International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I7P237

Volume 70 Issue 7, 355-365, July 2022

Review Article

Blockchain-based Asymmetric Searchable Encryption: A Comprehensive Survey

Beena G Pillai[1], Dayanand Lal N[2]

[1,2]*Department of Computer Science & Engineering, Gitam School of Technology, GITAM University, Bengaluru*

[1]bpillai@gitam.edu

Received: 13 May 2022 Revised: 15 July 2022 Accepted: 18 July 2022 Published: 26 July 2022

Abstract *- Blockchain-based encryption is currently a searchable technique that only supports specific keyword searches. With distributed storage on the blockchain, users can share the data without a centralized server. The cloud server and the user have a mutual distrust due to concerns about losing control over the outsourced personal data. In the current scenario, secretive service providers could not evaluate personal information. One of the most typical problems was locating encrypted cloud services. Searchable encryption is an excellent way to use encrypted data sent to a remote server, such as cloud infrastructure. Users can receive the search results without downloading the encrypted data stored in the cloud. The blockchain-based searchable encryption approach includes fuzzy keyword search, verification of search results, and dynamic file updates. The asymmetric searchable encryption can be deployed in index tree structures to guarantee backward and forward privacy.*

Keywords *- Asymmetric Searchable Encryption, Blockchain, Backward and Forward privacy, Fuzzy Keyword.*

1. Introduction

Cyber threats in cloud computing, identity theft, and data mining-based attacks apply to blockchain networks. Privacy leakage may occur when a successful linking attack is an anonymous cloud dataset[1], [2]. The information accessed by authorized users and data stored in blocks implies that mining block data could lead to privacy breaches. Data stored on remote cloud servers are in a similar situation. Thus, two technologies are under threat from both outside and inside threats. Cloud computing resources supplement the blockchain system to enhance security, efficiency, and service quality[3].

Distributed networks, blockchain, and cloud computing have unique qualities and face comparable network-related difficulties[4]. A higher degree of coverage that integrates various network-related technologies could include future integration. Although adversary techniques may differ, a few cyber threats in cloud computing, for example, identity theft and data mining-based attacks, also apply to blockchain networks[5]. The information accessed by authorized users and stored in blocks implies that mining block data could lead to privacy breaches. Data stored on remote cloud servers are in a similar situation. Privacy leakage may occur when a successful linking attack is on an anonymous cloud dataset[6]. Thus, two technologies are under threat from both outside and internal threats. Cloud computing resources supplement the blockchain system to enhance security, efficiency, and service quality. As much as software, hardware plays a role in computers and covers blockchain-related equipment[7].

SSE uses cloud storage, permitting customers to send encrypted data to a cloud server[8]. The most amazing immediate cloud storage enables a client to safely outsource information to an unreliable third-party cloud provider. SSE has been the subject of considerable investigation, with various methods proposed to accomplish contrary levels of efficiency and safety[9], [10]. Any basic SSE approach should have sublinear search speed, protection against adaptively picked keyword assaults, tiny indexes, and the ability to add and remove files swiftly. SSE allows a customer to source an accumulation of encrypted records to the cloud while maintaining the capacity to execute keyword searches without disclosing any information about the substance of the articles and requests. In recent years, cloud computing has been prevalent for handling personal data because of cost savings and administrative flexibility. Before using typical data retrieval operations, such as plaintext keyword searches, sensitive information must first be encrypted and transferred to cloud servers. There are two forms of encryption searched methods now available: Symmetric Searchable Encryption (SSE) and Public Key Searchable Encryption (PSE)[11].

1.1. Private Keyword Search

A keyword search method based on the blockchain is called searchain. It allows a careless search in the decentralized storage using a set of permitted keywords. In the transfer phase, the OKSA system features a one-way connection and a continual expense of communication. The searchain protocol, developed by OKSA and ordered multi

signatures (OMS), achieves order-preserving peer-to-peer retrieval transactions. Searchain's research and evaluation indicate that it maintains a fair cost without sacrificing retrieval privacy, ensuring usability. A decentralized, encrypted storage system can provide security and private keyword search features. Searchable encryption uses to search encrypted data. However, implementing this fundamental is enough to address specific dangers in the decentralized service model. For example, peer users would refuse to pay service costs based on fraud, while service peers would deliberately return inaccurate results. Therefore, create safe data adding and client-side authenticity and fair search results judgments via blockchain-based keyword search protocols.

1.2. Fair payment based on blockchain

Outsourcing services imply online payment and data security challenges, and reciprocal consumer and service provider distrust could hinder the implementation of cloud computing. The majority of existing solutions merely consider a single form of service and enlist the help of a third party to ensure clean remuneration. BPay is a fair payment system based on the blockchain for cloud computing services and solutions. It generally ensures safe and equitable payment of outsourced services without relying on anyone else, trustworthy or not. BPay's adversary model, implementation phases, and technical requirements are represented first, followed by the designing specifics. BPay provides a strong foundation and is compatible with both Bitcoin and Ethereum blockchains, according to security and characteristics analysis. A top-down checking protocol and an all-or-nothing checking protocol mechanism are the keys to ensuring reliable fairness and compatibility.

Furthermore, BPay is a low-cost payment method. Jianfeng Wang et al. [12] proposed a verifiable fuzzy keyword search approach that thoroughly examined for security and efficiency. Ethereum's smart contracts, a decentralized blockchain-based platform that offers a new computer architecture based on trust and transparency, have many promises. Swapping the central server for a more secure alternative created a smart contract. A privacy-preserving decentralized search method allows the data owner to be confident of receiving accurate search results without worrying about a rogue server's possible wrongdoings. As a result, an honest person gets what he deserves, whereas a malicious one receives nothing. It built a modern digital contract for a cost-effective search structure to better support actual applications. Everyone who takes part is rewarded equally and incentives to comply with proper computations. Extensive tests and evaluations show that a decentralized search strategy can use to search encrypted data.

The method of searching for ambiguous terms returns the results of a search. If the participant's input is "keyword," the server returns a file containing the key phrase that perfectly matches a pre-programmed keyword[13], [14]. The server delivers the closest possible results on a predefined relationship if the searching input has typos and format issues. Searchable encryption allows users to extract documents with cipher from data in the cloud that encrypt via a search with keywords[15], [16]. Jin Li et al. [17] use a fuzzy keyword search technique to create storage-efficient fuzzy keyword sets. Individuals or businesses can send encrypted information to a cloud-based storage service using a searchable encryption provider while searching the encrypted text for keywords. To avoid information leaking, users send many encrypted documents to the cloud. A valuable resource is the capacity to access encrypted data using a searchable encryption technique. When attempting to generate meaningful and reliable results, most existing searchable encryption systems exclusively focus on exact keyword searches and ignore the practically inevitable materials under inspection; there are typographical errors. These techniques fail to produce the desired result whenever the information user makes a grammatical error.

2. Relative Work and Comparative Study

2.1. Searchable Encryption

Song et al. [18] suggested a two-layered scheme based on symmetric encryption that became a distinctive first-generation search encryption strategy. An encryption and search algorithm are used to search the encrypted outsourced data. SSE (Searchable Symmetric Key Encryption) based on Cipher Text Scanning at the server end E.-J. Goh et al.[19]introduced Z-IDX, a safe file search method based on pseudo-random factors and Bloom filters, and explained how to apply it. Key design restrictions were specific set membership tests, private database query techniques, and cumulative hashing systems. Philippe Golle et al.[20] investigating search options with certain keyword sections would be fascinating. The Decisional Diffie-Hellman (DDH) algorithm and Boolean searches on encrypted data, Conjunctive Keyword Search, and Disjunctive Keyword Search were all used in this model[21]. Security games do not address the information disclosed by capabilities, which is a significant issue.

RezaCurtmola et al. [22] pushed for security even when people undertake more precise searches. Which systems are the most efficient and effective so far? It considers inter SSE, which broadens the search scope to include people other than the owner. It proposes two new SSE constructs and an indexing architecture called "file-keyword." Its effectiveness in both non-adaptive and adaptive attack scenarios. Seny Kamara et al.[23]propose searchable symmetric encryption, an inverted index technique, SSE's usefulness is extremely limited, and its possibilities of being used in real-world cloud storage systems are small. Seny Kamara et al. [24] suggested a new method for producing sub-linear SSE techniques and multi-core architecture upgrades. This approach is very

dynamic and parallelizable [25]. In [26] proposed an attribute encryption technique, whose addition and multiplication have a high computational cost. GUO et al. [27] present more efficiently supporting dynamic operations in a document, such as removals and insertions. This method analyzes [28] the scheme using an attribute encryption technique. And addition and multiplication have a high computational cost. The similarity between the contents and the query request using the vector space model.

Qi Chai et al[29] present a verifiable SSE (VSSE) technique. On a laptop and a smartphone running Android 2.3.4, the suggested VSSE was implemented and tested. Kurosawa et al. [30] describe an efficient verifiable SSE approach based on SSE-2. Under non-adaptive threats, U.C. protection is the same as privacy and reliability definitions. Xiu Jiang et al.[31] suggested a multi-keyword ranked search approach over encrypted cloud Data VMRS Scheme. According to Jianting Ning et al.[32] passive attacks develop judgments based on prior information and notice of user queries. Present improved attacks based on shakier assumptions about the amount of past knowledge an attacker may gather, with keyword recovery rates ideal or close to ideal.

Table 1. Symmetric Searchable Encryption

Survey	Major Contributions	Limitations
Ref. [18]	It remotely queried encrypted data on an untrustworthy server and provided security proofs for the results of cryptosystems.	The difficulty for more complex search queries
Ref. [20]	Boolean Conjunctive and Disjunctive keyword search over encrypted data using a security model.	Security games do not address information leakages
Ref. [22]	For Multiuser, the searchable Encryption ”file keyword” index structure works in non-adaptive and adaptive assault scenarios.	The server’s work per returned document is consistent regardless of the data size.
Ref. [24]	Sub-linear dynamic SSE schemes have developed.	The client does not save and update the tree’s root hash.
Ref. [26]	The scheme uses an attribute encryption technique.	Addition and multiplication have a high computational cost.
Ref. [27]	The Bloom filter-based search index tree uses to identify the relevant documents.	The precision of the scheme is affected by the search index tree.

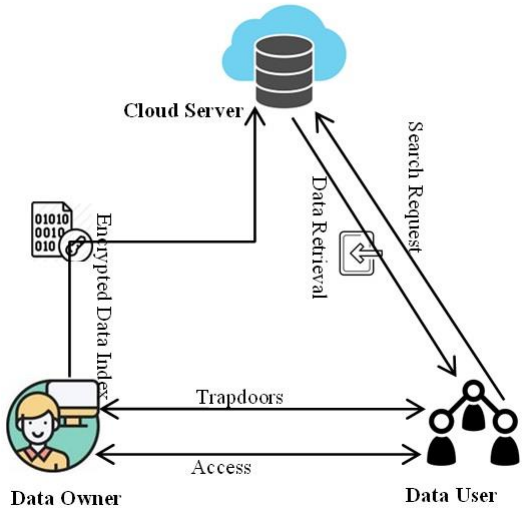

Fig. 1. Search Encrypted Cloud Data Framework

In Fig.1. The authoritative user has access to the server in the cloud with a search feature via encrypted data. They assumed that the person who owns the data and uses it had completed mutual authentication. The data user first delivers to the cloud server a large gathering of documents D in encrypted form C and an encrypted search index produced from D. The cloud server searches the index when a user makes a search request. It then sends back all the return information, including the exact trapdoors. The trapdoors are created, and the keywords are transmitted to the cloud server by the authorized user.

2.2. Searchable Encryption Using Blockchain

Recent research has focused on resolving issues with existing blockchain-based systems. For example, when employing a distributed hash table technique to combine encryption with keyword searching, the researchers discovered that hostile nodes might sabotage search results. However, the method could find and delete malicious nodes because most nodes follow a self-determining approach.

To allow data exchange, Jie Niu et al. [33] advised employing attribute-based encryption with searchable encryption. The CPA secure(Chosen Plaintext Attack) scheme and the CCA secure scheme are secured against Key-Leakage. Peng Jiang et al. [34]ensure a private search with the same retrieval order for all allowed terms. Chengjun Cai et al. [35] proposed a multi-set, incremental hashing technique to process data integrity checks. A decentralized, encrypted storage architecture with secure and private keyword search capabilities. When a client peer recognizes erroneous search results, a storage peer claims that the client opposes that the exemplary search service is supplied and

refuses to pay the service price. User peers would refuse to pay service prices, while service peers would purposefully return incorrect results. Shengshan Hu et al.[36] created a smart contract for constructing a search in which all players are treated equally and have a financial incentive to support correct computations. Aiqing Zhang et al. [37] introduced a searchable public encryption system in the context of sharing personal health information. BSPP (blockchain-based safe and privacy-preserving PHI) mechanism has been created to improve diagnosis in e-Health systems. Yinghui Zhang et al. [38] suggested a Time Commitment Scheme, and a top-down validation mechanism is used to determine the compatibility of BPay. In [39] created a blockchain-based searchable encryption scheme. The EHR extracts using a clever Boolean technique to create the index. The smart contract for the proposed method is designed to track monetary rewards among participants in a multi-user setting, including transaction fees—the cost of document I.D.s from EHRs and carrying out Ethereum smart contract operations. SEPSE, safe Public-key encryption with keyword search (PEKS) approach in which users encrypt keywords using dedicated key servers in a threshold and oblivious way, was proposed by Yuan Zhang et al.[40] as an alternative to KGA.

Table 2. Blockchain-based searchable encryption

Survey	Major Contributions	Limitations
Ref. [33]	BAI-KASE scheme and Data sharing	The payload is tiny
Ref. [34]	OKSA and Ordered Multi Signatures (OMS) to present a Searchain protocol	High bandwidth consumption.
Ref. [36]	Packing method - used to reduce the cost. Ethereum's smart contracts promise a Decentralized platform based on the blockchain.	The keyword search scheme is not proper.
Ref. [38]	A top-down checking technique establishes outsourced services' secure and fair payment.	Payment fairness
Ref. [39]	The EHR index's integrity, anti-tampering, and traceability are all ensured by blockchain technology.	Malicious nodes could harm search results.
Ref. [40]	SEPSE can effectively fend off online KGA, in which each user's keyword request turns into a public blockchain transaction.	Addressing Key leakage issue.

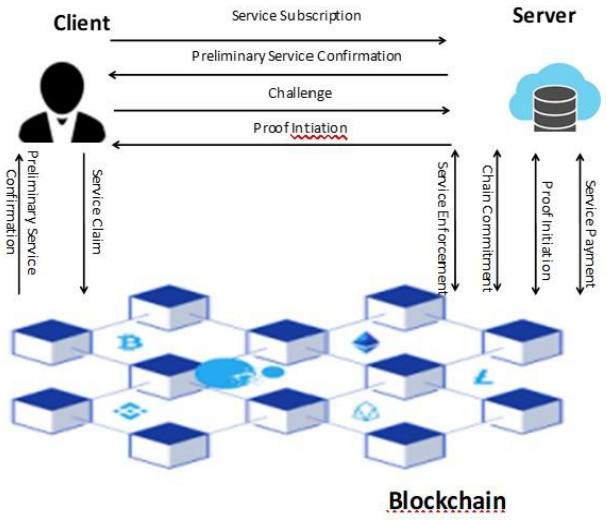

Fig. 2 BPay Architecture

In figure2, Client C receives S.V. from S and subscribes to it as a user. S can give C after S.V. imposes by S. An initial service verification based on the blockchain C challenges S to verify the use of cryptocurrency before making a payment. If S is malevolent, S must first create a claim promise to assure that C receives sufficient defense reaction in deposits. Then, C and S collaborate to start the service proof by defining some essential requirements. Finally, suppose S fails to make enough deposits. In that case, C can demand them from S to deliver legitimate assistance evidence that the platform's deployment complies with the requirements standards before a given period. It's worth noting that the proofing and payment of service accomplish through a series of steps and the initial installation of services verification and proofing.

Server S tries to gain service fees from C as an outsourcing service provider by enforcing the S.V. subscription C purchased. S offers valid service proof to obtain the service charge from C before the stage of service payment at the specified time after the joint defense starts. S completes the blockchain-based execution of S.V. and sends a tentative confirmation to C after receiving C's request for a service subscription. Following C's challenge, S makes the claimed commitment.

2.3. Fuzzy Keyword Search

Data owners opt to store their data in the cloud as cloud computing becomes more widespread, allowing them more freedom and cost savings. More and more confidential information would be transmitted and consolidated into Cloud Computing. Sensitive data is frequently encrypted before being outsourced to preserve data privacy, making practical data usage difficult [41–43]. Existing methodologies are unsuited for Cloud Computing because of

this severe flaw, which hurts user searching, is complex, and has low system effectiveness due to connection accessibility. Fuzzy keyword search dramatically increases system usability by providing relevant documents whenever clients' requesting parameters match predefined keywords. If an exact match fails, keyword resemblance criteria use to find the most likely matched files. Cong Wang et al. [44] presented a suppressive technique. The private trie-traverse similarity is employed to generate search requests in this strategy. The Basic Scheme is a Fuzzy Searching Scheme that uses a symbol-based Trie-Traverse Searching Scheme. Develop a storage-efficient fuzzy keyword set and an efficient and successful search technique. To create a reliable and efficient fuzzy keyword search technique that allows the user to double-check the accuracy and completeness of the search results.

In [45] proposed, the outsourced document collection is refreshed and verified using secure fuzzy keyword search techniques. And it has some probability issues. To make U.C. secure against a hostile server, Xiaoyu Zhu et al. proposed a verified and dynamic fuzzy keyword search (VDFS) technique. Users must detect potential misbehavior, which necessitates searchability that can be verified. Zhangjie Fu et al. [46] introduced a Multi- keyword fuzzy ranked search approach, which incorporates a stemming algorithm based on the unigram, enhancing accuracy and allowing for other spelling errors. For cloud computing, GUOXIU LIU et al.[47] proposed FSSE stands for fuzzy semantic searchable encryption, providing for multi-keyword searches over encrypted material. XINRUI GE et al. [12] presented a fuzzy keyword search technique based on the verified same keyword search system (VEKS). To get efficient storage, use a linked list as a specific index, and make an authentication label for each fuzzy word to ensure that the returned ciphertexts are correct.

Shahzaib Tahire and colleagues[48] suggested a revolutionary ranking Searchable Encryption (S.E.) technique. Hong Zhong et al.[49] introduced a dynamic multi-keyword fuzzy search approach. Uni-gram-based key word transformation, Bloom-filter-based index/query vector creation, index tree construction, and Index tree-based top-k search are used in the proposed system. The index tree is used to build a Top-k search algorithm, which searches k files most relevant to a given query. The authors used Locality-Sensitive Hashing (LSH), the KNN methodology, and a pseudo-random function to ensure the solutions' security.

Table 3. Comparison of Fuzzy keyword search

Survey	Major Contributions	Limitations
Ref. [43]	Privacy-preserving fuzzy search is used to encrypt data in Cloud Computing.	Conjunction of keywords
Ref. [44]	The symbol-based is the Trie Traverse Searching Scheme and suppressing technique supporting Fuzzy Search.	Validity Issue
Ref. [45]	The outsourced document collection is refreshed and verified using secure fuzzy keyword search techniques.	Probability Issues
Ref. [46]	Introduce the stemming algorithm and develop a revolutionary way of keyword transformation.	It only supported a single keyword search.
Ref. [47]	A linked list is used for a specific index to accomplish efficient storage.	Low search efficiency
Ref. [48]	To be implemented on the public Cloud architecture of British Telecommunications and assessed on a real-life voice corpus.	The issue with the Multi-user setting
Ref. [49]	The Bloom filter construction of the index tree is used to create the index/query vector.	Real-world data set demonstration

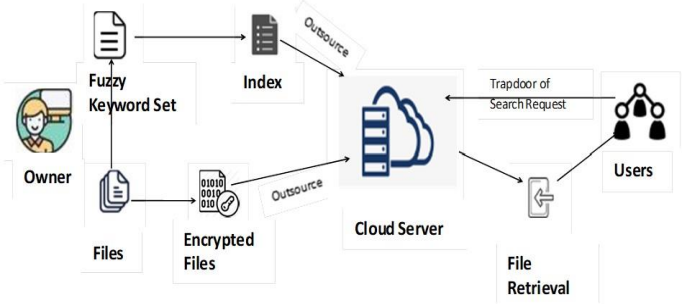

Fig. 3 Fuzzy keyword Search Architecture

Exact keyword search algorithms are of limited use in real-world applications. Privacy information is encrypted, a revolutionary verified keyword search with some fuzziness strategy[50]. In the fuzzy keyword search strategy,[51–54] each precise term represents three nodes in a linked list, from which a fuzzy keyword sets to generate, instead of developing each fuzzy keyword as its index vector to protect against fraudulent cloud server behavior. Every fuzzy keyword has a verification label to validate the validity of the ciphertexts. Since it allows users to create grammatical or formatting error discrepancies, fuzzy keyword search increases system usability.

A new ranked searchable encryption scheme uses probabilistic trapdoors to help defend against distinguishability attacks. SEaaS (Searchable Encryption as a Service) is tested using the British Telecommunications public Cloud architecture on a real-world speech corpus. The design provides high-security assurances while still relatively light by assessing its performance over the speech corpus. These strategies operate in isolation, reducing the usefulness and effectiveness of the service significantly. A ranked fuzzy keyword search improves system usability and performance [55]. It returns the files that match the criteria in a prioritized order based on keyword similarity semantics and some relevance criteria. It uses the edit range to measure fuzzy set creation based on keyword matching and dictionaries to create fuzzy keyword sets, reducing indexing, preservation, and transmission costs.

3. Taxonomy in Searchable Encryption Techniques

3.1. Searchable Symmetric Encryption or Private Key Encryption

A verifiable SSE (VSSE) technique [56] provides verifiable searchability and data privacy, supported by a thorough security study. A multi-keyword ranked search [57–59] strategy that includes search results verification through encrypted cloud data. To build a blockchain-based data-sharing system and searchable key aggregation encryption method that improves search efficiency and connects the world[60–62]. Concrete implementations of a CPA-resistant searchable key aggregation encryption scheme justify the efficiency and performance study. The BAI-KASE approach allows users to combine multiple encryption keys into a single key to reduce bandwidth[63]. A blockchain-based searchable symmetric encryption scheme is a dynamic, proven data possession mechanism. [64–66]. According to security and compatibility evaluations, BPay provides faires and robust, and it is interoperable with the Bitcoin and Ethereum blockchains.

Algorithm Design

Y = (KeyGen, Preprocss, QueryGen, SearchOutput, Verify)
1. Secret Key ‘K’ and Security Parameters ‘n.’
2. Documents N: Di, 1<=I<=N.

$$q_j \in \left[q_{j-1} \, X \, |\epsilon| \; + 1, \left(1 + q_{j-1}\right) X \, |\epsilon|\right]$$

$$q_{j+1} \in \left[q_j \, X \, |\epsilon| \; + 1, \left(1 + q_j\right) X \, |\epsilon|\right]$$

Privacy Preserving Query $\pi = (\pi(1), \ldots\ldots, \pi(m+1))$

The steps for searchable encryption are as follows:

- The data user encrypts a plaintext file uploaded to a public cloud with the key. Concurrently, it encrypts keywords and publishes them to the consortium blockchain using a searchable encryption key.
- The user encrypts the keywords waiting for queried using the searchable encryption key to create a trapdoor during the query procedure. Simultaneously, Before transferring the encrypted keywords to the blockchain database, the trapdoor hides no information about the keywords.
- The trapdoor accepts as input by the blockchain network. It employs match analytics to identify the trapdoor's indexes and search the necessary cloud server file depending on all encrypted files that successfully match the index value return.
- The key uses to decode the encrypted file that the user gets. A blockchain transaction sheet must build while encrypting chain data. The blockchain transaction sheet now includes a keyword for ciphertext search without altering the blockchain database's original setup. This keyword uses to search ciphertext in the blockchain network, and it is created by encrypting the keyword by the client, a public encryption key searched.

3.2. Asymmetric Searchable Encryption or Public Key Encryption

In [67], malicious nodes are easy to discover and remove because most nodes take a self-determining strategy. A security investigation and performance review show that SEPSE provides improved security assurance at a reasonable computing cost. SEPSE can effectively withstand online KGA.

Algorithm Design

Y= Setup,PEKS, Trap_door
$fi(X) = ai0 + ai1x + \ldots\ldots + ai, t\text{-}1xt\text{-}1$
$e(\sigma k, p) = e(w,Qk)$
Trap_door: $tdw = \alpha H1(sdw)$

Using edit distance as the similarity measure, generate a list of similar keywords that may be stored efficiently from a particular document collection [68–70]. To achieve the required similarity search feature while maintaining a consistent search time complexity. Extensive trials using real data sets on Amazon’s cloud platform further illustrate the validity and applicability of the proposed technique.

Algorithm Design

Π = (setup(1λ), Enc(sk), Dec(sk)

wi $\mathcal{E}(1 \leq i \leq p)$

Trapdoor :Twi = f(sk,wi)

Encryption(sk,FIDwi || wi)

In [71] proposed public key cryptography asymmetric searchable encryption as an extension of Song et al. To [72] achieve multi-keyword search, the work suggested a conjunctive keyword search approach. In [73], present a new PAEKS security model that covers both chosen multi ciphertext attacks (from the outside) and keyword guessing attacks (from the inside). Make an accurate PAEKS scheme and show it is secure using the new PAEKS security approach. It uses an identity-based key exchange protocol,

which was promoted as a way for data senders to handle their keys more easily. In [74], proposed colleagues provide Bidirectional Keyword Search with Public-key Encryption, a cryptographic system that allows two types of users to search on encrypted phrases (PEBKS). An attacker can adaptively access several keywords and search trapdoors. The theoretical definitions of a PEBKS scheme and its indistinguishable security model reflect the situation in which no attacker can dependably distinguish between two ciphertexts of keywords. In [75, 76] propose a more comprehensive picture of what may be accomplished in asymmetric searchable encryption approaches; trapdoor privacy is introduced, filling the gap between earlier definitions that only provide limited privacy guarantees practice against search patterns. Key Unlinkability for IBE is a security concept in PEKS that leads to robust trapdoor privacy safeguards. Any anonymous IBE scheme used to build PEKS schemes; the scheme that provides this security concept is well-known.

In [77] proposed ”FFSSE,” a new flexible forward secure SSE algorithm with the best performance in the literature, incorporates rapid token generation, quick search, and O(1) update complexity. This one-of-a-kind situation also allows for both add and remove actions. It uses a groundbreaking ”key-based blocks chain” symmetric cryptography scheme, primitives that may be used to guarantee forward privacy in any index tree or key-value structure. In [78] developed the MDO architecture, researched searching over encrypted data, and developed a groundbreaking approach that allows inverted indexing, intelligent search, and dynamic update. The proposed method is practical and safe according to a thorough analysis and multiple tests. In [79] allows for conjunction and disjunction within each keyword field.

Algorithm Design

Y = (KG, SG, BI, Adopt, Ge_Trap, Record, SearchOutput, Decryption)

$1 \leq t \leq |wi|$, $1 \leq u \leq |Fi|$, $a \leftarrow HK(Wt) \bmod p$, Compute EK(id (Fn))

Create random keys Ki, kn, $(krb, kub) \leftarrow \{0, 1\}\alpha$

Calculate a-1 and store it in A [1] [t],

Calculate Ek (id (Dn)), store it in A [t] [1].

4. Discussion

Soundness: Blockchain can ensure that users receive accurate and reliable search results without verification. Every node in the Ethereum network can detect changes to the search results.

Fairness: All transactions are funded by gas purchases. The fraudulent action will be identified, and the deceptive user will receive nothing in return.
SSE [80] has three models: 1. SERVER-USER Model Servers operate as both a data owner and a storage server, 2. USER-SERVER-USER Model - Users act as both owners and recipients of data, 3. USERA-SERVER-USERB Model - UserA uploaded some material to the server and gave UserB permission to perform a keyword search.

The Asymmetric Searchable Encryption using a blockchain system, trapdoor generation has a somewhat more significant computing cost than others; however, it is essential to avoid key production and utilization. The existing systems’ principal operations depend on basic symmetric cryptography or hash algorithms. ASEB is a high-performance Asymmetric system.

Table 4. Comparison with challenges of Searchable Encryption

Approaches	Service Model	Category	Verification	Fairness	Soundness	Accountability	Model Configuration	Updated
Ref. [19]	Transaction	VSSE	Server Side	No	No	No	User Server Model	No
Ref. [20]	Transaction	SSE	No Need	Yes	Yes	No	User A-Server-User B Model	No
Ref. [24]	Transaction	SSE	Server Side	Yes	Yes	Yes	User Server Model	Yes
Ref. [26]	Transaction	OKSA	Provider Side	No	No	Yes	Server-User Model	No
Ref. [27]	Transaction	SSE	Client-Side	Yes	Yes	Yes	User-Server-User Model	Yes
Ref. [31]	Smart Contract	SSE	No Need	Yes	Yes	No	User A-Server-User B Model	Yes
Ref. [32]	Smart Contract	PEKS	No Need	No	Yes	No	User A-Server-User B Model	Yes
Ref. [33]	Smart Contract	VDFS	Both Client and Server Side	Yes	Yes	No	User A-Server-User B Model	Yes
Ref. [34]	Smart Contract	VEKS	No Need	Yes	Yes	No	User A-Server-User B Model	Yes
Ref. [35]	Smart Contract	SEaas	No Need	Yes	Yes	No	User A-Server-User B Model	Yes
Ref. [36]	Smart Contract	FSSE	No Need	Yes	Yes	No	User A-Server-User B Model	Yes

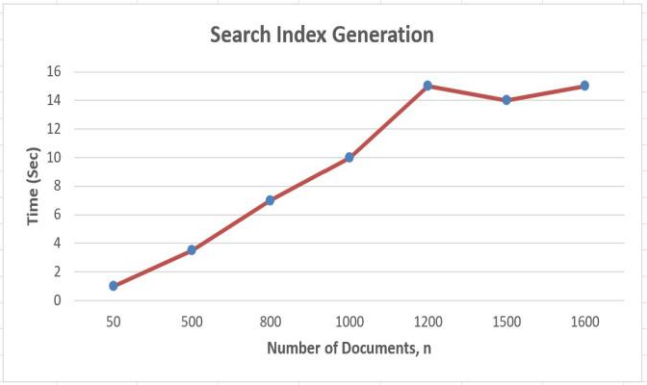

Fig. 4 Computational Time for Search Index Generation

Figure 4 depicts the algorithm's computing cost. A set number of keywords, 120,000, and a variable number of pages are generated via the inverted index. The experiment begins with 100 papers and increases by 100 every iteration until it reaches 1600. The x-axis represents the quantity of records, while the y-axis represents the duration in seconds. The size of the papers in question determines the graph's trend. The documents in the corpus are organized by size in ascending order. The reports continue to grow until they reach 1200 documents, which stops growing. The graph's trend demonstrates this. The inverted index takes 14.68 seconds to generate for 1600 documents.

Because the quantity of documents has no bearing on the fuzzy index, only the number of keywords is altered. The results are represented graphically in Figure 5. The experiment begins with 10,000 keywords and quickly grows to 120,000 by adding 10,000 per iteration. The x-axis represents the number of keywords, while the y-axis represents the time in seconds. As the number of keywords grows, the fuzzy index looks to expand fairly linearly. For 120,000 keywords, the fuzzy index construction takes about 2.84 seconds.

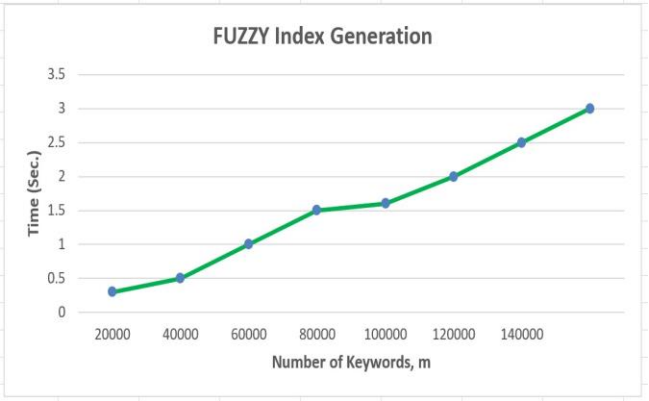

Fig. 5 Fuzzy Index Generation Computational Time

Asymmetric Searchable Encryption has substantial security advantages over other methods since it allows backward and forwards privacy. The security qualities ensure that ASEB defends against file injection attacks and prevents erased data information from being leaked. As a trade-off for improved security, the ASEB system has a somewhat higher computational cost than other systems.

5. Conclusion

Nowadays, many documents are in the cloud, and it is tough for cloud customers to search their outsourced data using searchable encryptions. Cloud Service providers may be trustworthy, while they can be suspicious or malicious. The encrypted search results could be inaccurate and deceptive. The legitimacy of the search results is ensured by utilizing blockchain technology, transaction verification, and smart contracts. The bulk of blockchain-based searchable encryption solutions has addressed SSE's concerns. From the above research, I can conclude that it is safe to use Asymmetric Searchable Encryption for retrieving the data. More investigation into blockchain in PEKS is required.

References

[1] C. Liu, L. Zhu, M. Wang, and Y.A. Tan, "Search Pattern Leakage in Searchable Encryption: Attacks and New Construction," *Information Sciences*, vol. 265, pp. 176–188, 2014.

[2] K. Gai, K.-K. R. Choo, and L. Zhu, "Blockchain-Enabled Reengineering of Cloud Datacenters," pp. 21–25, 2018.

[3] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities," *Re-Newable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

[4] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[5] B. B. Gupta, K.-C. Li, V. C. Leung, K. E. Psannis, S. Yamaguchi, et al., "Blockchain-Assisted Secure Fine- Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1877–1890, 2021.

[6] D. Cash, P. Grubbs, J. Perry, and T. Ristenpart, "Leakage-Abuse Attacks Against Searchable Encryption," in Proceedings of the 22nd *ACM SIGSAC Conference on Computer and Communications Security*, pp. 668–679, 2015.

[7] M. Asif, Z. Aziz, M. Bin Ahmad, A. Khalid, H. A. Waris, and A. Gilani, "Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities," *Sensors*, vol. 22, no. 7, pp. 2604, 2022.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous Ibe, and Extensions," in *Annual International Cryptology Conference, Springer*, pp. 205–222, 2005.

[9] J. Li, X. Lin, Y. Zhang, and J. Han, "Ksf-oabe: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715–725, 2016.

[10] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and Efficiently Searchable Encryption," in *Annual International Cryptology Conference, Springer*, pp. 535–552, 2007.

[11] Z. Brakerski and G. Segev, "Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting," in *Annual Cryptology Conference, Springer*, pp. 543–560, 2011.

[12] J. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. Chen, "Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 667–684, 2013.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public Key Encryption with Keyword Search Revisited," in *International Conference on Computational Science and Its Applications, Springer*, pp. 1249–1259, 2008.

[14] B. Qin, Y. Chen, Q. Huang, X. Liu, and D. Zheng, "Public-Key Authenticated Encryption with Keyword Search Revisited: Security Model and Constructions," *Information Sciences*, vol. 516, pp. 515–528, 2020.

[15] R. Ramasamy, S. S. Vivek, P. George, and B. S. R. Kshatriya, "Dynamic Verifiable Encrypted Keyword Search Using Bitmap Index and Homomorphic Mac," in 2017 *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE*, pp. 357-362, 2017.

[16] A. Mahmood, S. A. Khan, S. Hussain, and E. M. Almaghayreh, "An Adaptive Image Contrast Enhancement Technique for Low-Contrast Images," *IEEE Access*, vol. 7, pp. 161 584–161 593, 2019.

[17] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," in 2010 Proceedings *IEEE INFOCOM, IEEE*, pp. 1–5, 2010.

[18] D. X. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proceeding *IEEE Symposium on Security and Privacy, S&P 2000, IEEE*, pp. 44–55, 2000.

[19] E.-J. Goh, "Secure Indexes," *Cryptology ePrint Archive*, 2003.

[20] P. Golle, J. Staddon, and B. Waters, "Secure Conjunctive Keyword Search Over Encrypted Data," in *International Conference on Applied Cryptography and Network Security, Springer*, pp. 31–45, 2004.

[21] D. J. Park, K. Kim, and P. J. Lee, "Public Key Encryption with Conjunctive field Keyword Search," in *International Workshop on Information Security Applications, Springer*, pp. 73–86, 2004.

[22] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," *Journal of Computer Security*, vol. 19, no. 5, pp. 895–934, 2011.

[23] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic, Searchable Symmetric Encryption," in Proceedings of the 2012 *ACM Conference on Computer and Communications Security*, pp. 965–976, 2012.

[24] K. S. P. Charalampos, "Parallel and Dynamic Searchable Symmetric Encryption financial Cryptography and Data Security 2013 Berlin," *Heidelberg Springer Berlin Heidelberg*, vol. 258, no. 274, pp. 10–1007, 2013.

[25] K. Kurosawa, K. Sasaki, K. Ohta, and K. Yoneyama, "UC-Secure Dynamic Searchable Symmetric Encryption Scheme," in *International Workshop on Security, Springer*, pp. 73–90, 2016.

[26] D. Wu, Q. Gan, and X. Wang, "Verifiable Public Key Encryption with Keyword Search Based on Homomorphic Encryption in a Multi-User Setting," *IEEE Access*, vol. 6, pp. 42 445–42 453, 2018.

[27] C. Guo, R. Zhuang, C.-C. Chang, and Q. Yuan, "Dynamic Multi-Keyword Ranked Search Based on Bloom Flter Over Encrypted Cloud Data," *IEEE Access*, vol. 7, pp. 35 826–35 837, 2019.

[28] J. Li, Y. Shi, and Y. Zhang, "Searchable Ciphertext-Policy Attribute-Based Encryption with Revocation In Cloud Storage," *International Journal of Communication Systems*, vol. 30, no. 1, pp. e2942, 2017.

[29] Q. Chai and G. Gong, "Verifiable Symmetric Searchable Encryption for Semi-Honest-But-Curious Cloud Servers," in 2012 *IEEE International Conference on Communications (ICC), IEEE*, pp. 917–922, 2012.

[30] K. Kurosawa and Y. Ohtaki, "UC-Secure Searchable Symmetric Encryption," in *International Conference on financial Cryptography and Data Security, Springer*, pp. 285–298, 2012.

[31] X. Jiang, J. Yu, J. Yan, and R. Hao, "Enabling Efficient and Verifiable Multi-Keyword Ranked Search over Encrypted Cloud Data," *Information Sciences*, vol. 403, pp. 22–41, 2017.

[32] 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, 2018.

[33] J. Niu, X. Li, J. Gao, and Y. Han, "Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for Iot," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1502–1518, 2019.

[34] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain-Based Private Keyword Search in Decentralized Storage," *Future Generation Computer Systems*, vol. 107, pp. 781–792, 2020.

[35] C. Cai, X. Yuan, and C. Wang, "Towards Trustworthy And Private Keyword Search in Encrypted Decentralized Storage," in 2017 *IEEE International Conference on Communications (ICC), IEEE*, pp.1–7, 2017.

[36] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications, IEEE*, pp. 792–800, 2018.

[37] A. Zhang and X. Lin, "Towards Secure and Privacy-Preserving Data Sharing in E-Health Systems Via Consortium Blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–18, 2018.

[38] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Outsourcing Service Fair Payment Based on Blockchain and its Applications in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 14, no. 4, pp. 1152–1166, 2018.

[39] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain Based Searchable Encryption for Electronic Health Record Sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.

[40] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-Assisted Public-Key Encryption with Keyword Search Against Keyword Guessing Attacks for Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1335–1348, 2019.

[41] C. Bo¨sch, R. Brinkman, P. Hartel, and W. Jonker, "Conjunctive Wildcard Search Over Encrypted Data," in *Workshop on Secure Data Management, Springer*, pp. 114–127, 2011.

[42] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An Efficient PHR Service System Supporting Fuzzy Keyword Search and fine-Grained Access Control," *Soft Computing*, vol. 18, no. 9, pp. 1795–1802, 2014.

[43] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. Jia, "Cloud-Based Electronic Health Record System Supporting Fuzzy Keyword Search," *Soft Computing*, vol. 20, no. 8, pp. 3243–3255, 2016.

[44] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving Usable and Privacy-Assured Similarity Search Over Outsourced Cloud Data," in 2012 Proceedings *IEEE INFOCOM, IEEE*, pp. 451–459, 2012.

[45] X. Zhu, Q. Liu, and G. Wang, "A Novel Verifiable and Dynamic Fuzzy Keyword Search Scheme over Encrypted Data in Cloud Computing," in 2016 *IEEE Trustcom/BigDataSE/ISPA, IEEE*, pp. 845–851, 2016.

[46] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward Efficient Multi-Keyword Fuzzy Search over Encrypted Outsourced Data with Accuracy Improvement," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2706–2716, 2016.

[47] G. Liu, G. Yang, S. Bai, Q. Zhou, and H. Dai, "Fsse: An Effective Fuzzy Semantic Searchable Encryption Scheme Over Encrypted Cloud Data," *IEEE Access*, vol. 8, pp. 71 893–71 906, 2020.

[48] S. Tahir, S. Ruj, A. Sajjad, and M. Rajarajan, "Fuzzy Keywords Enabled Ranked Searchable Encryption Scheme for a Public Cloud Environment," *Computer Communications*, vol. 133, pp. 102–114, 2019.

[49] H. Zhong, Z. Li, J. Cui, Y. Sun, and L. Liu, "Efficient Dynamic Multi-Keyword Fuzzy Search Over Encrypted Cloud Data," *Journal of Network and Computer Applications*, vol. 149, pp. 102469, 2020.

[50] Q. Xu, H. Shen, Y. Sang, and H. Tian, "Privacy-Preserving Ranked Fuzzy Keyword Search Over Encrypted Cloud Data," in 2013 *International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE*, pp. 239–245, 2013.

[51] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-Preserving Multi-Keyword Fuzzy Search Over Encrypted Data in the Cloud," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications, IEEE*, pp. 2112–2120, 2014.

[52] Y. Yang, S. Yang, and M. Ke, "Ranked Fuzzy Keyword Search Based on Simhash Over Encrypted Cloud Data," *Chinese Journal of Computers*, vol. 40, no. 2, pp. 431–444, 2017.

[53] Y. Yang, J. Liu, S. Cai, and S. Yang, "Fast Multi-Keyword Semantic Ranked Search in Cloud Computing," *Chinese Journal of Computers*, vol. 41, no. 6, pp. 1346–1359, 2018.

[54] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full Verifiability for Outsourced Decryption in Attribute-Based Encryption," *IEEE Transactions on Services Computing*, vol. 13, no. 3, pp. 478–487, 2017.

[55] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search Over Encrypted Cloud Data," in 2010 IEEE 30th *International Conference on Distributed Computing Systems, IEEE*, pp. 253–262, 2010.

[56] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access Pattern Disclosure on Searchable Encryption: Ramification, Attack and Mitigation," in *NDSS*, vol. 20, pp. 12, 2012.

[57] J. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. Chen, "A New Efficient Verifiable Fuzzy Keyword Search Scheme," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 3, no. 4, pp. 61–71, 2012.

[58] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving Effective Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 164–172, 2014.

[59] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, 2013.

[60] C. Cai, X. Yuan, and C. Wang, "Hardening Distributed and Encrypted Keyword Search Via Blockchain," in 2017 *IEEE Symposium on Privacy-Aware Computing (PAC), IEEE*, pp. 119–128, 2017.

[61] S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing with fine-Grained Access Control in Decentralized Storage Systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018.

[62] H. Li, H. Tian, F. Zhang, and J. He, "Blockchain-Based Searchable Symmetric Encryption Scheme," *Computers & Electrical Engineering*, vol. 73, pp. 32–45, 2019.

[63] H. G. Do and W. K. Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search," in 2017 *IEEE World Congress on Services (SERVICES), IEEE*, pp. 90–93, 2017.

[64] Q. Liu, G. Wang, and J. Wu, "An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing," in 2009 *International Conference on Computational Science and Engineering, IEEE*, vol. 2, pp.715–720, 2009.

[65] Q. Liu, G. Wang, and J. Wu. "Secure and Privacy Preserving Keyword Searching for Cloud Storage Services," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 927–933, 2012.

[66] G. Amanatidis, A. Boldyreva, and A. O'Neill, "Provably-Secure Schemes for Basic Query Support in Outsourced Databases," in *IFIP Annual Conference on Data and Applications Security and Privacy, Springer*, pp. 14–30, 2007.

[67] J. Katz, A. Sahai, and B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer*, pp. 146–162, 2008.

[68] M. T. Goodrich, R. Tamassia, and J. Hasic, "An Efficient Dynamic and Distributed RSA Accumulator," arXivpreprint arXiv:0905.1307, 2009.

[69] J. Wang, X. Chen, H. Ma, Q. Tang, J. Li, and H. Zhu, "A Verifiable Fuzzy Keyword Search Scheme Over Encrypted Data," *J. Internet Serv. Inf. Secur.*, vol. 2, no. 1/2, pp. 49–58, 2012.

[70] Y. Yang, Y.-C. Zhang, J. Liu, X.-M. Liu, F. Yuan, and S.-P. Zhong, "Chinese Multi-Keyword Fuzzy Rank Search Over Encrypted Cloud Data Based on Locality-Sensitive Hashing," *Journal of Information Science & Engineering*, vol. 35, no. 1, 2019.

[71] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," *International Conf. on the Theory and Applications of Cryptographic Techniques*, Interlaken, Switzerland, 2004.

[72] L. Ballard, S. Kamara, and F. Monrose, "Achieving Efficient Conjunctive Keyword Searches Over Encrypted Data," in *International Conference on Information and Communications Security, Springer*, pp. 414–426, 2005.

[73] Y. Lu, J. Li, and Y. Zhang, "Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks," *IEEE Transactions on Services Computing*, 2019.

[74] W. Zhang, B. Qin, X. Dong, and A. Tian, "Public-Key Encryption with Bidirectional Keyword Search and its Application to Encrypted Emails," *Computer Standards & Interfaces*, vol. 78, pp. 103542, 2021.

[75] Arriaga, Q. Tang, and P. Ryan, "Trapdoor Privacy in Asymmetric Searchable Encryption Schemes," in *International conference on cryptology in Africa, Springer*, pp. 31–50, 2014.

[76] M. M. Tajiki, M. Akhaee, and B. Bahrak, "Improved Secure Searchable Asymmetric Encryption for Cloud Storage Services," *Computing and Security*, vol. 2, no. 3, pp. 185–194, 2015.

[77] S. Lv, Y. Huang, B. Li, Y. Wei, Z. Liu, J. K. Liu, and D. H. Lee, "Forward Secure Searchable Encryption Using Key-Based Blocks Chain Technique," in *International Conference on Algorithms and Architectures for Parallel Processing, Springer*, pp. 85–97, 2018.

[78] L. Sardar and S. Ruj, "Fspvdsse: A Forward Secure Publicly Verifiable Dynamic SSE Scheme," in *International Conference on Provable Security, Springer*, pp. 355–371, 2019.

[79] S. Xiao, A. Ge, J. Zhang, C. Ma, and X. Wang, "Asymmetric Searchable Encryption from Inner Product Encryption," in *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Springer*, pp. 123–132, 2016.

[80] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, "Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries," in *Annual Cryptology Conference, Springer*, pp. 353–373, 2013.