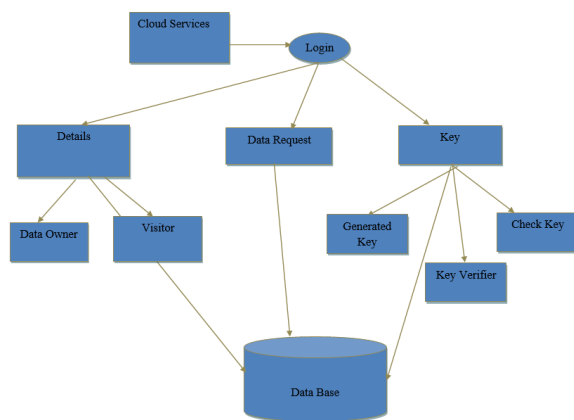
1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



2. Cloud Services

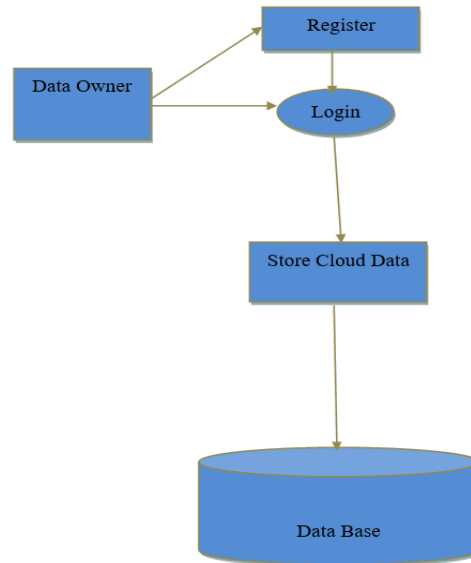
Cloud services has an id and password. Cloud services has a details of a data owner and visitor details. The cloud services have a data request to share a data. The cloud services has a key generate a key. The cloud services has a key verifier to share a data. The cloud services has a check a key to download whether the cloud services key are match the decrypt a visitor.



3. Data Owner

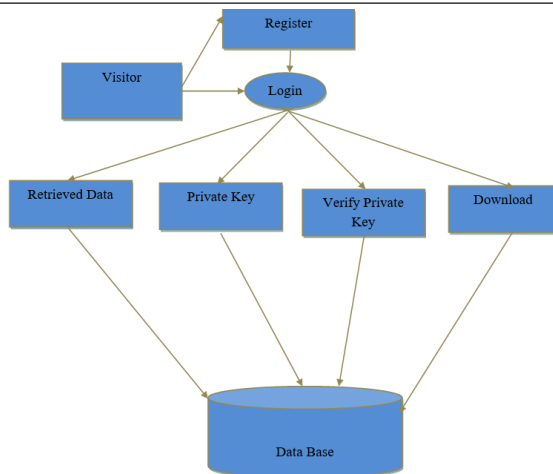
The data owner has a register with a detail. The data owner has a login with a user id and

password. The data owner has a store a cloud data to share in a database.



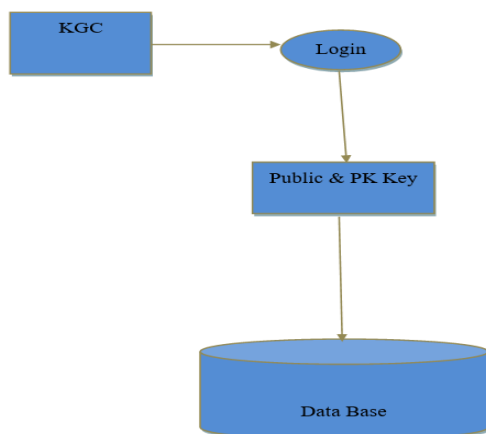
4. Visitor

The Visitor module has a register with all details. The visitor has a login with a user id and password. The visitor has a retrieved a data to get from a data owner. The visitor have a private key to generated a data. The private key has a verify a cloud services if the private key has match the data will be decrypt a data.



5. Key Generation Center

Key generation center has a fifth module. KGC has a public and private key has generated by data sharing in a database.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrate that the scheme enables efficient keyword search over encrypted IoT data while preserving fine-grained access control. The forward

security mechanism effectively prevents compromised keys from exposing previously encrypted data with minimal computational overhead. Compared with existing searchable encryption methods, the proposed approach achieves lower search latency, improved data confidentiality, and scalable performance, making it well suited for secure cloud-assisted IoT environments.



Fig. 2: Home Page

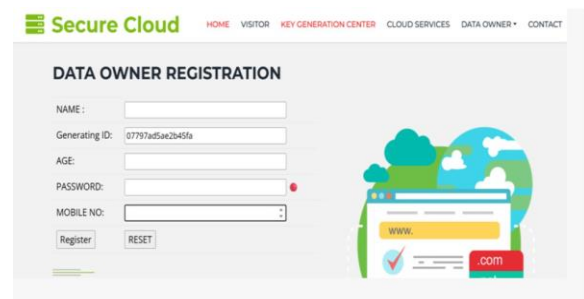


Fig. 3: Data Owner Registration

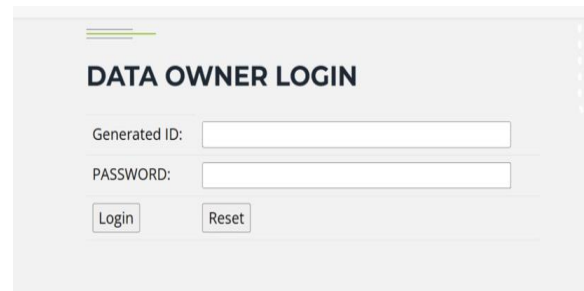


Fig. 4: Data Owner Login

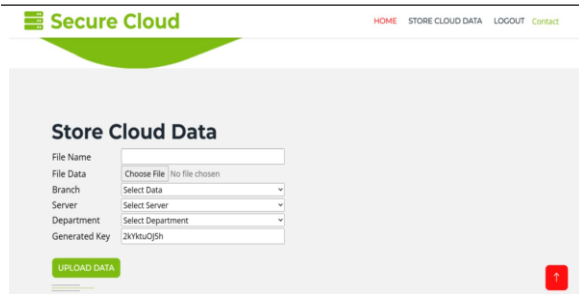


Fig. 5: Store Cloud Data

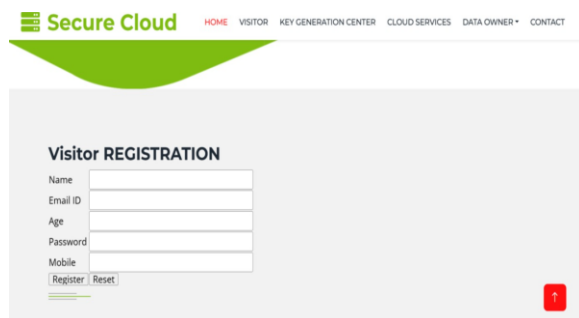


Fig. 6: Visitor Registration

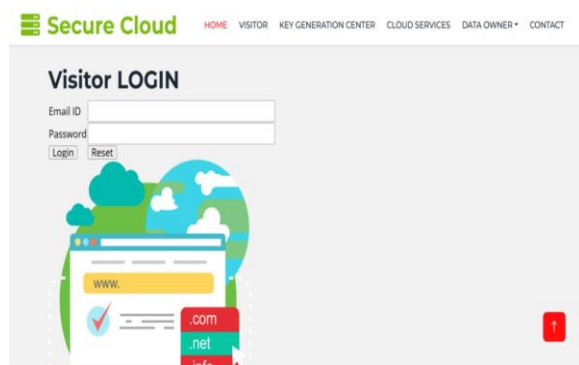


Fig. 7: Visitor Login

V. CONCLUSION

In this paper, we have introduced an advanced self-controlled data deletion scheme within a searchable mechanism. This scheme empowers DOs to effectively and permanently delete the ciphertext by

puncturing their trapdoors with specific labels corresponding to the ciphertext. The data deletion process does not relay to trusted third parties, which will not generate additional communication overhead, and the data deletion process ensures forward security

REFERENCES

- [1] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 821–829, Jan. 2023.
- [2] Y. Wan, X. Lin, K. Xu, F. Wang, and G. Xue, "Extracting spatial information of IoT device events for smart home safety monitoring," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2023, pp. 1–10.
- [3] Y. Miao, F. Li, X. Li, J. Ning, H. Li, K. R. Choo, and R. H. Deng, "Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system," *IEEE Trans. Dependable Secure Comput.*, early access, Jul. 4, 2023, doi: 10.1109/TDSC.2023.3292129.
- [4] D. Ghopur, J. Ma, X. Ma, Y. Miao, J. Hao, and T. Jiang, "Puncturable ciphertext-policy attribute-based encryption scheme

for efficient and flexible user revocation,”
Sci. China Inf. Sci., vol. 66, no. 7, Jul.
2023, Art. no. 172104.

- [5] X. Feng, J. Ma, S. Liu, Y. Miao, X. Liu, and K. R. Choo, “Transparent ciphertext retrieval system supporting integration of encrypted heterogeneous database in cloud-assisted IoT,” IEEE Internet Things J., vol. 9, no. 5, pp. 3784–3798, Mar. 2022.
- [6] T. Liu, Y. Miao, K. R. Choo, H. Li, X. Liu, X. Meng, and R. H. Deng, “Time-controlled hierarchical multikeyword search over encrypted data in cloud-assisted IoT,” IEEE Internet Things J., vol. 9, no. 13, pp. 11017–11029, Jul. 2022.

AUTHORS Profile



Ms. D. KRSHINA VENI

has received her B.Tech from JNTUH, Hyderabad in 2011, M.Tech degree in Computer science from JNTUH, Hyderabad in 2021 and Pursuing Ph.D degree in Computer Science from Guru Nanak University, Ibrahimpatnam. She is dedicated to teaching field from the last 8 years. Her research area Machine Learning. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.



Ms. GURRAM

SHIRISHA pursuing B. Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. POSHABOINA

VYSHNAVI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions

Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. ASARAPALLY
MOHAN VENKATA**

SAI pursuing B. Tech
degree in Computer
Science and
Engineering at Guru

Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.



Mr. G MAHESH

pursuing B. Tech degree
in Computer Science
and Engineering at Guru
Nanak Institutions
Technical Campus

affiliated to JNTUH in 2022-2026.