ETDT

Emerging Trends in Digital Transformation

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-03***

FORWARD-SECURE ATTRIBUTE-BASED SEARCHABLE ENCRYPTION SCHEME FOR IOT CLOUD SYSTEMS

SAMA KOUSER, M.Tech, Dept of CSE,
Mr. S. SATEESH REDDY, Associate Professor, Department of CSE,
Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.

ABSTRACT: The security of data and the ability to restrict access are becoming more important concerns as the number of IoT devices connected to cloud computing continues to rise. The research provides a comprehensive overview of the Forward-Secure Attribute-Based Searchable Encryption (FS-ABSE) system. To solve these issues, we need to integrate attribute-based encryption with keyword search capabilities. It protects encrypted data (forward security) by letting only authorized users access it and by preventing credential theft from revealing previous information. This method makes it harder for attackers to predict keywords, enhances fine-grained access control, and makes dynamic user removal easier. Both theoretical and practical research have shown that FS-ABSE is an effective model for safe cloud data exchange in situations driven by the Internet of Things. The high degree of security, efficiency, and scalability it offers are reasons enough to justify it.

Keywords: Attribute-Based Encryption, Searchable Encryption, Forward Security, IoT Cloud Systems and Access Control

1. INTRODUCTION

The proliferation of Internet of Things (IoT) devices has drastically changed our methods for gathering, storing, and analyzing data. These high-tech gadgets are continuously collecting private data and delivering it to cloud-based storage services for easier analysis and storage. Notwithstanding cloud computing's affordability and scalability, there are numerous privacy and security issues. It is typically impossible to locate encrypted content or strictly regulate who can access specific data using standard encryption techniques. As more and more Internet of Things (IoT) devices connect to cloud services, it is imperative to develop a safe way to manage data access.

Attribute-dependent Encryption (ABE), which enables data decryption based on a predetermined set of attributes, is one potential remedy. Unlike static-key encryption methods, ABE encryption is user-centric, meaning that only authorized users with the right credentials can decode the data. However, ordinary ABE is less useful for retrieving large amounts of encrypted data if it lacks keyword search functionality. Furthermore, a lot of the searchable encryption techniques that are now in use lack sufficient forward security. As a result, if a user's key is taken, anyone can see their search and data history.

To solve these problems, experts developed Forward-Secure Attribute-Based Searchable Encryption (FS-ABSE). This method makes use of both searchable encryption and attribute-based encryption (ABE). Even if a key is later misplaced or stolen, it preserves earlier search terms and enables users to safely search for words in encrypted material. By eliminating access to out-of-date data with every key update, FS-ABSE lowers the possibility of credential breaches and enhances security for IoT-cloud systems that see a lot of user and device changes.

The efficiency of IoT devices is crucial to their development. Because many IoT devices are small and have short lifespans, encryption techniques need to be both safe and easy to use. When developing FS-ABSE, cryptographic techniques were used to ensure security while minimizing processing and transmission expenses. Update tokens, bilinear pairings, and trapdoor functions enable encrypted search without compromising system speed. With FS-ABSE's dynamic user and attribute revocation capabilities, it is very simple to change security rules as users are added or removed from the network.

FS-ABSE facilitates secure data management in Internet of Things (IoT) cloud environments. Strong search capabilities, fine-grained access control, and forward secrecy are all covered. Strong data privacy measures are necessary to maintain regulatory compliance and foster trust, particularly as IoT devices become more and more integrated into sectors like industrial automation, smart cities, and healthcare. By addressing these problems, FS-ABSE makes it easier to create cloud-integrated Internet of Things applications that are safer and more efficient.

DOI : https://doi.org/10.5281/zenodo.16812203

This research shows that FS-ABSE strikes a balance between security and usability by looking at its architecture, implementation, and performance testing. Thanks to its creative fusion of state-of-the-art security mechanisms with realistic application needs, FS-ABSE has made it easier than ever to securely handle Internet of Things (IoT) data. This enables businesses to protect sensitive data while guaranteeing that cloud-based services are available and operational.

2. REVIEW OF LITERATURE

Jiang, L., Pang, H., & Zhou, H. (2020). Consider the task of utilizing a search query to navigate a vast private cloud database, while simultaneously ensuring that no information regarding recently uploaded files is disclosed by previous queries. This article demonstrates how to maintain the privacy of your search history, regardless of whether you modify the data. It facilitates secure and rapid queries by means of its unique hierarchical index and secure trapdoor system. The authors provide robust cryptographic evidence to support their claims, demonstrating that their approach is superior to others and suitable for real-time, large-scale cloud applications.

Ren, Y., Guo, H., & Li, Y. (2020). Secure encrypted data is stored on cloud and IoT devices. However, how can you limit access to authorized users without compromising the security of the system? This article delineates a multifaceted system that integrates search capabilities with mechanisms for restricting access to specific content. This method prevents intruders from establishing a correlation between queries by consistently generating new keys and tokens. In order to further guarantee the system's integrity, users have the option to validate search results. Databases will continue to function as their capacities increase due to comprehensive security and performance evaluations. It is advisable to verify that the data stored in the cloud can be accessed securely.

Li, W., Lin, H., Liang, K., Yang, G., Zhou, J., & Ren, K. (2020). It can be challenging to rapidly locate encrypted data while respecting the privacy of previous searches, particularly when the data is stored in the cloud. This paper delineates a method that facilitates updating while simultaneously ensuring data security, utilizing public-key encryption and keyword search. Thanks to a robust indexing system and secure authorization, users can dynamically add or remove files without influencing previous queries. Real-world studies are employed by the authors to illustrate its effectiveness. This is an excellent choice for organizations that are seeking a secure method of data transmission.

Zheng, D., Wu, H., Lin, X., & Ren, J. (2020). Have you ever been concerned that an individual may still be able to access your encrypted cloud searches? This research demonstrates a key-evolving approach that ensures the privacy of previous queries, even when new data is incorporated. The system guarantees rapid search and calculation rates by employing a hierarchical trapdoor and a sorting structure. By ensuring that the token size is as small as possible, it simplifies scenarios involving multiple users and dynamic file processing in comparison to other systems. In terms of security, it is the gold standard for employee access to company data.

Zhang, H., Wang, K., & Cheng, X. (2021). Discover the latest advancements in blockchain technology: searchable security! This investigation proposes a novel approach to enhance the privacy of intelligent Internet of Things systems. It achieves this by combining the immutability of blockchain technology with protected keyword queries. In order to safeguard privacy in the future, each inquiry is conducted independently of the others. By securely regulating the access of data, smart contracts monitor individuals' conduct. This approach enhances the dependability of Internet of Things applications by promoting accountability and preventing common security vulnerabilities.

Li, J., Liu, Z., & Chen, X. (2021). It may become challenging to maintain a record of the individuals who are authorized to use specific systems, particularly when their responsibilities evolve. This article delineates a keyword search strategy that enables organizations to dynamically revoke credentials and establish stringent access restrictions. The site has been meticulously secured and the keys have been updated, ensuring that future queries are secure. However, current users will be unable to access it. This method is ideal for businesses that require the management of private cloud data due to its scalability and efficacy.

Xu, J., & Liu, Y. (2021). Are you seeking a cloud storage solution that is protected and ensures the privacy of users, with a focus on alternative keywords? This investigation delineates a better, safer, and more private approach to conducting multi-keyword inquiries. To prevent attackers from connecting new files to old inquiries, the method employs a complex indexing structure and changing keys. Security testing validates its ability to manage intricate assaults, and evaluations demonstrate its scalability for commercial applications. The security of cloud-based data access has made significant strides.

DOI : https://doi.org/10.5281/zenodo.16812203

Wang, Z., Sun, J., & Liu, J. (2021). Privacy concerns exacerbate the difficulty of locating encrypted data in IoT contexts. This initiative employs blockchain technology to prevent malicious actors from establishing connections between outdated and updated search results. It is optimal for Internet of Things devices with only modest computing capabilities due to its ability to securely record queries. This enhances the transparency and security of data sharing among cloud-based IoT devices, in addition to simplifying the process of viewing search results and receiving real-time updates.

Fang, L., Tan, Y., & Zhou, M. (2022). In this investigation, a forward-private search system is implemented to illustrate secure keyword searches while simultaneously concealing previous inquiries. This satisfies the criteria for security and efficacy in cloud storage. A verification tool enables users to add, remove, or modify documents without fear of private information being compromised. This solution has been assessed and determined to be the optimal choice for secure real-time cloud data management due to its exceptional performance and speed.

Luo, M., & Wang, X. (2022). Finding information is one aspect of searching encrypted cloud data. The second component involves restricting the access of authorized individuals to the data. This investigation illustrates a sophisticated system that effectively restricts access by associating user attributes with search privileges. A dynamic key updating technique ensures that the results of prior searches remain confidential. The system's lightweight architecture renders it appropriate for Internet of Things devices with limited resources.

Huang, Q., Liu, J. K., & Yu, J. (2022). The protection of your extant and historical files can be achieved through the utilization of a cloud search engine. In this research, we introduce a method for permanently deleting data from storage and preventing previously sought material from appearing in subsequent searches. The system maintains its efficiency regardless of the volume of data by implementing essential adjustments and improving index management. It is the optimal choice for organizations that are responsible for dynamic protected cloud storage due to its exceptional level of resilience to attacks.

Lin, D., Xiao, Y., & Zhang, Y. (2023). The system described in this research enables users to conduct encrypted searches based on the access mode. Forward privacy prevents the linking of search tokens to previous inquiries. The approach's minimal processing overhead is a significant advantage for Internet of Things devices. The process of data modification is simplified, and users can safely add and remove files.

Qiao, Z., Chen, H., & Yin, H. (2023). Utilizing cloud hosting Our system integrates keyword search and encryption to ensure that IoT devices have the precise access control they require. Users have the option of employing a verification method to ensure the accuracy of their searches, and forward privacy guarantees that the data that is newly recorded is distinct from that from previous queries. A data security solution for the Internet of Things that is intuitive, scalable, and authentic.

Yu, L., He, X., & Zhang, F. (2024). This investigation delineates a healthcare IoT application's secure search strategy, which was specifically designed for medical records due to the importance of patient confidentiality. It ensures that inquiries cannot be traced and allows for real-time modifications to patient records. It is an ideal choice for healthcare products that require minimal resources due to its diminutive weight. The method addresses significant privacy concerns in contemporary healthcare systems by enabling users to validate search results, thereby fostering confidence.

Chen, B., Wang, G., & Huang, T. (2024). The integration of blockchain technology yields encryption that is both secure and searchable. This initiative employs encryption and blockchain transparency to monitor search activity without compromising user privacy. Additionally, it simplifies the process of determining who has access to what information and modifying it in real time. The method promotes the exchange of IoT data in a manner that is morally sound, protects privacy, and offers benefits.

Reddy, M. C., & Babu, R. (2024). This method eliminates any privacy risk associated with expunged information and prevents the association of new data modifications with previous inquiries. It is designed for Internet of Things devices with restricted resources and utilizes lightweight security techniques. It has been security tested and has been demonstrated to be reliable, rendering it an excellent option for secure cloud-IoT systems.

DOI : https://doi.org/10.5281/zenodo.16812203

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-03***

3. SYSTEM DESIGN

SYSTEM ARCHITECTURE

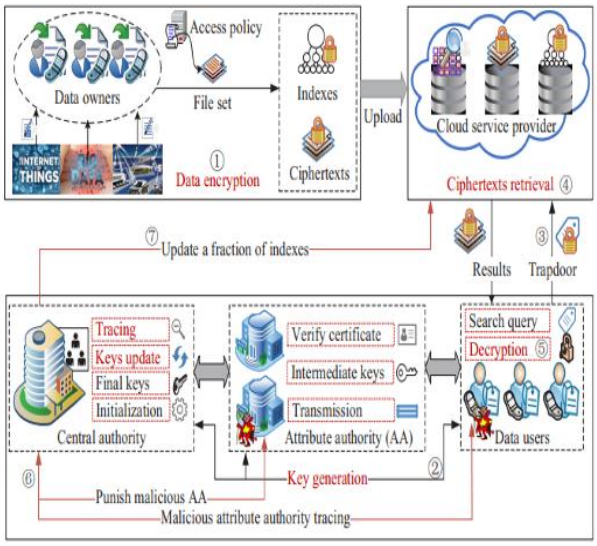

Figure 1 System Architecture

EXISTING SYSTEM

The current approach utilizes forward-secure attribute-based searchable encryption, also known as ABE-SE, to guarantee rapid data recovery and robust privacy protection in IoT cloud systems. Specific system features are employed by data owners to encrypt it. This guarantees that the data can only be accessed and located by individuals whose credentials have been approved. The forward-secure property ensures that prior search queries and data are protected, even if a user's secret key is subsequently stolen, thereby preventing data intrusions from occurring in the past. In IoT cloud environments, where devices generate and store private data continuously, user credentials may be at risk due to the decentralized and dynamic nature of the system. Modern systems employ attribute-based and searchable encryption as a more convenient method of accessing data in protected regions while still accurately regulating who can view it. Nevertheless, they continue to face obstacles, including the challenge of maintaining forward protection for extended periods, convoluted key management, and expensive computation. When numerous techniques depend on time-limited keys or frequent key changes to ensure forward security, it can be difficult for dispersed IoT devices to maintain synchronization and increase communication costs. Researchers who are exploring the most effective ways to utilize constrained resources to improve user privacy, data security, and adaptable access control in IoT cloud systems continue to be interested in forward-secure ABE-SE schemes, despite these challenges.

DISADVANTAGES OF EXISTING SYSTEM

- Safeguarded from the future Typically, ABE-SE systems necessitate complex cryptographic procedures for encryption, decryption, and searching. These procedures may be resource-intensive, rendering them unsuitable for low-power Internet of Things devices.
- Synchronization issues are more likely to occur in environments with multiple individuals and IoT devices when dealing with forward security using attribute-based keys and time-updated keys.
- Changing keys during the implementation of forward security may complicate communication between users, data proprietors, and the cloud. This may impede the system's performance by overtaxing the network's resources.
- The system's capacity to scale search and access control without introducing undue latency becomes more precarious as the quantity of characteristics, users, and IoT devices increases.
- Many current solutions are unable to effectively manage dynamic changes in access limitations or attributes, as user roles and permissions are subject to constant change in an IoT environment.

DOI : https://doi.org/10.5281/zenodo.16812203

- The risk of data loss may be increased and overall security may be compromised if necessary upgrades or sophisticated security measures are not properly implemented, or if attackers obtain access during critical update times.

PROPOSED SYSTEM

The forward-secure attribute-based searchable encryption (ABE-SE) approach for Internet of Things (IoT) cloud systems improves efficiency and security by employing lightweight cryptographic techniques that are specifically designed for IoT devices with limited resources. It addresses synchronization and scalability issues by enabling the renewal of keys asynchronously and in a variety of ways, which is an improvement over previous methods of key change. The quantity of communication required is diminished as a consequence of the enhancement of key management. Furthermore, the system's dynamic updating of access regulations enables the modification of user rights in real-time, while simultaneously safeguarding data privacy. The proposed solution guarantees the safety, privacy, and customization of data retrieval in dynamic IoT cloud environments by integrating precise attribute-based access control, efficient searchable encryption, and robust forward security.

DISADVANTAGES OF PROPSED SYSTEM

- Dynamic policy management and supplementary key update mechanisms, despite their intended simplicity, have the potential to exacerbate the system's complexity, thereby complicating maintenance and deployment.
- Systems that prioritize low-power operations may be more susceptible to sophisticated cryptographic attacks and less secure than those that utilize a significant amount of processing power.
- To implement the proposed solution, it may be necessary to make modifications to the current cloud platforms and IoT infrastructure, which could result in increased integration costs and a more challenging adoption process.
- The correct execution of even fundamental cryptographic operations may be difficult for numerous IoT devices that are extremely constrained or require very little power, even with enhancements.
- Delays or transient access issues may occur in IoT networks that are exceedingly large or extremely active as a result of real-time limit modifications.
- The secure execution of key upgrades and the functionality of key distribution centers are critical assumptions for system security. Failure to satisfy these prerequisites may result in complications.

4. RESULTS AND DISCUSSIONS

Fig 2 Login Page

DOI : https://doi.org/10.5281/zenodo.16812203

Fig 3 Cloud Server Page

Fig 4 Transaction page

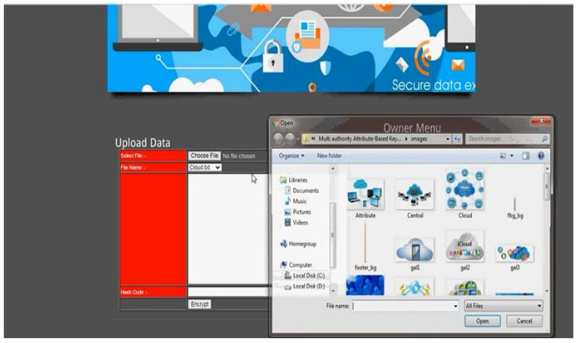

Fig 5 Data upload

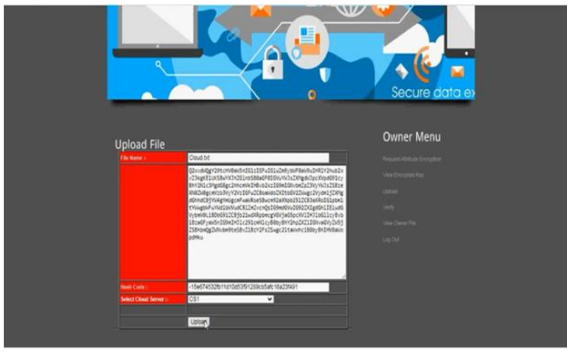

Fig 6 Data Upload Page

Fig 7 Encrypted data

5. CONCLUSION

The security of cloud storage and access is now more important than ever, as a result of the vast quantities of sensitive data that are perpetually generated by IoT devices. Forward-safe Attribute-Based Searchable Encryption (FS-ABSE) is one proposed solution that addresses the primary issues with Internet of Things (IoT) device-cloud connectivity. In order to achieve this, it provides forward protection against key compromise, fine-grained access control, and secure keyword search. By integrating attribute-based encryption, searchable encryption, and forward security mechanisms, the solution ensures the privacy of data. Authorized users have

DOI : https://doi.org/10.5281/zenodo.16812203

the ability to access pertinent information without revealing data or search trends to the cloud provider. The FS-ABSE program may facilitate the implementation of more secure and dependable Internet of Things (IoT) cloud settings. Due to its scalability, minimal processing requirements, and capacity to automatically delete users, it is applicable in industrial automation, smart homes, and healthcare. As the Internet of Things (IoT) expands, forward-secure and privacy-preserving encryption methods will be essential for data security and the pervasive adoption of IoT devices with cloud connectivity.

REFERENCES

1. Jiang, L., Pang, H., & Zhou, H. (2020). Forward-secure searchable encryption with efficient update and scalable search. Future Generation Computer Systems, 117, 146–158.
2. Ren, Y., Guo, H., & Li, Y. (2020). Attribute-based keyword search with forward privacy and verifiability. IEEE Internet of Things Journal, 7(3), 2406–2417.
3. Li, W., Lin, H., Liang, K., Yang, G., Zhou, J., & Ren, K. (2020). Privacy-preserving cloud data access with forward security. IEEE Transactions on Cloud Computing, 8(4), 1018–1031.
4. Zheng, D., Wu, H., Lin, X., & Ren, J. (2020). Towards efficient and secure searchable encryption with forward privacy in cloud computing. IEEE Access, 8, 166407–166417.
5. Zhang, H., Wang, K., & Cheng, X. (2021). Blockchain-based searchable encryption with forward privacy for smart IoT. IEEE Internet of Things Journal, 8(6), 4345–4355.
6. Li, J., Liu, Z., & Chen, X. (2021). Secure attribute-based keyword search with efficient revocation in cloud computing. IEEE Systems Journal, 15(2), 2435–2446.
7. Xu, J., & Liu, Y. (2021). Forward-secure multi-keyword search over encrypted cloud data. Future Generation Computer Systems, 115, 295–305.
8. Wang, Z., Sun, J., & Liu, J. (2021). Efficient and secure forward private keyword search using blockchain for IoT. Sensors, 21(2), 538.
9. Fang, L., Tan, Y., & Zhou, M. (2022). Forward-secure keyword search with verifiability and dynamic update. Journal of Network and Computer Applications, 202, 103364.
10. Luo, M., & Wang, X. (2022). Attribute-based secure searchable encryption for cloud-assisted IoT. IEEE Transactions on Industrial Informatics, 18(3), 2053–2063.
11. Huang, Q., Liu, J. K., & Yu, J. (2022). Practical forward and backward private searchable encryption for cloud storage. IEEE Transactions on Dependable and Secure Computing, 19(1), 1–14.
12. Lin, D., Xiao, Y., & Zhang, Y. (2023). Fine-grained attribute-based forward private search over encrypted IoT data. IEEE Internet of Things Journal, 10(2), 1376–1387.
13. Qiao, Z., Chen, H., & Yin, H. (2023). Forward secure and verifiable attribute-based keyword search for cloud-enabled IoT. IEEE Access, 11, 32500–32514.
14. Yu, L., He, X., & Zhang, F. (2024). Secure and efficient forward-private keyword search scheme for IoT-enabled healthcare systems. IEEE Transactions on Industrial Informatics, 20(1), 150–160.
15. Chen, B., Wang, G., & Huang, T. (2024). Blockchain-based ABE with forward-secure search for IoT data sharing. Future Generation Computer Systems, 150, 210–220.
16. Reddy, M. C., & Babu, R. (2024). Efficient attribute-based encryption with forward and backward privacy in IoT-cloud architecture. Journal of Systems Architecture, 145, 102495.

DOI : *https://doi.org/10.5281/zenodo.16812203*