

How to Cite:

Krishna, K. J., Babu, S. A., Babu, I. J., Manikanta, J., Naidu, U. R., & Reddy, I. H. (2022). Attribute-based keyword search across encrypted cloud data with multiple authorities. *International Journal of Health Sciences*, 6(S5), 8192–8202. <https://doi.org/10.53730/ijhs.v6nS5.11383>

Attribute-based keyword search across encrypted cloud data with multiple authorities

K Jaya Krishna

Asst. Professor, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Sk Anjaneyulu Babu

Asst. Professor, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Inaganti Jagadeesh Babu

PG Scholars, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Jade Manikanta

PG Scholars, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Utlapalli Ramesh Naidu

PG Scholars, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Inakollu Hemanth Reddy

PG Scholars, Department of MCA, QIS College of Engineering & Technology (Autonomous), Ongole, AP, India

Abstract---Searchable Encryption (SE) is a crucial technique for cloud data security and usability (SE). When employing Ciphertext Policy Attribute-Based Encryption (CP-ABE) and the Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS), encryption and access control may be done simultaneously. A single attribute authority is responsible for authenticating user certificates and delivering secret keys in current CP-ABKS systems. A single point of failure results in distributed cloud systems. To address these difficulties, we explain in this paper the MABKS system, which is designed to help cloud devices with limited computing and storage capabilities. The MABKS system has added capability for tracing and modifying malicious attribute authority. According to our detailed security investigation, the MABKS system is safe in both selective-matrix and selective-attribute models.

Our trials using real-world datasets have shown the MABKS system's efficiency and usefulness.

Keywords---Searchable Encryption (SE), Ciphertext Policy Attribute-Based Encryption (CP-ABE), Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS), MABKS.

1. Introduction

Cloud computing and the Internet of Things (IoT) have led to a growth in the usage of cloud-assisted outsourced services. By offloading huge amounts of data (such as medical records) to a third-party cloud server, resource-constrained devices (such as mobile terminals and sensor nodes) can minimise their local data storage and computation requirements. Data outsourcing raises the risk of private information being compromised. It is common practise to encrypt data before moving it to a cloud environment that is less trustworthy or damaged to protect data security and privacy. Encrypted cloud data cannot be retrieved or searched for. There has been a rise in popularity of SE systems since they provide secure searches and selective recovery of encrypted cloud data based on user-specified keywords. In order to safeguard client data while yet allowing them to get it, cloud solutions must also offer fine-grained access control. One of the most helpful techniques for retrieving ciphertext and controlling access is the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS). Users' certificates and secret keys are verified and distributed by a single attribute authority in most existing CP-ABKS schemes[4],[5],[12],[13],[14]. Due to a single attribute authority, large-scale distributed cloud systems have low resilience and inefficiency. Taking down or hacking into this one attribute authority puts the entire cloud service at risk (e.g., being unavailable during that period). A considerable time may elapse before data consumers receive their secret keys, for example.

We describe a Multi-Authority Attribute-Based Keyword Search (MABKS) solution to overcome the challenges that cloud systems face due to single-point performance bottlenecks and massive storage and computation requirements (which are unrealistic for resource-limited devices). FIG. 1 shows the MABKS system's multi-authority design, which varies greatly from single-authority systems. The MABKS system's AAs must check the certificates of data users and produce intermediate secret keys for them, which are subsequently forwarded to the CA, which generates the final secret keys for DUs. Employees who need access to sensitive company information may be able to get it from only one department of a large corporation, but this department will be burdened with computation overhead as the number of employees grows, and it could even become a performance bottleneck if it is compromised or fails. If the fully-trusted division is overburdened, public servers (AAs) can be hired from other parties (such as Tencent, Amazon, Alibaba, and so on). This firm's fully-trusted department will get erroneous intermediate secret keys from these public servers in order to preserve computing and bandwidth. In addition, because of the high communication costs associated with setting up security channels, we are unable to use as many fully-trusted AAs in our schemes as we would want. Our MABKS CA allows us to trace down this nefarious AA.

Multiple levels of power in the architecture. For example, the hierarchical structure of the MABKS system allows multiple AAs to perform the time-consuming user certificate validation and intermediate secret key generation on behalf of the CA, thereby greatly reducing the CA's computation requirements, unlike the previous single authority CP-ABKS schemes [13, 14]. (or traditional multi-authority CP-ABE schemes [16], [17], [19]). Files may be searched for keywords. [4], [5], [12] are examples of CP-ABKS approaches that separate encrypting and constructing indexes, whereas the MABKS system combines these two steps into a single operation. Data owners may now regulate access to encrypted cloud data using the MABKS system while simultaneously allowing cloud clients (such as data owners and users) to access keyword-based ciphertexts.

2. Related Work

It's an Encryption That You Can Search For

The SE approach, which enables cheaper access to massive quantities of computing and storage resources, has sparked a lot of interest and utilisation [12–14]. Song et al. [8] developed the SSE approach in 2000 to make it possible to do a single keyword search over ciphertext. Boneh et al. [15] proposed the Public-Key Encrypted Keyword Search (PEKS) approach as an alternative to the SSE system, which has a wider variety of applications. One-to-one encryption is made possible by Sahai and Waters' Attribute-Based Encryption (ABE) approach, which was developed in 2005 and significantly reduces the number of keys generated. The ABE system has been widely studied by scholars since its inception.

The ABE system's key components are the Key-Policy ABE (KP-ABE) and the Ciphertext-Policy ABE (CP-ABE). It was Bethencourt et al. [18] who presented the CP-ABE approach in 2007 for dynamic situations, which encrypts and tokenizes the secret key of the user with characteristics, allowing anybody with the proper set of attributes to decode it. The KP-ABE technique, which incorporates an access policy within the secret key, was shown to be less appropriate for dynamic settings. To assist users rapidly find the data they need, researchers have spent a great deal of time on Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS) based on keyword search [9–11]. According to Qiu and colleagues [19], attribute keyword search was developed to ensure that keywords and access structures are not distinct. Miao et al. [10] suggested an attribute-based encrypted keyword search strategy that takes into account a priority tree of attributes to establish access privileges for a particular data set for characteristics that can be verified. However, Zhang et al. [11] developed a searchable encryption protocol for industrial IoT that allows for a more efficient key generation and management process while also allowing for connected keyword search.

In light of the enormous amount of sensitive data collected by sensors on automobiles, researchers have paid particular attention to the issue of user privacy protection in the collection, transfer, and storage of vehicle data. V2V communication may be improved by combining pre- and post-verification countermeasures, as demonstrated by Wu et al. [22], who created a privacy protecting system. It was built using blockchain technology by Kumar et al. [13]

to detect and safeguard data in the blockchain. By utilising edge computing, Zhou et al. [14] provided the EVN architecture's location privacy dilemma with distinct privacy-preserving service framework. It is possible that fog computing might solve the problems of high latency and high cost, as Kang et al [15] suggest. Wu et al. [16] used physical layer security theory to estimate the privacy risks associated with computer offloading in automobiles.

IoV data privacy is effectively secured by previous systems, despite their concentration on vehicle location privacy or data storage privacy, which does not delve much into safe IoV data retrieval or interchange. As more people are concerned about their privacy while searching for information, experts have begun looking into ways to secure IoV data retrieval using current technologies. ' Chen et al. [7] developed a tamper-proof incentive scheme for IoV data sharing based on blockchain's tamper-proof performance. Although Cui and his colleagues [18] established an anonymous, traceable, and decentralised V2V data sharing system that relies on federated blockchain technology, it is not flexible enough to suit the needs of users who desire flexible data retrieval.

There are new ABE schemes that are more secure and fine-grained access control for IoV data retrieval and retrieval. Fuzzy retrieval may be performed using a single lattice technique and particle encryption, and keyword weights can be calculated using dependency grammar and phrase structure trees to improve search precision. An auditable user revocation idea and an online/offline calculation approach that can be verified were presented by Zhang and colleagues [20]. Confidently retrieving IoV data, they addressed the issue of fraudulent users accessing sensitive data, providing an online/offline calculation approach that can be verified. To allow parallel outsourced decryption, Feng et al. [21] presented edge computing, which can be applied to current ABE methods built on tree structure and linear secret sharing, despite serial outsourced decryption's high compute consumption and low efficiency.

An ABE method that is vulnerable to a single-point performance bottleneck is used in these research to create and manage complex keys with a single attribute authority. Maintaining both efficiency and security in IoV circumstances requires keeping computational complexity to a minimal.

3. System Analysis

Keywords can be used to simultaneously regulate access and retrieve ciphertexts in an existing BKS system. Single attribute authority scenarios are most commonly used for CP-ABKS procedures because they eliminate lengthy user certificate verification and secret key delivery. It follows that a single point of performance bottleneck emerges in large-scale distributed cloud systems (e.g., inadequate robustness and efficiency). Taking down or hacking into this one attribute authority puts the entire cloud service at risk (e.g., beingun available during that period). The time it takes to deliver secret keys to data users might be prohibitively long. If a single point of performance limitation exists, the CP-ABKS system's availability may be jeopardised. With these downsides, users no longer have physical access to their data while using the cloud.

We propose a multi-authority attribute-based keyword search (MABKS) for cloud systems as a solution to the dilemma of a single point of failure and high storage and computation requirements (which are unrealistic for resource-limited devices). FIG. 1 shows the MABKS system's multi-authority design, which varies greatly from single-authority systems. The MABKS system's AAs must check the certificates of data users and produce intermediate secret keys for them, which are subsequently forwarded to the CA, which generates the final secret keys for DUs. When compared to traditional traceable CPABE systems, the MABKS strategy concentrates on tracking malicious data users who could leak their secret keys, rather than those who might unintentionally divulge their secrets to unauthorised groups. A new attribute update enabled by the upgraded MABKS system means that anybody who attempts to access personal information in the cloud using an outdated secret key will be unable. MABKS allows only some of the changed characteristics' secret key components and indexes to be updated, whereas CP-ABE schemes formerly required updating all ciphertexts to achieve this. According to a thorough security investigation, the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Customers may be fooling the cloud service provider, but third-party arbitrators may quickly detect dishonest cloud service providers.

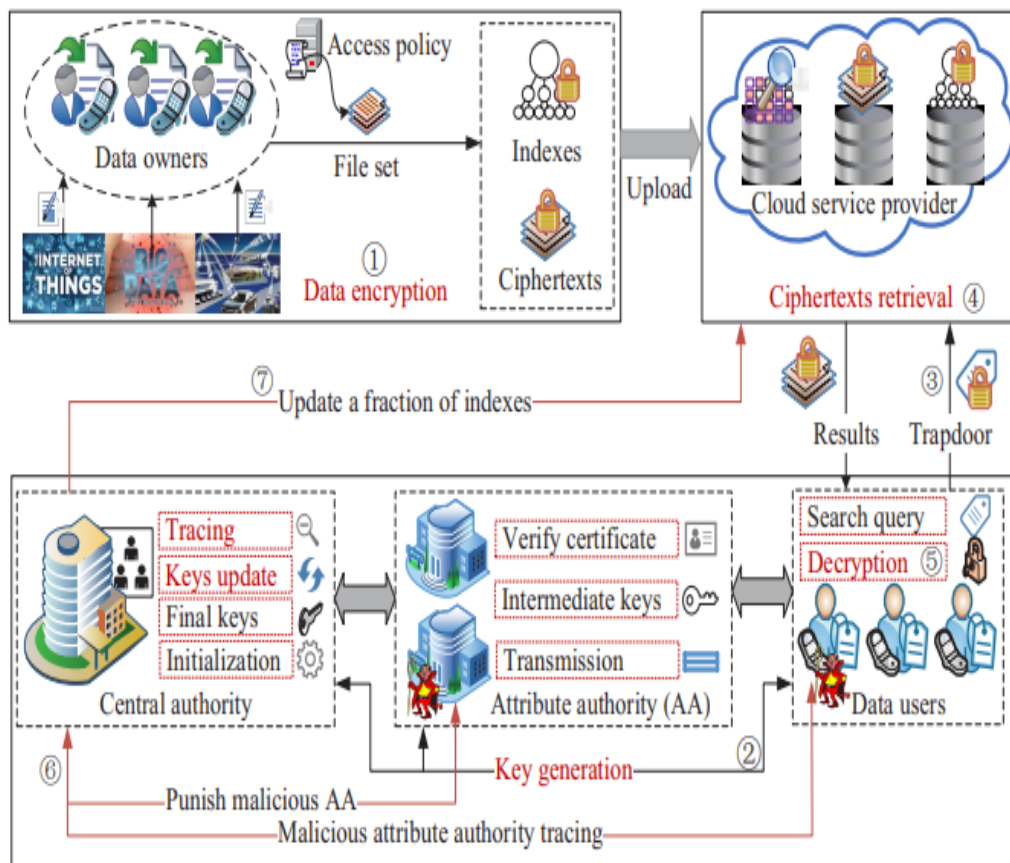


Fig 1. Architecture of our system

4. Implementation

A. Data Upload and Encryption:

Using the cloud to quickly and securely upload encrypted data. It is possible for a semi-trusted proxy to turn one encrypted communication into another encrypted message without having access to the original content of the message. To allow a user to upload our files to a certain database location. Encrypted data may be uploaded by any user and stored in the database. In this case, the user wishes to use the file download and see our encrypted file using the secret key.

B. Data Sharing:

The collecting of clients is a sign of mutual information. It's impossible to sidestep the question of whether or not the two meetings are related. As a result, the role of a dispute mediator is critical to the development of a workable review strategy. By separating the evaluator (TPAU) and the referee (TPAR) and placing varying levels of trust suspicion on each, we magnify the hazard already demonstrated in open layouts. It is important that the referee be someone who is not part of either the TPAU or the CSP because the TPAU is primarily tasked with verifying that the information provided by customers is accurate. The TPAR, on the other hand, we find to be honest yet a little unsure. Most of the time, it will act honourably, but it is also intrigued about what the auditing data contains. Consequently, the auditing data's privacy should be taken into account.

C. Auditing:

It is common for public auditing schemes to use third-party auditors (TPAs) in order to reduce the burden on clients as much as feasible. Assuming a valid owner versus an unknown CSP, these models fail to take into account the issue of fairness. Can the CSP rely on the audit results if the TPA is acting on behalf of the owner? Suppose the owner and TPA work together to sabotage an honest CSP in order to make money. As a result, auditing systems become less useful and applicable as a result of these models.

D. Join Group:

Our work is the first to incorporate public verifiability, data dynamics support, and conflict arbitration all at the same time, in relation to these schemes. Supplements for both PDPs and Pors are included. Introduced a system for verifying the accuracy of network-encoded data in a multi-server environment. A distributed storage environment should have many copies of all of your data to ensure complete data ownership. The principle of proxy resignatures, where shared data are signed by a group of users, is used to give quick user revocations. Forward error-correcting codes are also included into PDP to ensure resilient data possession.

5. Results

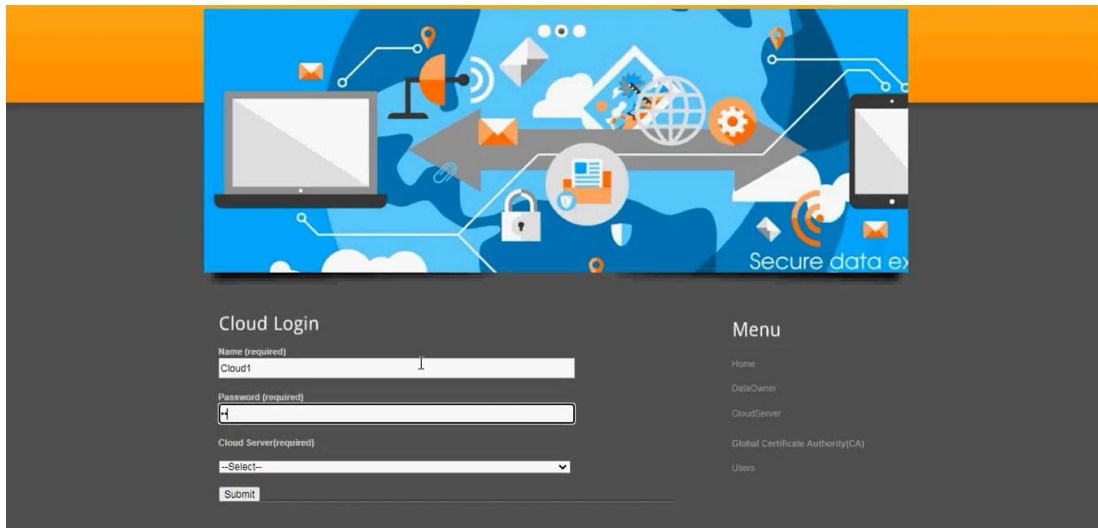


Fig 2 Login Page



Fig 3 Cloud Server Page



Transaction Details of CS1

User Name	File Name	Cloud Name	Task	Date
Gopi	Dbase.jpg	CS1	Upload	15/09/2021 17:44:49
Mala	Dbase.jpg	CS1	Download	15/09/2021 17:48:07
Mala	Dbase.jpg	CS1	Download	15/09/2021 17:49:51
Mala	Dbase.jpg	CS1	Download	15/09/2021 17:59:55
Gopi	Android.bt	CS1	Upload	16/09/2021 13:03:37
Mala	Android.bt	CS1	Download	16/09/2021 13:04:17
Ashok	Bigdata.bt	CS1	Upload	16/09/2021 13:06:53
Mala	Bigdata.bt	CS1	Download	16/09/2021 13:07:52

Fig 4 Transaction page

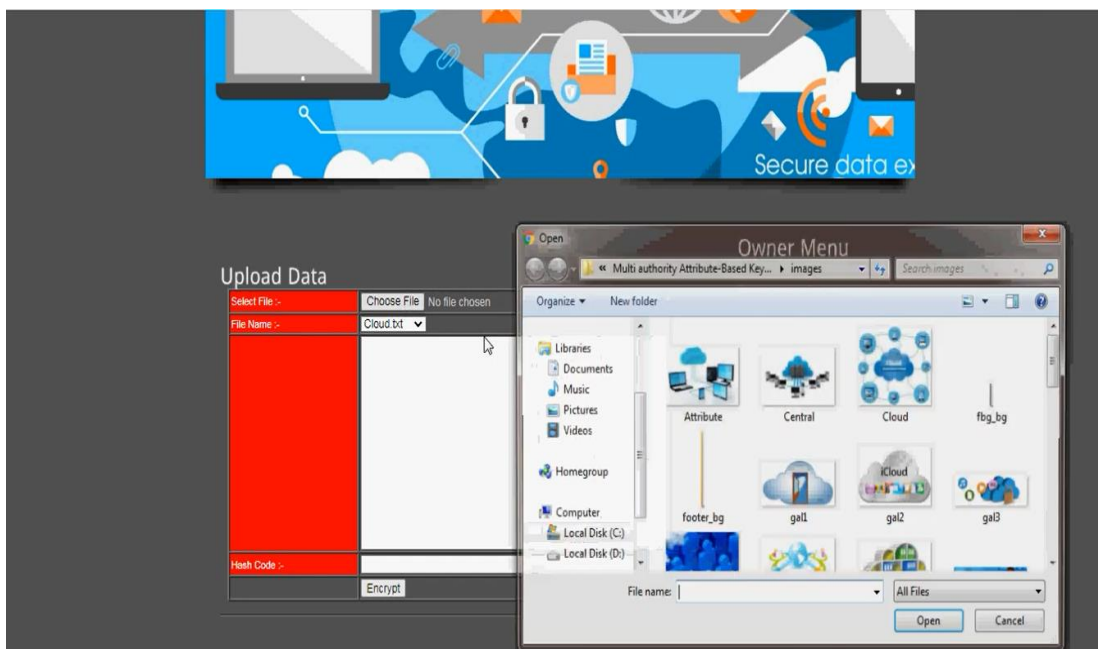


Fig 5 Data upload

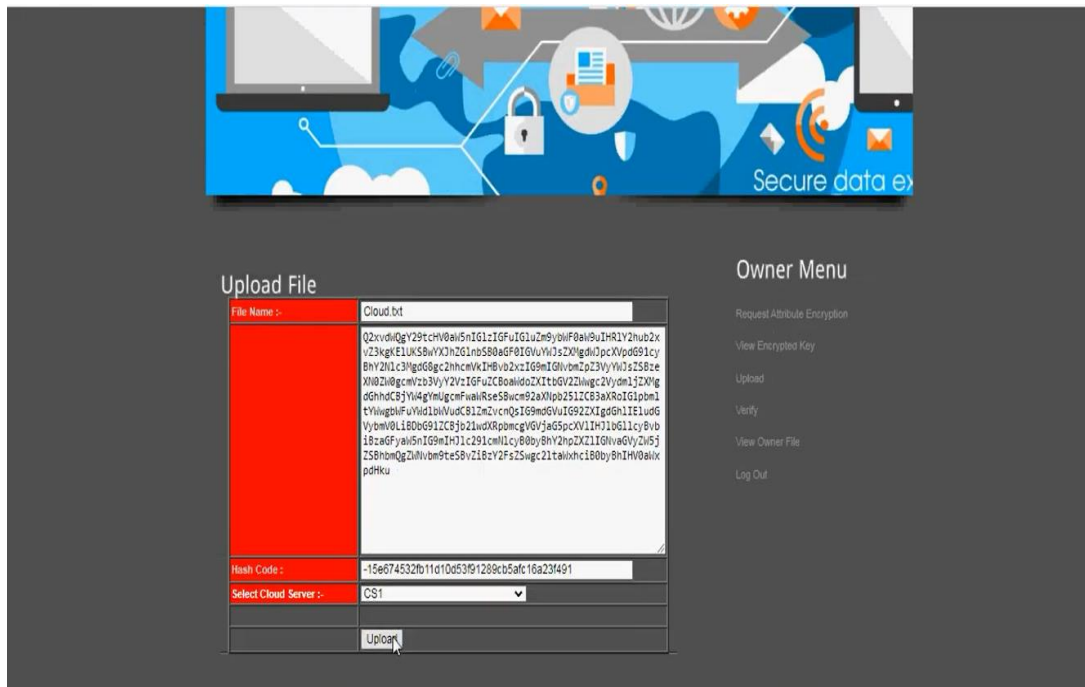


Fig 6 Data Upload Page



Fig 7 Encrypted data

6. Conclusion

The performance bottleneck in cloud systems may be avoided by using our efficient and viable MABKS technology, which supports numerous authorities. We can also trace malicious AAs and support attribute updates with the MABKS system described. Using selective-matrix and selective-attribute models, we

showed the system's selective security level in BDHE and DBDH assumptions, respectively. While the system's performance has been reviewed, it has been shown to have significant cost savings over previous implementations of the same algorithm. There's a major drawback to the MABKS system, though, which is that it doesn't have the ability to handle complex queries like conjunctive keywords and fuzzy searches. The MABKS system will be able to accommodate a wide range of search queries in the future by developing an efficient and flexible index design.

References

- [1] C. Huang, R. Lu, H. Zhu, J. Shao, and X. Lin, "Fssr: Finegrained ehcs sharing via similarity-based recommendation in cloud-assisted ehealthcare system," in *Proc. ACM on Asia Conference on Computer and Communications Security (AsiaCCS'16)*, 2016, pp. 95–106.
- [2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04)*, vol. 3027, 2004, pp. 506–522.
- [3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy (SP'00)*, 2000, pp. 44–55.
- [4] Ernawati, E., Baso, Y. S., Hidayanty, H., Syarif, S., Aminuddin, A., & Bahar, B. (2022). The effects of anemia education using web-based she smart to improve knowledge, attitudes, and practice in adolescent girls. *International Journal of Health & Medical Sciences*, 5(1), 44-49. <https://doi.org/10.21744/ijhms.v5n1.1831>
- [5] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 1, pp. 97–109, 2018.
- [6] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.
- [7] J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, and W. Lou, "Searchable symmetric encryption with forward search privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, pp. 1–15, 2019.
- [8] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.
- [9] J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable cp-abe for cloud storage service: how to catch people leaking their access credentials effectively," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 883–897, 2018.
- [10] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 789–802, 2019.
- [11] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "Raac: Robust and auditable access control with multiple attribute authorities for public

- cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 953–967, 2017.
- [12] K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” *IEEE transactions on parallel and distributed systems*, vol. 25, no. 7, pp. 1735–1744, 2014.
 - [13] L. Harn and J. Ren, “Generalized digital certificate for user authentication and key establishment for secure communications,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2372–2379, 2011.
 - [14] M. Chase, “Multi-authority attribute based encryption,” in *Proc. IACR Theory of Cryptography Conference (TCC’07)*, 2007, pp. 515–534.
 - [15] Q. Zheng, S. Xu, and G. Ateniese, “Vabks: verifiable attribute based keyword search over outsourced encrypted data,” in *Proc. IEEE Conference on Computer Communications (INFOCOM’14)*, 2014, pp. 522–530.
 - [16] Suryasa, I. W., Rodríguez-Gómez, M., & Koldoris, T. (2022). Post-pandemic health and its sustainability: Educational situation. *International Journal of Health Sciences*, 6(1), i-v. <https://doi.org/10.53730/ijhs.v6n1.5949>
 - [17] V. K. A. Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, “Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage,” *Journal of Network and Computer Applications*, vol. 129, pp. 25–36, 2019.
 - [18] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2016.
 - [19] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, “Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage,” *Information Sciences*, vol. PP, pp. 1–15, 2019.
 - [20] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine-grained search over encrypted data in fog computing,” *IEEE Transactions on Services Computing*, vol. PP, no. 1, pp. 1–14, 2018.
 - [21] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attribute based keyword search over hierarchical data in cloud computing,” *IEEE Transactions on Services Computing*, vol. PP, no. 1, pp. 1–14, 2017.
 - [22] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, “Practical attribute based multi-keyword search scheme in mobile crowdsourcing,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3008–3018, 2018.
 - [23] Y. T. Demey and M. Wolff, “Simiss: A model-based searching strategy for inventory management systems,” *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 172–182, 2017.
 - [24] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, “Efficient traceable authorization search system for secure cloud storage,” *IEEE Transactions on Cloud Computing*, vol. PP, pp. 1–14, 2018.
 - [25] Y. Miao, J. Weng, X. Liu, K.-K. R. Choo, Z. Liu, and H. Li, “Enabling verifiable multiple keywords search over encrypted cloud data,” *Information Sciences*, vol. 465, pp. 21–37, 2018.