International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I9P218

Volume 71 Issue 9, 186-211, September 2023

Review Article

Analysis of the Challenges Involved in Efficient and Secure Ranked Multi- Keyword Search over Encrypted Cloud Data

Sheenam Malhotra[1], Williamjeet Singh[2]

[1,2]*Department of Computer Science and Engineering, Faculty of Engineering and Technology, Punjabi University, Patiala, Punjab, India.*

[1]*Corresponding Author : sheenam.malhotra@gmail.com*

Received: 16 May 2023 Revised: 29 July 2023 Accepted: 15 August 2023 Published: 03 September 2023

Abstract *- Current IT-based applications primarily use the concept of on-demand network access to satisfy their resource requirements. Cloud computing has emerged as the most viable platform for delivering the above service due to its cost-efficient and secure service delivery model. Due to this increasing reliance on on-demand resource access, the research community is paying exponentially increased attention towards optimizing the cloud along with improving the deployed security model. A massive amount of work has been done in this field by researchers in the past few years, as every technology has certain challenges associated with it. Although it is secure, it still demands more work to be done in the fields of security, resource management, traffic management, energy efficiency and data retrieval. This paper gives a review of research done in the field of secure and efficient retrieval of encrypted cloud data, which is the hottest area of research these days. The main contribution of this review is to get the gist of data retrieval systems over the cloud and to bring awareness about the contribution of various researchers in this emerging and challenging area. The paper also provides a secure three-tier encryption algorithm to encrypt the index and data over the cloud. For security, the paper focuses on searchable encryption schemes. For efficiency, it focuses on indexing techniques, searching strategies for single and multi-keyword search and ranking and retrieval methods for encrypted data over the cloud.*

Keywords *- Cloud computing, Searchable encryption, Multi-keyword search, Cloud storage, Document ranking and retrieval.*

1. Introduction

With the advent of computing-based applications, the demand for more resources, internet data usage, and many other essentials arises. Nowadays, most of the population is taking the benefits and advantages of internet services, storing their personal data over the cloud and retrieving essential information. As the development phase of science and technology is reaching new changes, many challenges still need to be resolved. In the past, people usually worked or ran their applications on the downloaded software on a physical computer or server in a building.

However, with a cloud environment, people can access the same applications through the internet. Social interactions and checking bank balance on the phone is now possible only with the cloud. Many businesses are moving towards cloud computing only because of its increasing efficiency. With the help of the cloud, we can access work from multiple devices and anywhere, making it easier for teams to collaborate on shared data. According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing has drastically changed, leading to reduced hardware and software costs. Cloud provides a high-security mechanism as well as handles data storage remotely. Cloud provides a huge amount of applications in various areas that include business, online entertainment, telecommunication, finance and banking, educational sector and healthcare. The business delivery model provides a user experience by which hardware, software and network resources are optimally leveraged to provide innovative services over the web and servers. For organizations currently using traditional infrastructures, a cloud will enable users to consume IT resources in the data center in ways that were never available before [90].

The paper here provides a survey of various techniques used over the cloud, its applications, benefits, challenges and services that the cloud offers to its users. The paper is organized as follows: Section 1 comprises an introduction, Section 2 comprises the preliminaries, Section 3 consists of existing studies surveyed, i.e. related work, Section 4 analysis the Futuristic Scope Based on Existing Studies, Section 5 dicusses the results and followed by conclusions in section 6.

2. Preliminaries

In order to achieve efficient and secure search in a cloud computing environment, researchers are focusing efforts on two preliminary aspects: the storage space model and retrieval efficiency structure. Both aspects affect the outcome of the system and contribute towards an effective model in their own way.

2.1. Storage Vector Space

The storage and retrieval of documents incorporate vector space modeling based on calculating some weight value assigned to each file. Every file contains relative weight, which converts it into vector model architecture.

This model allows for calculating similarity features between the file and the trapdoor or query, and then, based on the relevance score, ranking can be done for a given search.

2.2. Encrypted Index

For every document file that is stored in encrypted form on a cloud server, there exists a certain set of keywords and an encrypted index value. For every search term in the query, the trapdoor is generated, and a relevant set of documents is retrieved based on some neutral index value.

The figure shown below describes the general framework for ranked data retrieval using a multi-keyword search. Functions performed by a general model of ranked data retrieval are described below:

2.2.1. Generate Key

The secure key Sec K is generated by the data owner.

2.2.2. Build Index

The plaintext index tree is constructed by the data owner and then encrypted using key SK and sent to CSP along with the encrypted data.

2.2.3. Generate Query

The query keywords Sq are transformed into the query TQ by the data user. The data user sends query TQ to the Cloud Server.

2.2.4. Execute Search

Cloud Server performs the secure multi-keyword text search to obtain search results and then return them to the data user.

2.3. Ranking Function

The ranked searchable symmetric encryption scheme depends on searching by keywords. The ranking function or the relevance function score is used to sort the relevant documents by ranking them based on keywords contained within them. Various ranking methods have been used, but the most commonly prevalent among all is TF*IDF. It calculates the relevance function based on the keywords or watchwords. The term frequency and Inverse document frequency are calculated depending on keywords in trapdoor.TF*IDF comes in various versions where every new version overcomes the other in terms of output efficiency [50, 79].

3. Related Work

The section discusses the existing studies surveyed, including various techniques used or implemented over the cloud. The data is stored in an encrypted form over the cloud before outsourcing so that an unauthorized user cannot access it, and it can be well protected from various attacks. The data retrieval system involves five components, and each component has its own research gaps. The first component is the encryption of plain text to cipher text, the second is the indexing scheme to be implemented on encrypted data, and the third is searching techniques to find results relevant to the search query; fourth is authentication protocol to be implemented for authentication of data user; and fifth is ranking of results based on user relevance and retrieval techniques developed for efficient retrieval of cloud data.

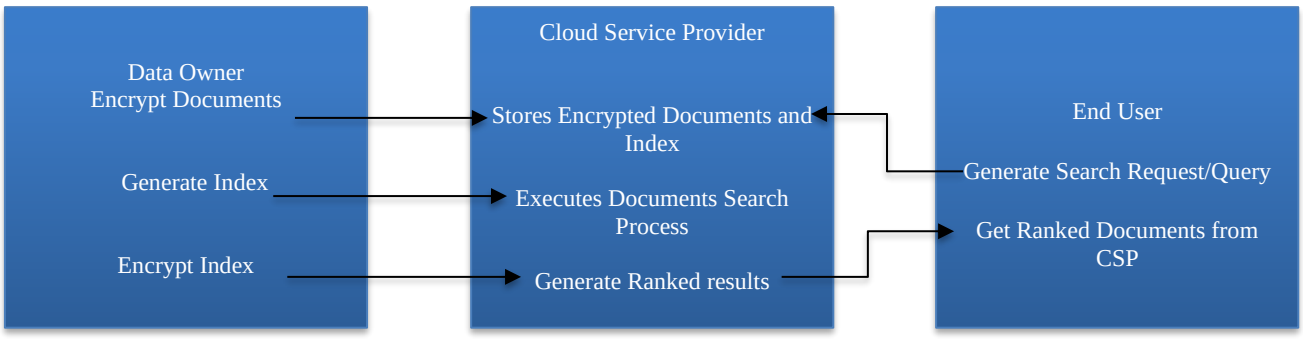


Fig. 1 General framework for ranked data retrieval using keyword search

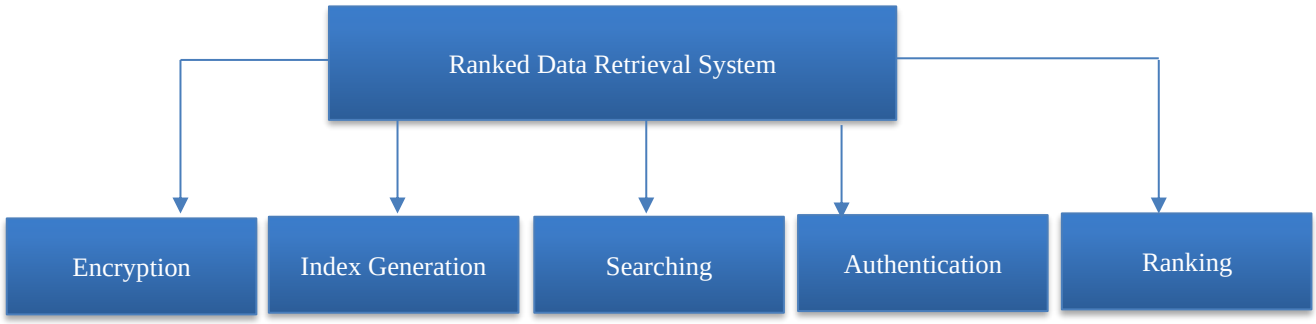


Fig 2. Components of ranked data retrieval system over cloud

3.1. Encryption of Data and Index

In this era, data security and confidentiality is the main aspect to focus on, as everyone wants his data to be protected from other users. An enormous amount of work has been done in the past on encryption algorithms to protect the data as it is converted into an unreadable format. While talking about the cloud environment, the basic concept is that algorithms are either public key or private key, but the only difference is that they need to be enhanced or improved by enforcing certain frameworks or encryption schemes, as CSP is solely responsible for the secrecy of data of many data owners. As the size of data stored on the cloud is enormous, to enable efficient search on data, the index is also stored on the cloud. Now, if it remains unencrypted, this index may reveal a lot of information to CSP, so index encryption was introduced to enable good privacy. The evolution of searchable encryption schemes, along with their pros and cons, is described as follows:

To access the data from the cloud, the client encrypts data by generating search tokens to send as queries to a storage server. Searchable Symmetric Encryption (SSE) is the most widely used scheme to search for encrypted data. Seny Kamara et.al. (2012) constructed dynamic SSE against adaptive chosen keyword attacks and provided optimal search time. Pseudo-RANDOM Functions (PRF) and Pseudo-Random Permutations (PRP) are used, which are polynomial-time computable functions. The scheme was an extension of SSE-1 from the previous studies based on an inverted index. SSE-1 is unsuitable for use in cryptographic cloud storage services as it is only secure against non-adaptive chosen keyword attacks, and it is not explicitly dynamic. However, the proposed scheme fails to secure the information as it leads to leakage problems, and it also does not include the cost of producing a plain text index as a computation cost. But SSE satisfies all the above properties related to search time, security, etc.[6, 52, 77].

Jyun-Yao Huang and I-En Liao (2012) propose a fault-tolerant scheme for cloud computing. The earlier studies have a limitation related to range queries and cannot provide text search. So, they provide an integrated scheme for numeric data and text data queries and provide corresponding searchable encryption. The architecture of the proposed scheme is partitioned into two parts: trusted private cloud service and un-trusted cloud service [10].

Various attribute-based encryption schemes were used earlier to encrypt data for security purposes in the cloud. Cheng-Chi Lee et al. (2013) present a survey on various encryption schemes based on attributes used for access control in the cloud environment. Attributes play an important role and are used to generate public keys and as an access policy to control the access rights of users. The access policy can be a key-based policy or a ciphertext-based policy. Attribute based encryption helps to reduce the communication overhead of the internet and provides a fine-grained access control suitable for private clouds. [12, 93]

Comparison of cryptographic techniques ECC and RSA with the key size of 160 bit and 1024 bit respectively is performed in previous studies that provide ECC has the advantage in resource-constrained devices over RSA algorithm. Both algorithms are efficient schemes of Public Key Encryption [13].

Vishwanath S. Mahalle and Aniket K Shahade (2014) present a Hybrid (RSA & AES) encryption algorithm for data security. The work provides the biggest advantage of key generation based on system time, and an attacker cannot even guess them. Cloud administrators cannot access user's private data because the private key and secret key are only known to the user. RSA and AES provide three keys for the main purpose of using these algorithms: public key for encryption, private key, and secret key for decryption. After uploading, the data is stored in an encrypted form and can be decrypted only by the user's private and secret keys. The method provides good security to the user's data on the cloud [14].

K. Seekar and M. Padmavathamma (2016) present an approach for encrypting and decrypting the data before sending it to the cloud. Data security is also a main challenge that needs to be resolved as the attacker makes a fake request, but when a legitimate request wants to execute, the system denies processing the same request due to the unavailability of resources. So, they present an approach that prevents the fake

request using double data encryption, which they used to choose Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA) as symmetric and asymmetric algorithms. Data encryption is considered a suitable mechanism for solving the data level issues. Among the above algorithms, AES uses less encryption and decryption time and also consumes less buffer space as compared to DES and RSA algorithms. AES is considered a better algorithm than DES and RSA [33, 94].

After the discovery of RSA, Fully Homomorphic Encryption (FHE) was introduced; this allows a worker to perform arbitrary computations on the encrypted data. Jian Liu, Jing-Li Han Zhao-Li Wang (2016) constructed a new secure searchable encryption scheme for single keyword searching. The scheme is achieved using a Multikey Fully Homomorphic Encryption Scheme (MFHE). They discuss the applications of Multikey Homomorphic Encryption (MFHE). It provides security and privacy of the data, but query efficiency was not much better. [35, 80]

As discussed in the cloud applications above in Section 1, we know it is also widely used in healthcare services and medical organizations. Abdelali El Bouchti, Samir Bahsani, and Tarik Nahhal (2016) present data encryption mechanisms in the healthcare cloud computing environment. They explore the healthcare cloud environment and design and implement cryptography algorithms, namely homomorphic encryption and RSA, in the proposed architecture to provide security to information. They also presented Elliptic-based additive homomorphic encryption to be used in the OpenStack framework in the healthcare cloud. [36]

Many hybrid approaches are used or implemented in the cloud to provide security. But Chengliang Liang, Ning Ye, Reza Malekian, and Ruchuan Wang (2016) propose a hybrid encryption scheme to provide security to lightweight data on the cloud. They firstly improve the RSA algorithm so that it can quickly generate big primes in a cloud environment, as the earlier RSA has low efficiency in generating big primes. Then, they combine or merge the AES and improved RSA algorithms to get a suitable hybrid encryption scheme for the security of lightweight data. The hybrid algorithm improves the RSA speed and solves the key management issue in the AES algorithm.

The results show that the scheme provides many hybrid approaches are used or implemented in the cloud to provide security. But Chengliang Liang et al. propose a hybrid encryption scheme to provide security to lightweight data on the cloud. Firstly, they improve the RSA algorithm to quickly generate big primes in a cloud environment, as the earlier RSA has low efficiency in generating big primes. Then, they combine or merge the AES and improved RSA algorithms to get a suitable hybrid encryption scheme for the security of lightweight data. The hybrid algorithm improves the RSA speed and solves the key management issue in the AES algorithm. The results show that the scheme provides a fast encryption and decryption mechanism, is more secure, and can handle security issues efficiently [41]. Multiple-user searchable encryption with keyword authorization is also introduced in cloud storage, which satisfies all data security properties, sublinear search time, concise indexes and authorizes or revokes a user efficiently. Asymmetric bilinear map groups and keywords authorization binary tree for constructing multi-user searchable encryption was also proposed, which was able to authorize a designed user to search for a subset of keywords [44, 51]. Then, RSE was proposed based on relevance score in a single keyword search [48].

Table 1. Analysis of encryption schemes

Encryption Scheme	Key management	Key length	Time overhead	Speed	Security	Storage overhead
AES	Difficult	Long	Less	Fast	Excellent	Less
CBC	NA	Long	More	Slow	Low	Less
PKCS5	Easy	NA	More	Slow	High	Less
PEKS	Easy	NA	More	Slow	High	Less
IPEKS	Easy	NA	Less	Fast	Low	More
RSA	Easy	Long	More	Slow	Very high	More
DES	Easy	Too short	More	Very slow	High	Less
ECC	Easy	Short	Less	Very fast	Very high	Less
IBE	Easy	NA	More	Slow	High	More
RSA+ECC	Easy	Long	Less	Very fast	Excellent	Less
AES+RSA	Easy	Long	More	Fast	Very high	More
SSL	NA	Short	More	NA	Excellent	More
Homomorphic	Easy	Medium	Less	Fast	High	Very high
NTRU-PEKS	Easy	Short	Very less	Fast	Excellent	More

Table 2. Analysis of the research gaps in encryption schemes used for encryption of data/index

Algorithm	Index	Data	Research Gaps/ Scope of Improvement	Reference
AES	Y	Y	Key management issues and indexes consist of entire documents, which makes searching slow.	[22][33][73][77]
CBC	Y	Y	The index consists of an entire document, which makes searching slow.	[22]
PKCS5	Y	Y	The index consists of the entire document, which makes searching slow.	[22]
PEKS	N	Y	It has limited search capabilities.	[22]
Ipeks	N	Y	It removes the limitation of perks but at the cost of storage overhead, which can further be improved.	[22]
RSA	N	N	It has a slow speed, which can further be improved.	[16][33][74][75][76][77]
DES	N	N	It has too short a key length, so it is more prone to side attacks.	[33][75]
ECC	Y	Y	It has a shorter key length as compared to RSA.	[16][73][76]
IBE	N	N	Less efficient as compared to RSA+ECC.	[37]
RSA+ECC	Y	Y	Secure and more efficient than IBE.	[37]
Homomorphic	N	N	It is computationally complex.	[34]
AES+IMPROVED RSA(by Montgomery algorithm)	Y	Y	It is the most efficient and secure and offers easy key management, but the index consists of whole documents instead of certain keywords to reduce search time.	[20][41]
128 bit SSL	Y	Y	It can be used for single-keyword searches, but supporting multi-keyword searches still needs improvement.	[9]

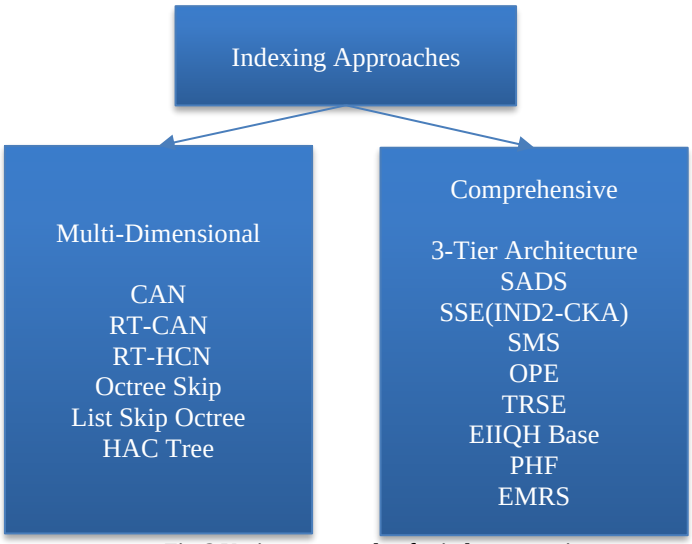


Fig. 3 Various approaches for index generation

3.2. Index Generation Techniques for Cloud Data

Constructing an index for improving the search efficiency is the most important aspect of research in data retrieval from CSP. The index structure can be constructed either by a multidimensional approach or a comprehensive approach. The multidimensional approach focuses on different aspects of the same problem in parallel, whereas the comprehensive approach enables drawing expertise to have the single best possible solution to the problem [68]. Index construction involves both approaches, which are further elaborated as follows:

A multidimensional indexing scheme in epic is proposed, which is referred to as RT-CAN. RT-CAN supports multidimensional query processing in the cloud. The global index is distributed in this scheme, and the servers are organized into an overlay structure. A mapping function is used to map R-tree nodes and CAN servers. A consistent hashing scheme retrieves data from the index; it is key-based and unsuitable for multidimensional or range queries. So, a variant of CAN is used to support multidimensional data, as CAN has a high routing cost. In the query processing mechanism, three types of queries are processed, i.e. point, range, and KNN, using uniform (3-dimensional) and traffic (2-dimensional) datasets. Only the network cost is considered in the cost model. System performance is affected by query processing cost and index maintenance cost in the RT-CAN indexing system. The performance of range queries, KNN queries [67] and updates are evaluated, and the effect of index tuning, routing cache and dimensionality is also studied and considered [3].

Data protection in the cloud is a challenge or an emerging issue. Authorized users can access data, and various kinds of attacks can be possible on data that may lead to information leakage problems. Anna Squicciarini, Smitha Sundareswaran, and Dan Lin (2010) explore the data leakage issue due to indexing in the cloud. To overcome the problem, the three-tier data protection architecture was designed, and a portable data binding technique for users' privacy requirements was developed. It provides various benefits; it does not depend on trusted computing architectures and provides full control from the user end. With SAML infrastructure servers, authentication is achieved. As an executable enforcement mechanism, this maximises the programmable capacity of JAR files. This will further lead to enclosing the data and its related policies as access rights can be converted to executable codes—the technique consists of binding policies, authentication in indexing, and policy and data enforcement. Still, the approach can be further extended for better results [4].

Mariana Raykova et al.(2012) provide an exact keyword matching scheme referred to as a secure, anonymous database search scheme (SADS). They describe a general framework for engineering usable, secure private information with the help of which semantic errors can be minimized and query flexibility can be enhanced. In the proposed system, the search time is more than the round-up time, but it does not have any additional overhead, so it is suitable for real-world search systems [5].

Fangquan Cheng et al. present an SSE scheme that provides support to highly efficient one-round multiple-keyword queries over large data that is symmetrically encrypted. The proposed scheme provides security against chosen-keyword attacks (IND2-CKA) and overcomes the problem of search pattern leakage. Indexes are prone to adaptive chosen keyword attacks. In order to avoid a successful guessing attack, the data owner will add entry gamma(G) in the Build Index before sending it to the server. Now, G(yi) will be a non-empty bucket at a particular position to which gamma will point. It will send G(yi) along with the real data vector to avoid guessing the actual data by the attacker. It provides a security mechanism for indexing using fake rules. The work focuses on the best possible solutions for search efficiency [21].

Hongwei Li et al. provide experiments for EMRS that depict the scheme as having high functionality and search efficiency.[28][95] Also, the Cuckoo hashing technique for searchable index construction was proposed to improve privacy, security and query efficiency of data retrieval over cloud storage. The F-measue, precision and recall are taken as parameters to evaluate the performance of cuckoo hashing and Latent Semantic Search (LSS)[84].

Various keyword-searching techniques are reviewed by Arpitha T V Mallikarjuna Shastry (2016) to find successful techniques for retrieving information and documents over the cloud. Secured Multiple-Keyword Search (SMS) helps to develop a safe cloud data consumption method but fails to get relevant data, which does not provide ranking and Boolean search. Order Preserving Encryption (OPE) provides some security for data leakage. Two Round Searchable Encryption (TRSE) further improved retrieved results' security and prevented leakage. Multi-Keyword Text/Keyword Search (MTS) provides secure cloud server search over encrypted data. Searchable Symmetric Encryption (SSE) uses TRSE to give top-k multi-keyword retrieval results. Synonym-based search and multi-keyword ranked search uses TF-IDF algorithms. The paper provides a review of various searchable encryption techniques in view of single keyword, multiple keywords search, Ranking, Similarity search and Fuzzy resilience [30].

Xin Zhou et al.(2016) discuss interval query and indexing. They analyze the existing studies related to interval indexing and searching. There is very little research carried out on interval indexing. They propose a new secure index structure, Indexing for Interval Query Hbase (EIIQHbase), to improve existing EPI+MRST and searching algorithms are

also proposed so that space overhead and respond time can be reduced. EIIQHbase overcomes the drawbacks of the existing study of EPI+MRST. With the help of the proposed index structure, query performance is improved, and results demonstrate that the scheme is effective and efficient [39].

Zhu Xiangyang et al. (2017) propose an efficient and accurate verifiable privacy-preserving multikeyword text search over encrypted cloud data known as MUSE. HAC-tree index structure is proposed to improve the efficiency of text searching based on hierarchical agglomerative clustering. The index structure HAC-tree also collects documents of high relevancy in clusters. Two search schemes are discussed based on MUSE: Basic multi-keyword text search over encrypted cloud data (BMUSE) and Enhanced secure multi-keyword text search over encrypted cloud data (EMUSE). BMUSE secure the documents, index and query confidentiality by resisting cipher text attacks, but if the query keyword to be searched is the same next time, then the trapdoor and access part will also be the same so that BMUSE may disclose the trapdoor unlink ability and keyword privacy. However, EMUSE adds random values to the relevant scores between documents and queries to overcome cipher text attacks. The scheme has good efficiency and accuracy compared to existing schemes and methods [46, 101].

As the amount of data drastically increases over the cloud, the traditional searching methods require content tagging with descriptive metadata and then matching search queries with metadata. The user experience degrades if the quality of metadata generated is low. Based on the content similarity, the search methods involving content tagging are drawing more attention [70].

By looking at the content as the most important feature, the content-based search retrieves the relevant results. The state-of-art research for content-based data retrieval involves two aspects. Firstly, extract the descriptive features to represent the content and then reduce the latency of a single query trapdoor [69, 71, 72]. Table 3 and Table 4 show the analysis of comprehensive and multidimensional approaches used for indexing over cloud data.

Nan Zu et al.proposed and indexing system called Partitioned Rash Forest (PRF), which was update-efficient. It uses a hierarchical memory system that enables it to handle requests efficiently. It provides better quality results by using a small portion of the query as compared to the LSH indexing structure used in the framework of the cloud for healthcare monitoring [49, 81].

Table 3. Analysis of indexing techniques using a comprehensive approach

Technique	Scope of Improvement
3-tier architecture (provide different levels of security required for a variety of data in a single document)	Required improvement for information leakage attacks and scalability issues is still unaddressed.
SADS	The issue of long search time remains unaddressed.
IND2-CKA	Prone to adaptive chosen attack.
SMS	Do not provide ranked results and was inefficient.
OPE	Has data leakage loophole.
EMRS(index construction via blind storage)	It improves search efficiency and conceals search patterns but still has the issue of scalability of the index.
TRSE	Stemming is used to construct an index but has issues with pattern recognition attacks and results in low search accuracy.
Efficient Indexing for Interval Query Hbase (EIIQHbase)	Computational overhead is high because of the use of two sub-indexes. Also, index updation and scalability is still an issue. It has low index efficiency for interval queries.
PHF	Although being a scalable and efficient approach, it still causes query overhead when implemented.

Table 4. Indexing techniques using multidimensional approach

Technique	Scope of Improvement
CAN	It uses a hash function for routing between nodes of the tree. This approach suffers from high routing overheads.
RT-CAN	This approach maps R-Tree nodes to CAN servers. It supports point query processing but does not support range queries.
LSB TREE	In this, the hash key is converted into z order value to be indexed by the B tree. It suffers extra storage overhead, scalability issues and index update issues.
SKP LIST	It is an extension of the ordered list suitable for parallel computation applications. Still, it is not recommended because worse time complexity affects retrieval efficiency.
SKIPTREE	This approach has low storage capacity, is slow, and hence is less efficient.
SKIP OCTREE	It is a combination of skiplist and Octree. It supports dynamic index scaling and multidimensional queries but has scope for improvement in ensuring query efficiency by enhancing data consistency.
RT-HCN	Although being storage and space efficient, it deals with scalability issues if the size and the number of indices increase.
HAC TREE	Among all the multidimensional approaches, it is the most efficient and gives accurate results.

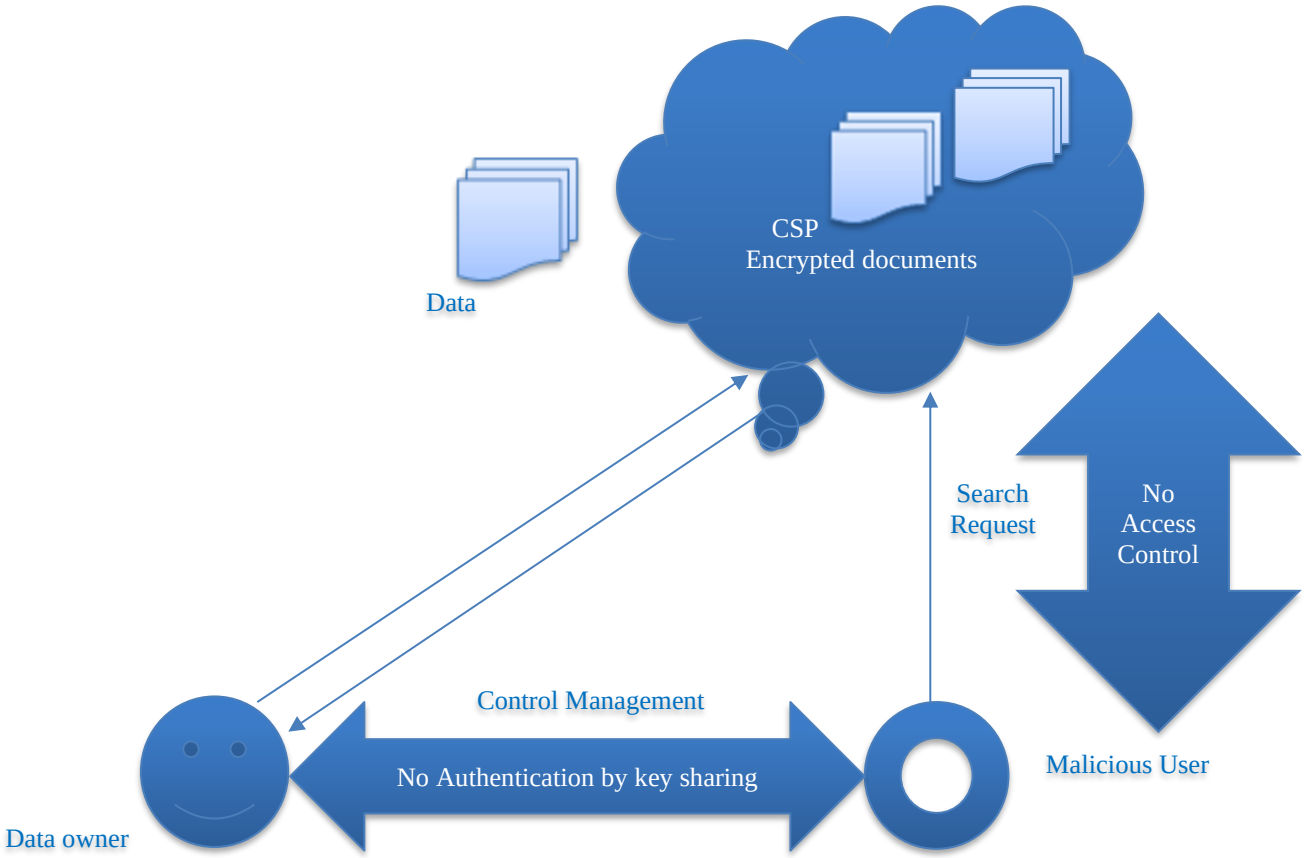


Fig. 4 Data retrieval without access control procedure

3.3. Index Generation Techniques for Cloud Data

While having adapted to cloud technology, the data owner uses services provided by the cloud like SAAS, IAAS, PAAS, CAAS, DAAS, etc. Since then, the cloud has been used for data storage as far as its usage is concerned. Data that is stored on the cloud is always in cipher form. This data conversion into cipher form, which is called encryption, is performed by CSP. But this approach makes the CSP a single point to attack by malicious users. The other way is that the owner encrypts the data and sends encrypted documents to CSP along with the encrypted index to search for the relevant data easily from CSP. Now, in this method, the owner becomes the source of temptation for hackers. In both cases, some provision is required to control the access of data by unauthorized users. It is also called access control, as the access is restrained or granted to the client by the data owner as per authentication or access control protocols. This is shown in the figure above.

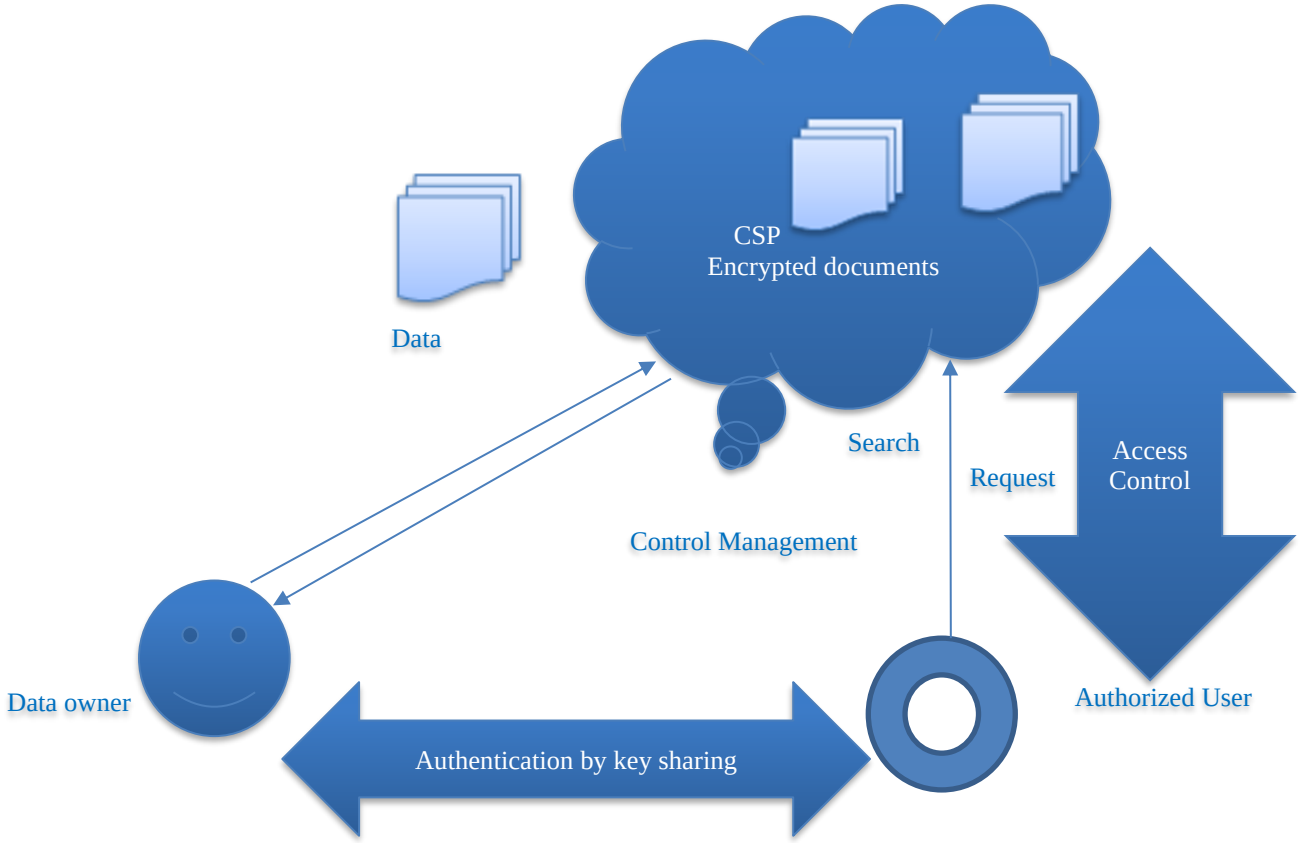


Fig. 5 Data Retrieval using access control procedure

Access control must be performed on CSP to restrict any attacker from getting data from CSP [58] and on the owner side to restrict access to his data by authenticated clients only. So, to embed this confidentiality, data owners, along with the encryption of documents, also frame an access scheme to allow only certain users to have access to those documents. CP-ABE allows this capability to secure the system and preserve data privacy from unauthorized users.

Traditional access control mechanisms like DAC[86], MAC[87], bell-la-pedula[88], and RBAC[89] are not suitable for cloud environments because of the following limitations:

1. These schemes are unsuitable for large-scale cloud applications as they are not flexible enough to support large data.
2. The user's role may vary from application to application, so these schemes are not dynamically adaptable.
3. There is a need for more secure algorithms to meet the needs of new authentication models.

CP-ABE overcomes all the above limitations and is more widely used for providing confidentiality on cloud platforms [85].

The timestamp approach, nonce approach and one-time secret-based approach provide the security mechanism and are also more efficient than the existing authentication schemes [40].

The table below represents the analysis of various access control techniques based on various attacks, computational complexity, scalability and flexibility of technique.

Table 5. Analysis of access control mechanism based on functional and security parameters [9]

Access control Mechanism	Cloud side	Data Owner Side	Flexibility	Scalability	Computational Complexity	DOS Attack	Replay Attack	Password Guessing Attack	Man in Middle Attack
Role-based	✓							✓	
Attribute-based	✓		✓	✓	✓	✓		✓	
Provenance based	✓							✓	
Blockchain-based	✓				✓				
Two-factor authentication framework of OOB factor and separate communication channels	✓					✓	✓	✓	✓
CP-ABE	✓	✓	✓	✓	✓	✓	✓	✓	✓

3.4. Searching Strategies for Single/Multi-Keyword Search

To search the document from the list of documents stored by the data owner, single keyword search or multi-keyword search can be implemented. Various researchers have implemented search strategies to achieve efficient results; still, there has always been scope for improvement in this area. The general model of ranked single/multi-keyword search is depicted in the figure below.

:

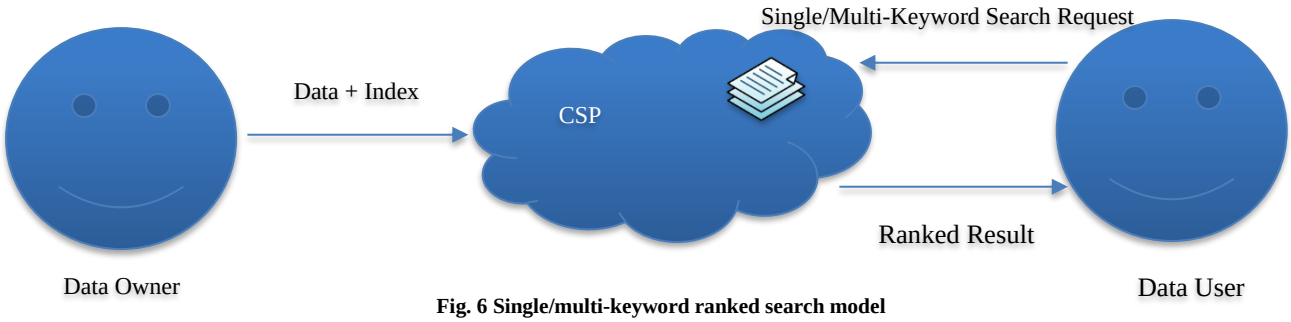


Fig. 6 Single/multi-keyword ranked search model

Many secure searching techniques have been proposed by various researchers like SCKS-XDH, SCKS-SS, Attribute-based encryption, RSSE, synonym-based search, fuzzy keyword search, etc [1, 2, 8, 15]. The comparison of search schemes is shown in table 6. SSE was first used to resolve the ranked search problem over encrypted cloud data, but the results were inefficient. DARPA recognized the era of searchable encryption considering data security for national and private information systems [53, 54, 78]. Pang et al. proposed SSE, basically referred to as SSE, that allows only authorized users to generate a search on the encrypted data and also allows Multiple Users Keyword Search (MUKS)[65]. SSE is implemented using public key encryption and private key encryption. PEKS conceals access patterns with the tradeoff between the overhead of search time and efficiency compared to private key search encryption [55, 66]. In the second private key method, the index and data are stored and encrypted on the server, which provides the confidentiality of data access patterns for the entire information [56, 57]. Synonym-based MKS was proposed over encrypted cloud data, but still, there is a scope to research a search scheme based on semantics that supports syntactic transformation, anaphora resolution and other NLP technology [92].

Semantic and secure keyword base search was proposed to get exact details required by the user. This technique also ensures that the same trapdoor does not produce the same results each time to address the issue of data confidentiality and integrity [99]. Another privacy-preserving semantic keyword-based searching algorithm was proposed, incorporating a stemming algorithm that reduces the index size [96, 97]. Semantic based scheme was extended for mobile

devices, making use of graphs to retrieve the results from the cloud server [98]. MT scheme with similarity-based ranking used A tree-based index structure [25], and various adaption methods for multidimensional (MD) algorithms are proposed to improve search efficiency [17].

A secure and efficient scheme was proposed to retrieve files in order of relevance to keywords without index updation overhead [38]. Another homomorphic encryption scheme is applied to assure the privacy of sensitive data. However, the scheme is highly computationally complex and has a high communication overhead that must be addressed[100]. A multiple keyword ranked search was developed to support search results verification to retrieve the results. Qset-based data structure TF*IDF and MAC are also used to make it efficient, and there is also a need to investigate the rank order of the search results [45].

The table clearly depicts strategies that use single-keyword or multi-keyword searches. In order to achieve accuracy in results, the multi-keyword search is preferred. The search time should be reduced for efficient search, which can further include many improvement parameters like an efficient index construction scheme, reduced encryption and decryption time, reduced delay time, etc. Focus can be made on storage techniques in a certain manner that can improve search efficiency.

Table 6. Analysis of various search schemes

Search Scheme	Single Keyword	Multiple Keyword	Ranked Results	Index Updation	Access Pattern/sensitive data hiding	Efficiency	Search Time
SCKS	✓					Low	More
SSE	✓					Low	More
Multi-user SSE[18]		✓		✓		Low	More
PEKS					✓	Low	More
RSSE	✓	✓	✓			Low	More
OPSE						Low	More
Synonym based MKRS		✓	✓			Low	More
Privacy-preserving MKtext search		✓			✓	High	Less
Verifiable fuzzy KS	✓				✓	Low	More
Semantic MKRS		✓	✓		✓	High	Less
Multi-owner ranked search		✓	✓	✓		High	Less

3.5. Rankings and Retrieval of Encrypted Cloud Data

Cloud computing provides an IAAS service that enables us to store an enormous amount of data at CSP. As discussed above, the two aspects of data storage and data search, the third major aspect is data retrieval. Data retrieval is useless if the results contain a major proportion of irrelevant results required by the user. So, ranking results in the order of relevance to the user is required. While retrieving essential data from the cloud, sometimes the queried search terms contain sensitive information that must be kept secret from the database holder to prevent the information leakage problem. Cengiz Örencik and Erkay Savas (2012) propose a privacy-preserving ranked keyword search scheme based on Private Information Retrieval (PIR) [19]. The scheme supports multi-keyword queries with the ranking criteria and also increases the keyword search scheme's security. The scheme also satisfies efficient communication and computation requirements. They solve the problem of efficient and secure ranked multi-keyword search on remotely stored encrypted database model stored on a remote machine where the database users are protected against privacy violations. A symmetric key encryption method is used for encrypting documents, increasing the scheme's efficiency. To access the contents of retrieved documents, blinded encryption is used. The proposed method fulfills security requirements, and the ranking method returns highly relevant documents. There are still further improvements that can be explored [7].

As cloud computing is recommended for various applications, security in the cloud is still an issue that must be resolved. Many researchers and scholars are working for the betterment of cloud security. Sandeep K. Sood (2012) proposes a framework that consists of various techniques and procedures that will protect the data from the owner to the

cloud and then to the user. Three cryptographic parameters for data confidentiality, availability and integrity are discussed. He uses Secure Socket Layer (SSL) 128-bit encryption for data protection and can be raised to 256-bit encryption. Message Authentication Code (MAC) is used in three sections in cloud storage for integrity check, division and searchable encryption of data [9].

Privacy of data, privacy of the data owner and privacy of the retriever are essential requirements in terms of privacy and security that are considered in designing a searchable encryption scheme. Existing searchable schemes fulfill these requirements but lag behind in search efficiency. Dongyoung Koo, Junbeom Hur, and Hyunsoo Yoon (2013) propose a new searchable encryption that makes use of an Attribute-Based Encryption (ABE) scheme and is elaborated in Figure 7 [82,11]:

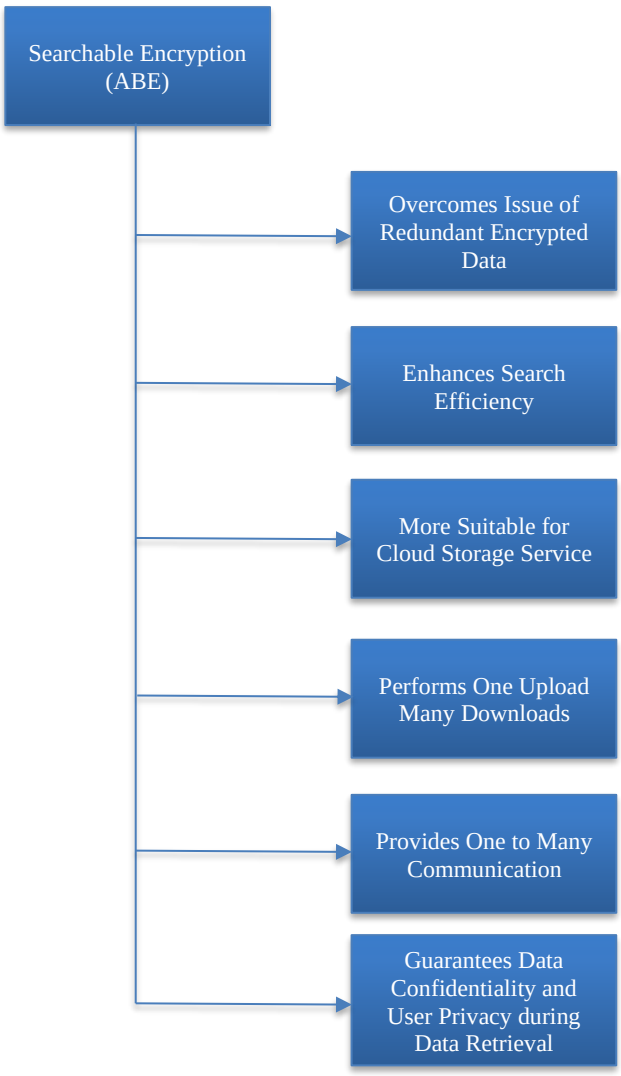


Fig. 7 Searchable ABE

Z. Jiang and L. Liu (2013) present a Disjunctively Oblivious Keyword Search (DOKS) that enables efficient, secure, and fast searching with short encrypted text. The drawback of the technique was that there was no relationship between an encrypted document and a query keyword, and it could not support multi-keyword search[59, 61]. Then, a new Dictionary and Lingual Keyword Search (DLKS) was proposed by S. Kumar Verma, S. Mathew, S. Srivastava, and S. Venkataesan, allowing multi-lingual searching and maintaining data integrity on CSP. The technique was more secure with reduced search time and computational overhead [62].

Y. Lu proposed a Logarithmic Search Over Encrypted Data (LSED), which was secure and supported query authentication. However, its drawback was that it was prone to pattern recognition attacks at CSP. Also, it gives all the control of data updation and query authorization to the data owner, which is more susceptible to a single hotspot of failure[63]. Z. Xia et. al. (2013) presented a similarity-based search over encrypted images to provide confidentiality of the image database. The technique was accurate in results with the tradeoff between accuracy and time complexity [64].

For secure and efficient retrieval of content, it is desired to ensure that the user can perform a search over the encrypted data in such a manner that the server is unaware of the content and searched keywords. The cryptographic method that provides this feature is Searchable Encryption (SE). In a privacy preservation-based search, the CSP is unaware of any content about the keywords and encrypted documents.

It can hide the data as well as the trapdoor during searching. Although it is semantically secure based on Identity-Based Encryption (IBE) and Bilinear Diffe-Hellman (BDH) assumptions, the practical efficacy is not proved by experimental setups [60].

Md Iftekhar Salam et al. (2015) present the searchable encryption schemes [22,26] shown in figure 8.

Vasudha Arora, S.S. Tyagi (2015) analyzes various SE schemes where the data owner is accountable for making his data secure. Order-preserving Encryption Scheme (OPE), Order-Preserving Mapping (OPM), Homomorphic encryption and Two Round Searchable Encryption (TRSE) schemes are discussed in detail. The proposed scheme does not leak any information and provides the original data to authorized users [24].

Cloud solved the problem of data storage and portability. However, most of the data is uploaded in the form of plaintext, which leads to more security and privacy risks. Lei Xu and Chungen Xu (2015) present a data retrieval system using a public key encryption system with keyword search.

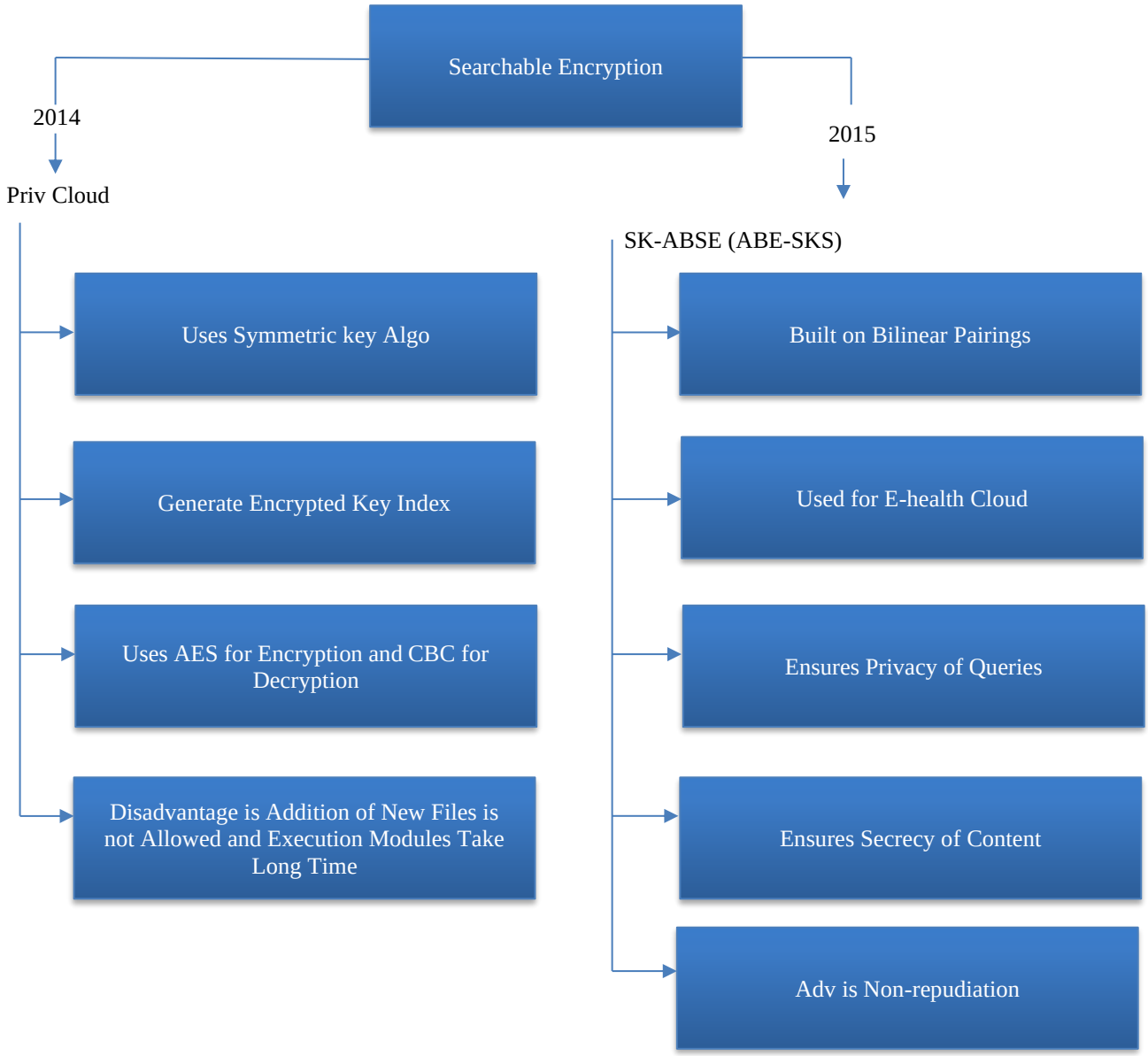


Fig. 8 Searchable encryption schemes in 2014 and 2015

To achieve a shorter key size scheme, they use asymmetric pairings. The dual system technique reduces it to decisional subspace assumptions to prove the scheme's security. The searchable encryption scheme is based on an identity-based encryption system, but an open challenge still exists [27].

C. Saranya, G.Radha, and R. Subash (2015) propose a searchable encryption scheme that includes new cryptography technologies, ECC and vector space model. While encrypting the searchable index data, the owner makes use of the kNN scheme. For the efficient top k retrieval, they use a multi-keyword ranked search. Two-round Searchable Encryption (TRSE) with top k retrieval is used, which is composed of a vector space model (for sufficient search accuracy) and homomorphic encryption (provides ranking criteria on the server side). For ranking the files so that most matched results can be retrieved, they use relevance scoring. Compare the precision, privacy and computation time results between Multi-keyword search with top k retrieval, SSE with multi-keyword retrieval and TRSE with top k retrieval. The scheme basically solves the problem of secure multi-keyword top-k retrieval over encrypted cloud data. A server-side ranking SSE scheme is introduced, which overcomes the information leakage problem of the OPE scheme. The scheme provides good efficiency and security [29].

Ashutosh Mishra, Velayutham. T M(SRS), Dr. C R S Kumar (2016) analyses the cloud computing security issues and challenges.

Table 7. Research gaps in encrypted data retrieval techniques over cloud

Technique	Aspects for Further Future Consideration
SSE	Security issue and computation cost.
Privacy-preserving Multi keyword ranked search (P) using k-Nearest Neighbor (k-NN)	Need for integrity checking of rank order in search results, Need to reduce computation and communication overhead and can be improved on security backgrounds.
Curtmola's SSE	Less efficient as it has a longer encryption time.
Multikey Fully Homorphic Encryption(MFHE)	It does not support multi-keyword search and ranking.
Multi Keyword Text Search (MUSE) using Hierarchical Agglomerative Clustering Tree (HAC-tree)	Less efficient as search time was large.
Ranked Searchable Encryption(RSE)	It does not support multi keyword search.
Hierarchical attribute-based encryption(HABE) with attribute-based retrieval feature (ARF) tree	Inflexible in assigning attributes to documents and can further be optimized to decrease the number of access trees.
Privacy-preserving data search scheme based on identifier-based Adleson-Veskii and Landis (ID-AVL) tree	Search efficiency can be improved and can be integrated with a data retrieval system with the ranking of results.
Tree-based ranked multi-keyword search with multiple data owners (TBMSM)	Needs improvement in search efficiency and minimization of storage space.
IDCrypt uses two-layer encryption scheme(TLES), i.e. identity-based encryption (IBE) and Public key encryption(PKE)	Needs improvement in security and technical issues.

They propose a solution to mitigate data retrieval and enhance data security against leakage. They use ENIGMA architecture for fast data retrieval and data confidentiality. AONT (all-or-nothing-transform) (AES- 256 BIT and LT encoding) is used for data encryption. The above two schemes provide fast data retrieval and better data availability and confidentiality. However, the fast data scanning through storage nodes also creates a bottleneck in data retrieval [42].

Tuhena Sen and Kumar Chaudhary (2017) discuss in detail the ranking algorithms that include Simples PageRank, HITS and Weighted PageRank Algorithms. Simple PageRank is based on link structure, mainly forward links. Weighted PageRank is based on a link approach and involves backward and forward links to rank the pages. HITS (Hypertext Induced Topic Search) uses authorities and hubs and works on content as well as the structure of the web.

All the above three algorithms have their own advantages and limitations, but Weighted PageRank and HITS outcomes better performance than Simple PageRank. However, getting appropriate results is challenging due to the involvement of fake sites. So, there is a need to improve the algorithms [47].

There has always been a tradeoff between storage and time to search for relevant data in the cloud environment. From the above table, it can be analyzed that to achieve efficient ranked data retrieval, there is still a need to develop a storage and time-efficient system. Also, security is another aspect that cannot be compromised in any case, as the data is in the hands of a third party, although trusted, but still lurking for an attacker.

4. Analysis of Futuristic Scope Based on Existing Studies

There is a need for a searchable algorithm with good efficiency for ranking; the searches must have various properties that provide result in ranked order of relevance and supports multiple keyword searches with quick response and with the minimum number of delays. With the above-mentioned properties, there is a need to propose a multiple-keyword ranked search scheme that also supports search results verification. Due to several gaps in searches, there is a wide scope of futuristic research:

4.1. Concise Indexes

Inappropriate accuracy of the schemes is a major drawback, and this leads to the main root cause for encryption being deflated as it was not at all done to improve the accuracy [28, 46].

Several indexing schemes, such as R-tree, Quard Tree, Octree, and Skip-Octree, are proposed to build an index over encrypted data. The index size is very important because it will be divided over multiple servers if it increases, so the index must be concise. Therefore, indexing leads to an issue of accessing indexes from multiple servers. [3]. The problem of tier structures of the data without analysing the requirement of structuring the form per particular application can be overcome by indexing RT-CAN and Portable data hiding technique, which are both multiple dimensional schemes. RT-CAN give a solution to the scalability of search nodes and minimum hops without taking into account the requirement and situational awareness of the deployment of required nodes.

A Portable data hiding technique provides a multidimensional 3-tier architecture without taking into account the situational requirement of the application, which can be understandable that different applications require different computing abilities, or this also means that different keywords require different amounts of complexity in search. So, a highly complex search structure is not required for the application that needs a less complex search structure [3]. RT-CAN works better than RT-HCN in the case when we increase the network scale as RT-HCN (hierarchical irregular compound network) is a two-layered architecture and uses an R tree-based indexing structure. It still brings space and query efficiency, and it deals with a limitation of scalability when the number of indices increases [83].

4.2. Consistent Indexes

The index should be consistent w.r.t updation because as both transactional and data analysis operations run simultaneously, there is a requirement to make better data query efficiency by increasing the data consistency. This will lead to a conflict between update and query, so this is also an issue in the cloud of index updation [43].

4.3. Secure Index

The concept of sub-index can be introduced to avoid leakage of search patterns and achieve strict indexing update security. Bucket locations can be randomized to achieve a higher level of security [21].

4.4. Sub Linear Search Time

Existing search schemes has a drawback in terms of accuracy and search time. Both the factors of accuracy and search need to work parallely and are only useful if the search takes less time. Implementation cost is also higher, and for successful implementation, that cost needs to be provided; if not, then for practical implications, the system is not suitable. So, there is a requirement to minimize the cost rather than reduce computing resources, such as minimum nodes. The computational cost, dependent on the number of documents and keyword dictionary size, also needs to improve. Moreover, computational costs include cryptographic operations, storing and retrieving index information, and file transfers over the network [28].

4.5. Security or Data Hiding

Collaboration of symmetric and asymmetric encryption provides good results for user data files and index files [31]. Data hiding and encryption services are mostly required for data security. SSE is compromised in the previous method as SSE is only for non-adaptive chosen-keyword attacks. By using general and inefficient techniques, it can support dynamic operations.

4.6. Multi-Keyword Search

In terms of elasticity and efficiency, both fuzzy and semantic-based search scheme fails, so there is a requirement for multiple keyword search technique [31].

4.7. Granting Authorized Access

Granting authorization access is the major key point to revoke the access of unauthorized users. There have been some worries about legitimate users' access, like being able to issue queries even using a resource-constrained device like a cell phone and query processing [23].

4.8. Ranking

While retrieving the documents in order of most relevant to least also involves issues relating to accurate retrieval per user expectations.

5. Results and Discussion

As discussed above, Cloud Computing is an interesting field with many possibilities for maintenance at the infrastructure and software layers. Two processes are associated with the storage architecture, namely the storage and the retrieval. The storage architecture plays a vital role in how fast the data is retrieved. The retrieved data is presented as per the weighted value.

The work presents a novel secure storage and ranking mechanism for the documents for the cloud. As no previous reference for any data is kept on the server, the data is encrypted based on the correlation between the data files calculated by Cosine similarity. The ranking of the retrieved data is done through a supervised machine-learning mechanism. The evaluation of the parameters is done on the base of computation time and the total number of true retrievals on multi-keyword search. Multiple Kaggle datasets are used to perform and cross-validate the proposed algorithm. The proposed solution is divided into two parts, namely storage and retrieval.

5.1. Storage

The set of documents T contains n*o data files. For the secure storage of T, a new encryption algorithm of three-level architecture A (A1, A2, A3) is used. An encryption selection algorithm is implemented to select the algorithm from set A cosine similarity is applied over T. Based on the cosine similarity of the data files at the time of storage. The average similarity index over the entire set of documents T is evaluated. For T having 5 documents, the complexity evaluator algorithm is applied, and the similarity index is calculated. Then, the encryption algorithm is applied to the document to ensure security.

Fig. 9 shows the various operations performed to encrypt the documents. It consists of uploading the documents, preprocessing the documents (removal of stop words and removal of case sensitivity), converting documents into feature vectors and finding cosine similarity between those vectors to find their complexity with respect to other documents in the database. Based on the complexity value, say R, the encryption algorithm is applied to the main document.

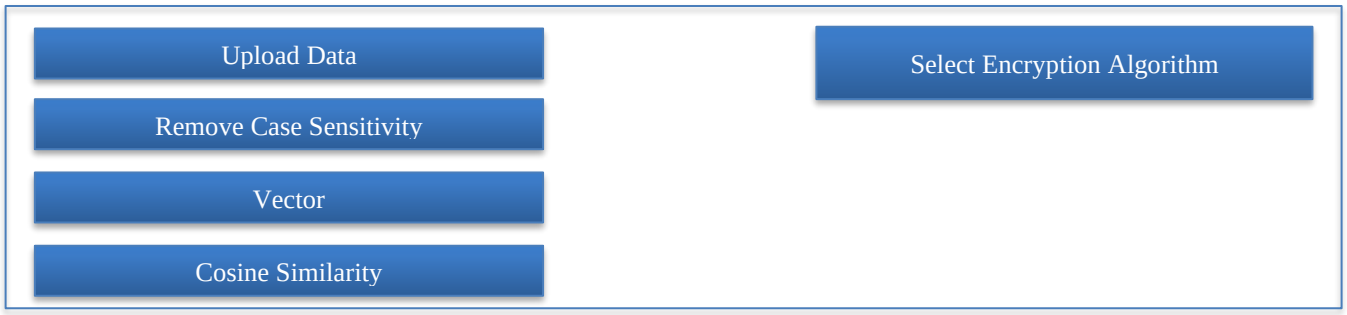


Fig. 9 Operations for encrypting documents

Fig. 10 shows the stop word removal process and case sensitivity removal process.

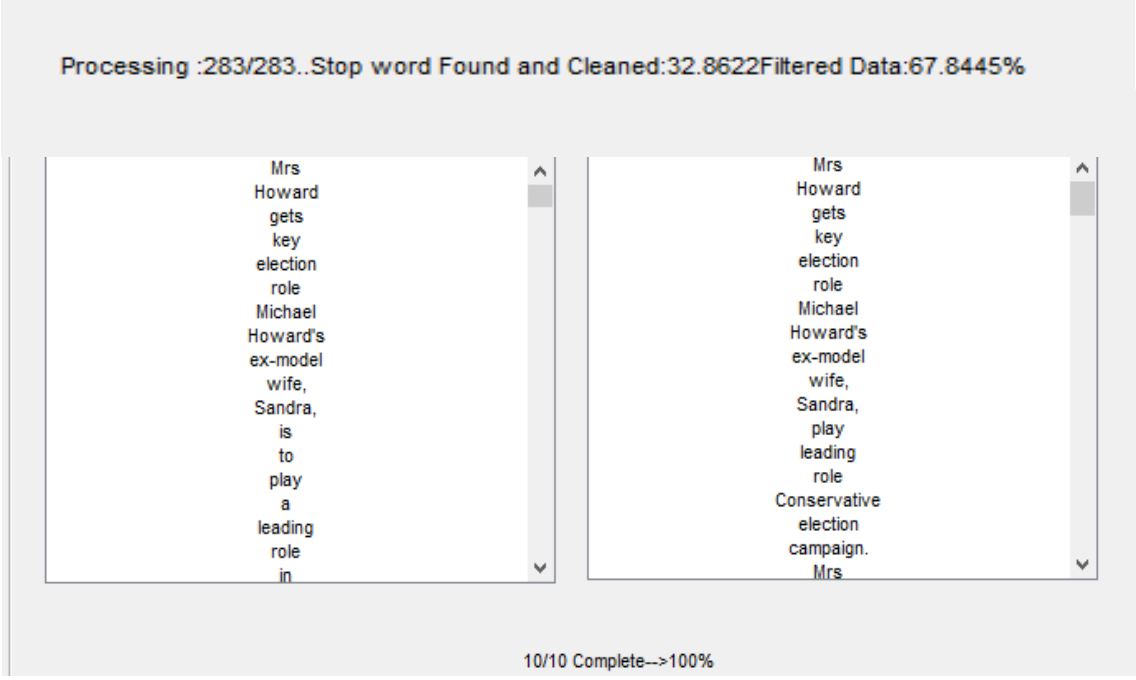


Fig. 10 Preprocessing text files

Fig. 11 shows the database screenshot. There are 2226 text files from online BBC news data.

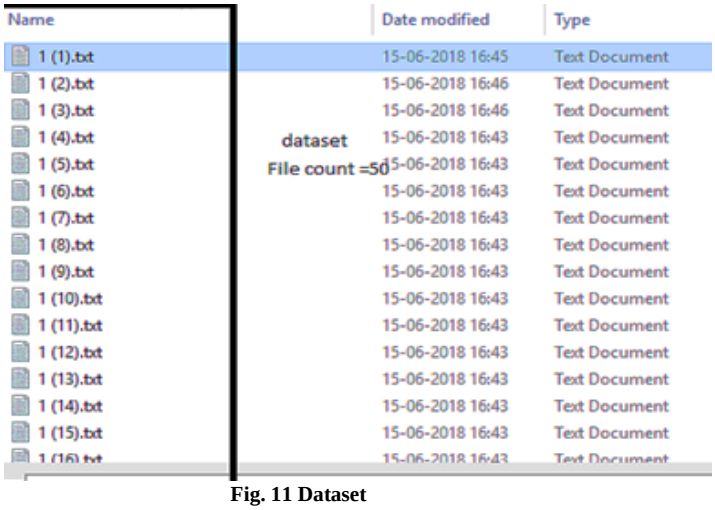
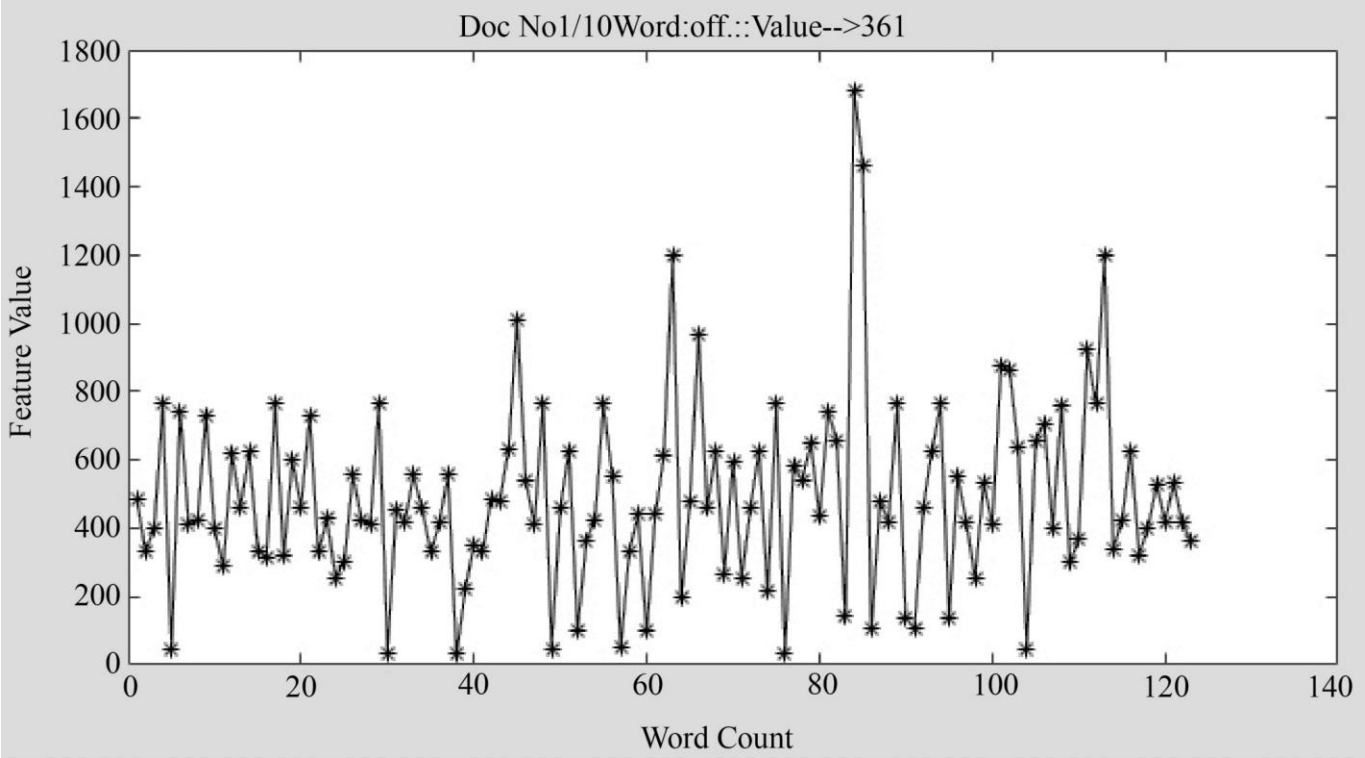
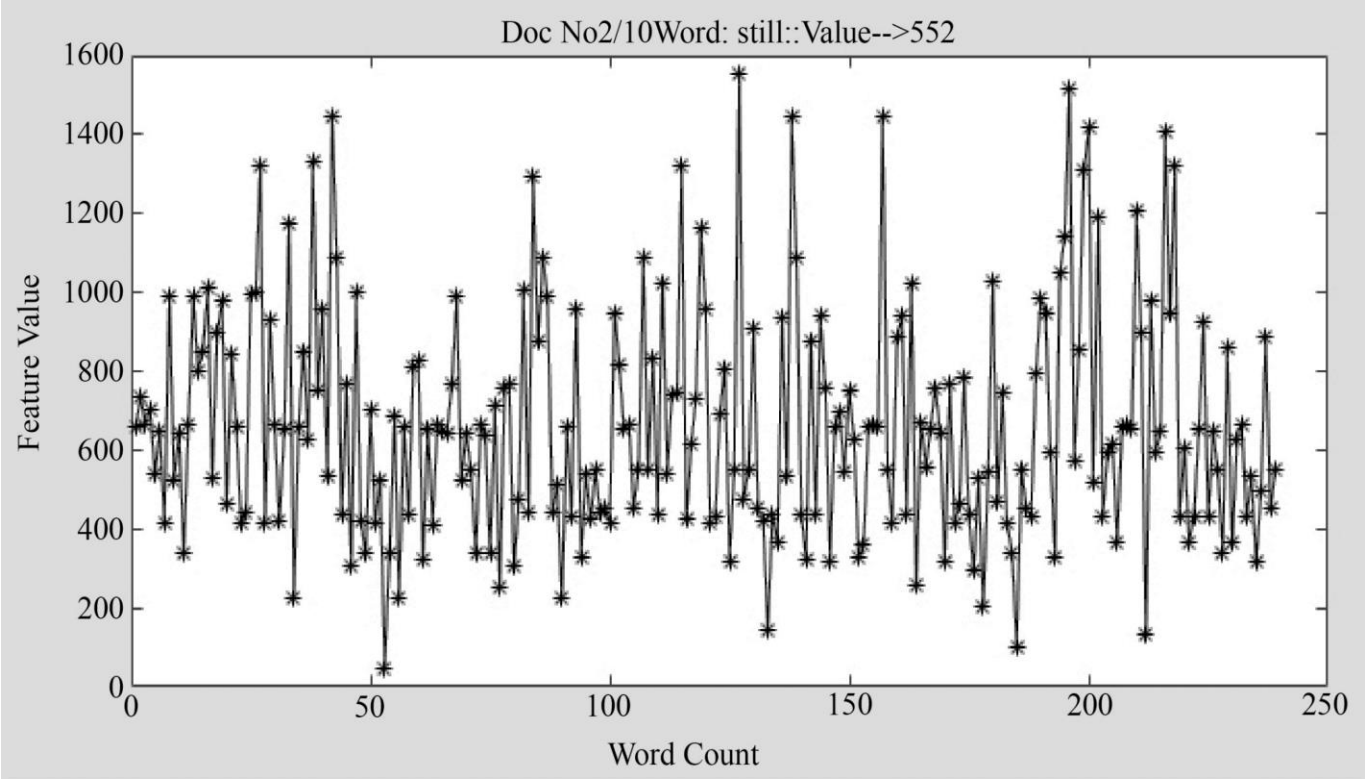


Fig. 11 Dataset

Figure 12 shows the process of converting each document word into a feature vector value. In Matlab, the generator function is used for converting text in the document to a feature vector.





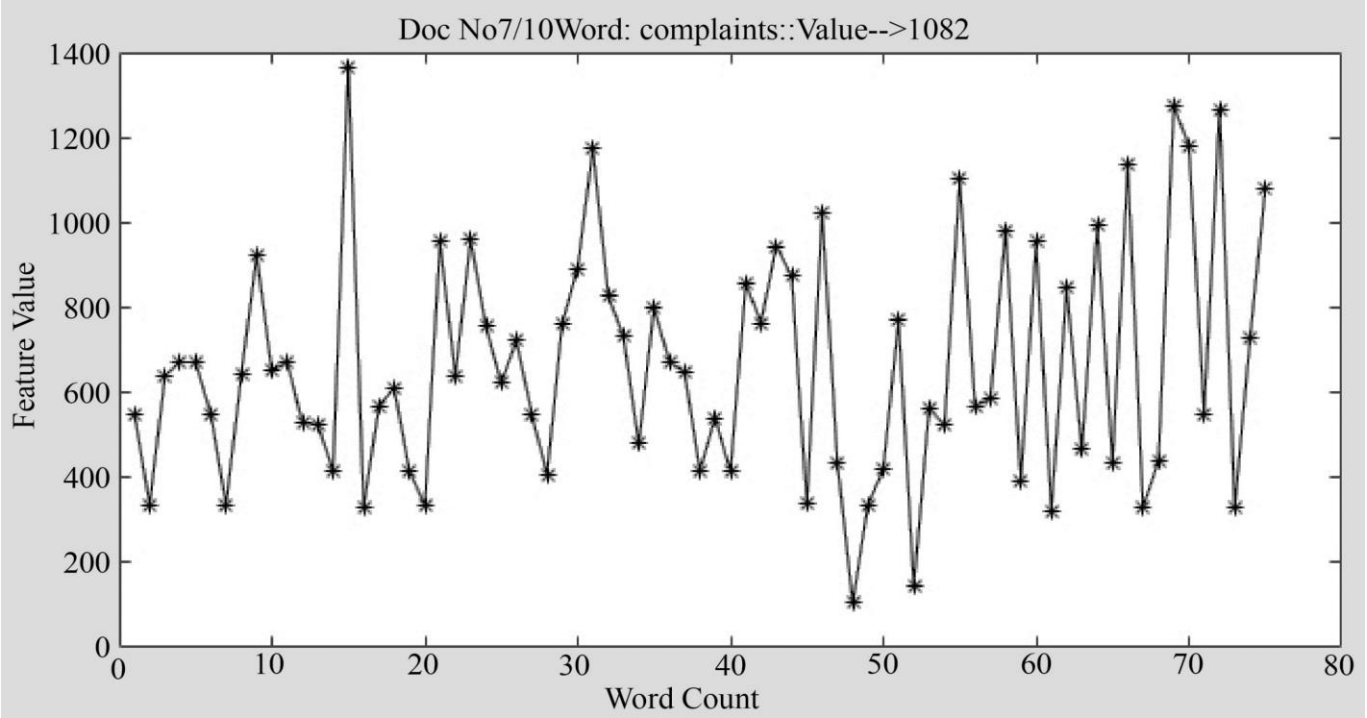


Fig. 12 Feature vectors

After finding the feature vector, the next step is to find the cosine similarity of each document within the documents stored in the database (Alewiwi, M., Orencik, C. and Savaş, E., 2015). It is calculated by the below-shown formula:

$$\cos\theta = \frac{A.B}{\text{mod A. modB}}$$

$$\cos\theta = \frac{\sum_{i=1}^{n}(A_i B_i)}{\sqrt{\sum_{i=1}^{n}(A_i^2)}\sqrt{\sum_{i=1}^{n}(B_i^2)}}$$

Where A and B are feature vectors, and $\cos\theta$ is the angle between A and B. Smaller the angle between A and B, the greater the similarity value and vice versa.

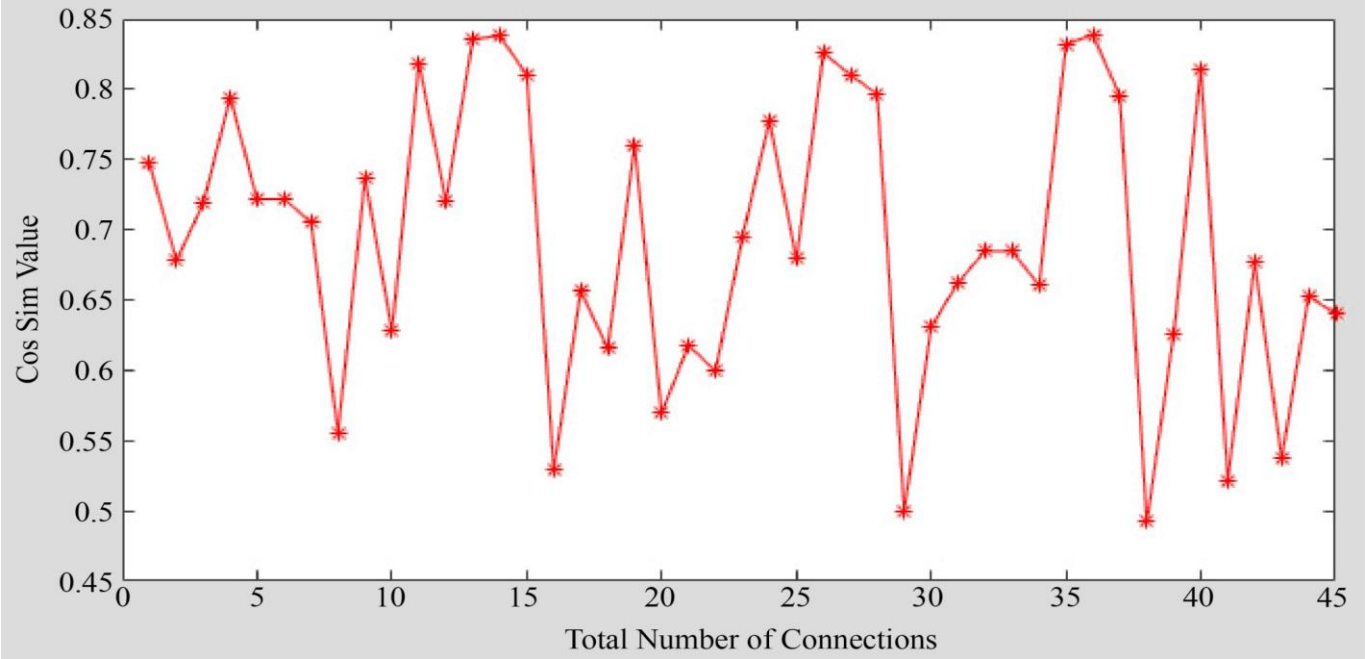


Fig. 13 Cosine similarity values

Fig. 13 shows the cosine similarity value of each document. The number of connections denotes the total number of comparisons. If there are n number of documents, then the number of connections will be $\frac{n(n-1)}{2}$. In the figure shown above, there are 10 total documents uploaded, so the number of connections is 45.

In order to select the best possible similarity value, the proposed work evaluated three different similarity measures, namely the Cosine similarity, Euclidean distance and the Jaccard Similarity. The best co-relation value is attained by the cosine similarity that can be viewed in Table 8 as follows.

The similarity measures demonstrate that the cosine similarity attains maximum value and is most suitable for the processing.

- Normalized Euclidean Distance: It measures the Euclidean distance between two vectors after normalizing them to have unit length. It ranges from 0 to 1, where 0 indicates identical documents, and 1 indicates completely dissimilar documents.
- Normalized Jaccard Similarity: It measures the similarity between two sets by taking the size of their intersection divided by the size of their union. It ranges from 0 to 1, where 0 indicates completely dissimilar documents, and 1 indicates identical documents.

Table 8. Comparison of similarity measures

Document Count	Cossim Values	Normalized Euclidean Distance	Normalized Jaccard Similarity
10	0.421	0.41392906	0.41285993
20	0.445	0.40716336	0.40265518
30	0.4567	0.45646042	0.44964952
40	0.4655	0.4491304	0.42939597
50	0.4789	0.45744601	0.42643305
60	0.47991	0.44758781	0.41385959
70	0.50112	0.47834007	0.44708133
80	0.50223	0.46144931	0.4285922
90	0.50446	0.48271227	0.44948679
100	0.501167	0.47026318	0.44435201

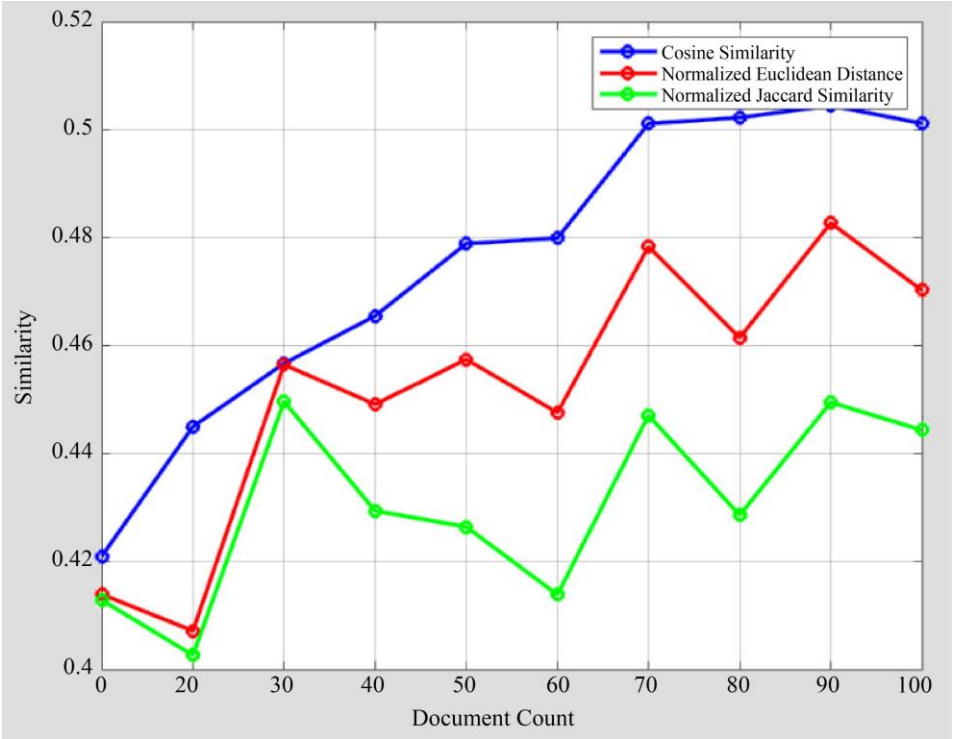


Fig. 14 Similarity measure comparison

The pseudocode of the cosine similarity function is a

```
function [simvalue] = cossim(A, B)
%COSSIM Summary of this function goes here
%   Detailed explanation goes here
a=numel(A);
b=numel(B);
if a==b
else
   if a>b
      df=a-b;
      B(b+1,b+df)=1;
   else
       df=b-a;
       A(a+1,a+df)=1;
   end
end
for i=1:numel(A)
  AB(i)=A(i)*B(i);

end
nume=sum(AB);
sum1=0;
for i=1:numel(A)
  sum1=sum1+A(i)^2;
end
sum2=0;
for j=1:numel(B)
  sum2=sum2+B(j)^2;
end
deno=sum1*sum2;
simvalue=nume/sqrt(deno);
```

Depending on the cosine similarity values, the encryption algorithm is applied. Let if the maximum similarity value is R, then 3 levels of encryption algorithms are considered based on ranges less than R/4, between R/4 and R/2, and between R/2 and R. If the range is less than R/4, then the RSA algorithm is applied. If the range is between R/4 and R/2, then AES is applied, as shown in fig. 14.

The pseudocode for encryption architecture is

```
load Similaritymeasure
encryptedfiles=[];
threshold=mean(connectionvalue(:,3));
range=[threshold/2 threshold];
[r,c]=size(connectionvalue);
for i=1:r-1
   [an,pos]=find(connectionvalue(:,1)==i);
   l1=mean(connectionvalue(pos,3));
   l1=mean(l1);
   l1=l1/(numel(pos)/2);
   if l1>range(1) &&  l1<range(2)
[s_box, inv_s_box, w, poly_mat, inv_poly_mat] = aes_init;
load lowereddata
ciphertext = cipher (plaintext, w, s_box, poly_mat, 1);
end
   elseif  l1>range(2)
plaintext=normaltext
p=59;
q=61;
M=plaintext;
[Pk,Phi,d,e] = intialize(p,q);
x=length(M);
c=0;
for j= 1:x
   for bi=0:122
      if strcmp(M(j),char(bi))
         c(j)=bi;
      else
         c(j)=M(j);
      end
   end
end
ciphertext=c;
encryptedfiles{i}=ciphertext;
```

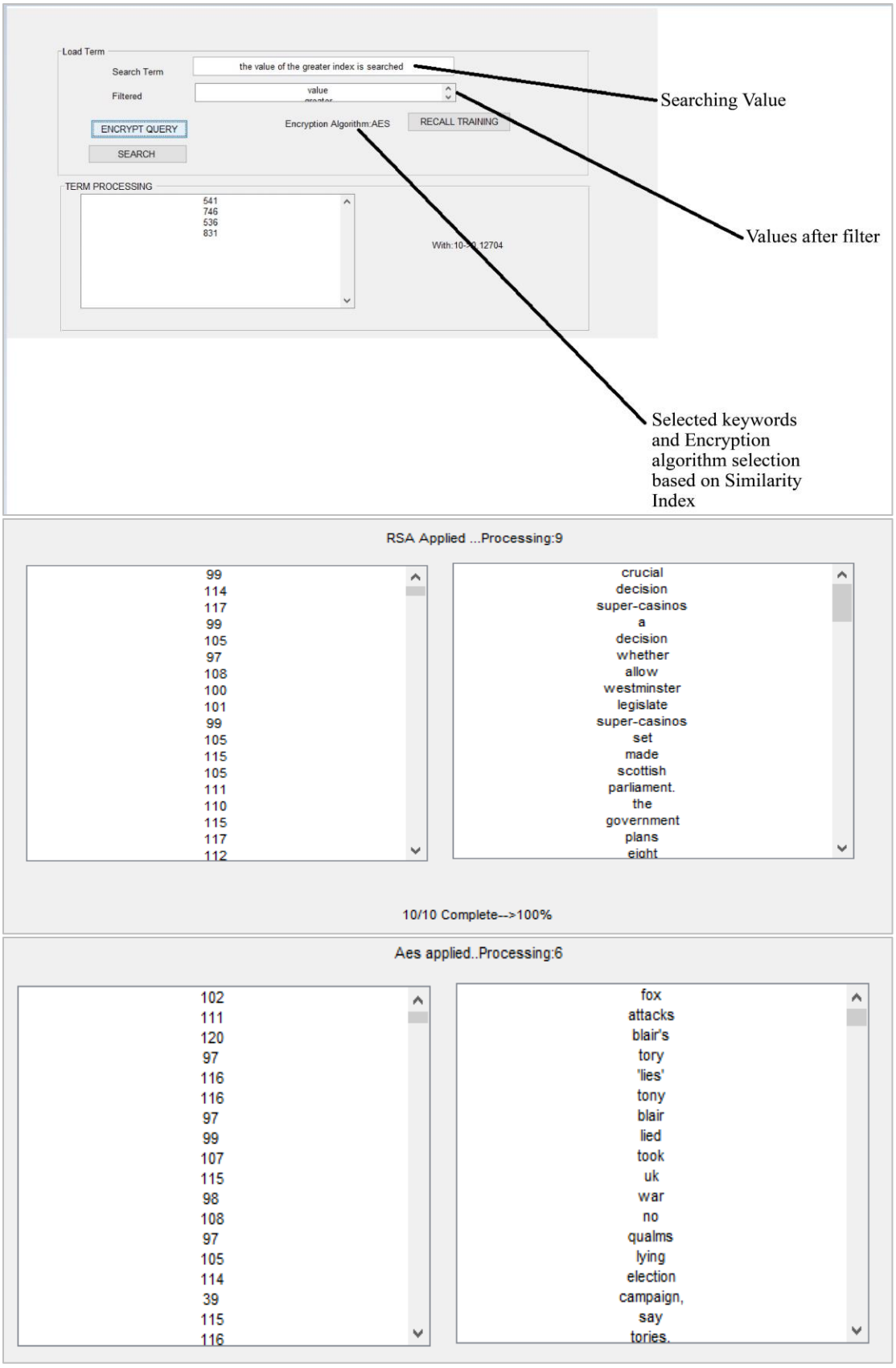


Fig. 15 Encryption algorithm

6. Conclusion

Cloud computing is a widely used platform in many applications, and it is growing very rapidly. Users store their data on the cloud in an encrypted form so that an unauthorized user cannot access it and can be protected from other well-known attacks. Various schemes and approaches are implemented over the cloud for protecting data and retrieving the most relevant documents. The paper discusses various existing schemes that are used for data retrieval over the cloud. Some provide advantages over the other and overcomes the drawbacks of existing study. But still, there exist issues related to security, user privacy, efficient retrieval of files, authorization, and many more need to be resolved so that users can securely store and retrieve their data from the cloud without compromising these issues.

Working on a cloud has always been a challenging task because the data is outsourced to a third party, which is a great risk in terms of security (encryption), and again, the retrieval of data from a third party imposes various challenges in terms of indexing, searching and ranking. Literature survey states various techniques that begin with a single keyword search but lack ranking of relevant documents. With limited efficiency, a ranked-based multiple-keyword search was introduced. Then, several user search schemes were developed using fuzzy and semantic search. In terms of user experience, all these schemes need improvement. So, there is a requirement for such an efficient multiple keyword-based encrypted index search scheme. This must include a better encryption algorithm for enhanced encrypted index search technique, encrypting documents and index, secure retrieval of documents and ranking of documents according to relevance order. The EFS basically refers to as Encrypted File System. This encrypts storage files, but until the encryption keys are secure, this system prevents information leakage. These EFS services were built only for local hard discs. Implementing such systems to remote and cloud storage needs enhancements and revisions. The paper has focussed on the secure encryption scheme that uses three encryption algorithms instead of a single algorithm. The application of cosine similarity in cloud data and index encryption has provided novelty towards secure ranked retrieval of cloud data.

Accuracy, time efficiency along with, accessibility and security are the major key points that need to be considered in the retrieval of data in an encrypted search. These research gaps highlight the important concern points that led to previous studies of encrypted search schemes. Only authorized users can access the data, which means the security of the user data must be maintained. By providing secure access, the system performance in terms of accuracy and efficiency should not degrade. The main factors that must be considered importantly are security, accessibility, search time, and data accuracy, which must work synchronically.

References

[1] Lucas Ballard, SenyKamara, and Fabian Monrose, "Achieving Efficient Conjunctive Keyword Searches Over Encrypted Data," *International Conference on Information and Communications Security*, vol. 3783, pp. 414-426, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[2] Cong Wang et al., "Secure Ranked Keyword Search over Encrypted Cloud Data," *IEEE 30th International Conference on Distributed Computing Systems*, pp. 253-262, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jinbao Wang et al., "Indexing Multi-Dimensional Data in a Cloud System," *Proceedings of the International Conference on Management of Data*, pp. 591-602, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[4] Anna Squicciarini, Smitha Sundareswaran, and Dan Lin, "Preventing Information Leakage from Indexing in the Cloud," *IEEE 3rd International Conference on Cloud Computing*, pp. 188-195, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mariana Raykova et al., "Usable, Secure, In: Private Search," *IEEE Security and Privacy*, vol. 10, no. 5, pp. 53-60, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[6] Seny Kamara, Charalampos Papamanthou, and Tom Roeder, "Dynamic Searchable Symmetric Encryption," *ACM Conference on Computer and Communications Security*, vol. 19, no. 5, pp. 965-976, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[7] Cengiz Örencik, and Erkay Savaş, "Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data," *Proceedings of the 2012 Joint EDBT/ICDT Workshops, ACM*, pp. 186-195, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[8] Cong Wang et al., "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1467-1479, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sandeep K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831-1838, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jyun-Yao Huang, and I-En Liao, "A Searchable Encryption Scheme for Outsourcing Cloud Storage," *IEEE International Conference on Communication, Networks and Satellite*, pp. 142-146, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[11] Dongyoung Koo, Junbeom Hur, and Hyunsoo Yoon, "Secure and Efficient Data Retrieval over Encrypted Data Using Attribute-Based Encryption in Cloud Storage," *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 34-46, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[12] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231-240, 2013. [Google Scholar] [Publisher Link]

[13] Mohsen Bafandehkar et al., "Comparison of ECC and RSA Algorithms in Resource Constrained Devices," *IEEE International Conference on IT Convergence and Security*, pp. 1-3, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Zhangjie Fu et al., "Multi-Keyword Ranked Search Supporting Synonym Query Over Encrypted Data in Cloud Computing," *IEEE 32nd International Performance Computing and Communications Conference*, pp. 1-8, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[15] Wang Jianfeng et al., "Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 667-684, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohsen Bafandehkar et al., "Comparison of ECC and RSA Algorithm in Resource Constrained Devices," *IEEE International Conference on IT Convergence and Security*, pp. 1-3, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[17] Wenhai Sun et al., "Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking," *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, pp. 71-82, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zhihua Xia et al., "An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data," *Advanced Science and Technology Letters*, vol. 31, pp. 323-332, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ning Cao et al., "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222-233, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[20] Vishwanath S Mahalle, and Aniket K Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm," *International Conference on Power Automation and Communication*, pp. 146-149, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[21] Fangquan Cheng et al., "Highly Efficient Indexing for Privacy-Preserving Multi-Keyword Query Over Encrypted Cloud Data," *International Conference on Web-Age Information Management*, pp. 348-359, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[22] MdIftekhar Salam et al., "Implementation of Searchable Symmetric Encryption for Privacy-Preserving Keyword Search on Cloud Storage," *Journal of Human-Centric Computing and Information Sciences, Springer*, vol. 5, no. 19, pp. 1-16, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[23] Bharath Kumar Samanthula, Wei Jiang, and Elisa Bertino, "Privacy-Preserving Complex Query Evaluation over Semantically Secure Encrypted Data," *European Symposium on Research in Computer Security*, vol. 8712, pp. 400-418, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[24] Vasudha Arora, and S.S. Tyagi, "Analysis of Symmetric Searchable Encryption and Data Retrieval in Cloud Computing," *International Journal of Computer Applications*, vol. 127, no. 12, pp. 46-51, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[25] Zhangjie Fu et al., "Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search Over Encrypted Cloud Data Supporting Parallel Computing," *IEICE Transactions on Communications*, vol. 98, no. 1, pp. 190-200, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[26] Yang Yang, "Attribute-Based Data Retrieval with Semantic Keyword Search for E-Health Cloud," *Journal of Cloud Computing*, vol. 4, no. 10, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[27] Lei Xu, and Chungen Xu, "Efficient and Secure Data Retrieval Scheme Using Searchable Encryption in Cloud Storage," *International Symposium on Security and Privacy in Social Networks and Big Data*, pp. 15-21, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[28] Hongwei Li et al., "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 127-138, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[29] C. Saranya, G. Radha, and R. Subash, "Top K Result Retrieval in Searching the File Over the Encrypted Data in Cloud," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 3, pp. 2226-2233, 2015. [CrossRef] [Publisher Link]

[30] Amrithasree Haridas, and L. Preethi, "A Survey on Data Retrieval Techniques over Encrypted Cloud Storage," *Second International Conference on Networks and Advances in Computational Technologies*, pp. 117-129, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] Sneha A. Mittal, and C. Rama Krishna, "Recent Developments in Searching over Encrypted Cloud Data," *5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, pp. 338-342, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[32] Fei Han, Jing Qin, and Jiankun Hu, "Secure Searches in the Cloud: A Survey," *Journal of Future Generation Computer Systems*, vol. 62, pp. 66-75, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[33] K. Sekar, and M. Padmavathamma, "Comparative Study of Encryption Algorithm Over Big Data in Cloud Systems," *3rd International Conference on Computing for Sustainable Global Development*, pp. 1571-1574, 2016. [Google Scholar] [Publisher Link]

[34] U. Arjun, and S. Vinay, "A Short Review on Data Security and Privacy Issues in Cloud Computing," *International Conference on Current Trends in Advanced Computing*, pp. 1-5, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[35] Jian Liu, Jing-Li Han, and Zhao-Li Wang, "Searchable Encryption Scheme on the Cloud via Fully Homomorphic Encryption," *IEEE Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC),* pp. 108-111, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[36] Abdelali El Bouchti, Samir Bahsani, and Tarik Nahhal, "Encryption as a Service for Data Healthcare Cloud Security," *IEEE Fifth International Conference on Future Generation Communication Technologies,* pp. 48-54, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[37] G. PrabuKanna, and V. Vasudevan, "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud," *IEEE International Conference on Electrical, Electronics, and Optimization Techniques,* pp. 3688-3693, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[38] Anuradha Meharwade, and G.A. Patil, "Efficient Keyword Search over Encrypted Cloud Data," *Procedia Computer Science*, vol. 78, pp. 139-145, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[39] Xin Zhou, Jun Zhang, and GuanYu Li, "Efficient Interval Indexing and Searching on Cloud," *International Conference on Web-Age Information Management*, pp. 283-291, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[40] S. Sridhar, and S. Smys, "A Hybrid Multilevel Authentication Scheme for Private Cloud Environment," *IEEE 10th International Conference on Intelligent Systems and Control,* pp. 1-5, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[41] Chengliang Liang et al., "The Hybrid Encryption Algorithm of Lightweight Data in Cloud Storage," *IEEE 2nd International Symposium on Agent, Multi-Agent Systems and Robotics,* pp. 160-166, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[42] Ashutosh Mishra, T.M. Velayutham, and C.R.S. Kumar, "Fast Data Retrieval and Enhanced Data Security of Cloud Storage in Luby Transform," *Procedia Computer Science*, vol. 85, pp. 86-91, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[43] Jing He et al., "Dynamic Multidimensional Index for Large-Scale Cloud Data," *Journal of Cloud Computing*, vol. 5, no. 10, pp. 1-11, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[44] Zuojie Deng et al., "A Multi-User Searchable Encryption Scheme with Keyword Authorization in a Cloud Storage," *Future Generation Computer Systems*, vol. 72, pp. 208-218, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[45] Xiuxiu Jiang et al., "Enabling Efficient and Verifiable Multi-Keyword Ranked Search over Encrypted Cloud Data," *Information Sciences*, vol. 403, pp. 22-41, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[46] Zhu Xiangyang et al., "An Efficient and Accurate Verifiable Privacy-Preserving Multi Keyword Text Search over Encrypted Cloud Data," *Security and Communication Networks*, vol. 2017, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[47] Tuhena Sen, and Dev Kumar Chaudhary, "Contrastive Study of Simple Page Rank, HITS and Weighted PageRank Algorithms: Review," *IEEE 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence,* pp. 721-727, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[48] Shahzaib Tahir et al., "A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 4, pp. 530-544, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[49] Nan Zhu et al., "A Content-based Indexing Scheme for Large-Scale Unstructured Data," *Third International Conference on Multimedia Big Data*, pp. 205-212, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[50] Justin Zobel, and Alistair Moffat, "Exploring the Similarity Space," *ACM SIGIR Forum*, vol. 32, no. 1, pp. 18–34, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[51] Sanjana M. Kavatagi, and Rashmi Rachh, "Implementation of Searchable Encryption using Key Aggregation for Group Data Sharing in Cloud," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 8, pp. 11-14,2017. [CrossRef] [Google Scholar] [Publisher Link]

[52] Eu-Jin Goh, "Secure Indexes," *IACR Cryptology ePrint Archive*, 2003. [Google Scholar] [Publisher Link]

[53] Yan-Cheng Chang, and Michael Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," *Applied Cryptography and Network Security*, pp. 442–455, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[54] J. Doug Tygar, Security with Privacy, ISAT 2002 Study, 2002. [Online]. Available: https://people.eecs.berkeley.edu/~tygar/papers/ISAT-final-briefing.pdf

[55] Dan Boneh et al., "Public Key Encryption that Allows PIR Queries," *Advances in Cryptology-CRYPTO*, pp. 50–67, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[56] R. Ostrovsky, "Efficient Computation on Oblivious RAMs," *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*, pp. 514–523, 1990. [CrossRef] [Google Scholar] [Publisher Link]]

[57] Oded Goldreich, and Rafail Ostrovsky, "Software Protection and Simulation on Oblivious RAMs," *Journal of the ACM*, vol. 43, no. 3, pp. 431–473, 1996. [CrossRef] [Google Scholar] [Publisher Link]

[58] Chih Hung Wang, and Chia-Chun Hsu, "Integration of Hierarchical Access Control and Keyword Search Encryption in Cloud Computing Environment," *International Journal of Computer and Communication Engineering*, vol. 3, no. 2, pp. 33–337, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[59] Qin Liu, Guojun Wang, and Jie Wu, "An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing," *Proceedings of the International Conference on Computational Science and Engineering*, pp. 715–720, 2009.[CrossRef] [Google Scholar] [Publisher Link]

[60] Dan Boneh, and Matt Franklin, "Identity-based Encryption from the Weil Pairing," *Proceedings of the Advances in Cryptology—CRYPTO 2001*, vol. 2139, pp. 213–229, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[61] Zheng Tao Jiang, and Ling Liu, "Secure Cloud Storage Service with an Efficient DOKS Protocol," *Proceedings of the IEEE International Conference on Services Computing*, pp. 208–215, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[62] Sushil Kumar Verma et al., "An Efficient Dictionary and Lingual Keyword based Secure Search Scheme in Cloud Storage," *International Journal of Computer Applications*, vol. 68, no. 15, pp. 40–43, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[63] Yanbin Lu, "Privacy-Preserving Logarithmic-Time Search on Encrypted Data in Cloud," *19th Annual Network and Distributed System Security Symposium*, 2012.[Google Scholar] [Publisher Link]

[64] Zhihua Xia et al., "A Similarity Search Scheme over Encrypted Cloud Images based on Secure Transformation," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 6, pp. 71–80, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[65] X. Pang et al., "Multi-user Noisy Keyword Search over Encrypted Data," *Journal of Computational Information Systems*, vol. 9, no. 5, pp. 1973–1981, 2013. [Google Scholar] [Publisher Link]

[66] Michel Abdalla et al., "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," *Advances in Cryptology–CRYPTO*, pp. 205–222, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[67] Guofeng Wang et al., "IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications," *IEEE Access*, vol. 6, pp. 2908-2921, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[68] Yingfan Liu et al., "An Efficient Index Structure for Approximate Nearest Neighbor Search," *Proceedings of the VLDB Endowment*, vol. 7, no. 9, pp. 745–756, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[69] Yufei Tao et al., "Quality and Efficiency in High Dimensional Nearest Neighbor Search," *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 563-576, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[70] Nan Zhu et al., "Marlin: Taming the Big Streaming Data in Large Scale Video Similarity Search," *IEEE International Conference on Big Data*, pp. 1755-1764, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[71] Mathias Björkqvist et al., "Minimizing Retrieval Latency for Content Cloud," *Proceedings IEEE INFOCOM*, pp. 1080-1088, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[72] Yingfan Liu et al., "An Efficient Index Structure for Approximate Nearest Neighbor Search," *Proceedings of the VLDB Endowment*, vol. 7, no. 9, pp.745–756, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[73] Srinivas Mudepalli, V. Srinivasa Rao, and R. Kiran Kumar, "An Efficient Data Retrieval Approach using Blowfish Encryption on Cloud Ciphertext Retrieval in Cloud Computing," *International Conference on Intelligent Computing and Control Systems*, pp. 267-271, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[74] AL-Museelem Waleed, and Li Chunlin, "User Privacy and Security in Cloud Computing," *International Journal of Security, and Its Applications*, vol. 10, no. 2, pp. 341-352, 2016. [CrossRef] [Publisher Link]

[75] K. Satyanarayana, "Multilevel Security for Cloud Storage using Encryption Algorithms," *International Journal of Engineering and Computer Science*, vol. 5, no. 7, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[76] Maryam Savari, Mohammad Montazerolzohour, and Yeoh Eng Thiam, "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application," *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic*, pp. 49-53, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[77] Ahmed El-Yahyaoui, and Mohamed DafrEch-Chrif El Kettani, "A New Cryptographic Method for Cloud Computing," *3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, pp. 1-8, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[78] Chaoqun Yu et al., "Research on Data Security Issues of Cloud Computing," *International Conference on Cyberspace Technology*, pp. 1-6, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[79] Zhen Yang, Jiliang Tang, and Huan Liu, "Cloud Information Retrieval: Model Description and Scheme Design," *IEEE Access*, vol. 6, pp. 15420-15430, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[80] Junjian Chen, "Cloud Storage Third-Party Data Security Scheme Based on Fully Homomorphic Encryption," *International Conference on Network and Information Systems for Computers*, pp. 155-159, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[81] Xingliang Yuan et al., "Enabling Secure and Fast Indexing for Privacy-Assured Healthcare Monitoring Via Compressive Sensing," *IEEE Transactions on Multimedia*, vol. 8, no. 10, pp. 2002-2014, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[82] Xiaoyu Li et al., "Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems," *IEEE Access*, vol. 5, pp. 393-405, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[83] Yang Hong et al., "Efficient R-Tree Based Indexing Scheme for Server-Centric Cloud Storage System," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 6, pp. 1503-1517, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[84] Ashok George, and A. Sumathi, "Efficient Data Storage and Retrieval in Cloud Environment Using Cuckoo Hashing and Latent Semantic Search," *Middle-East Journal of Scientific Research*, vol. 23, no. 6, pp. 1053-1058, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[85] Wei Teng et al., "Attribute-Based Access Control with Constant-Size Ciphertext in Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 4, pp. 617-627, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[86] R.W. Conway, W.L. Maxwell, and H.L. Morgan, "On the Implementation of Security Measures in Information Systems," *Communications of the ACM*, vol. 15, no. 4, pp. 211-220, 1972. [CrossRef] [Google Scholar] [Publisher Link]

[87] Dorothy E. Denning, "A Lattice Model of Secure Information Flow," *Communications of the ACM*, vol. 19, no. 5, pp. 236-243, 1976. [CrossRef] [Google Scholar] [Publisher Link]

[88] Bell D. Elliott, La Padula, and J. Leonard, "Secure Computer System: Unified Exposition and Multics Interpretation," *Defense Technical Information Center*, 1976. [CrossRef] [Google Scholar] [Publisher Link]

[89] K.J. Biba, "Integrity Considerations for Secure Computer Systems," *Defense Technical Information Center*, 1977. [Publisher Link]

[90] Kaiping Xue et al., "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062-2074, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[91] Ilya Sukhodolskiy, and Sergey Zapechnikov, "A Blockchain-Based Access Control System for Cloud Storage," *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, pp. 1575-1578, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[92] Amlan Jyoti Choudhury et al., "A Strong User Authentication Framework for Cloud Computing," *IEEE Asia-Pacific Services Computing Conference*, pp. 110-115, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[93] Adam Bates et al., "Towards Secure Provenance-Based Access Control in Cloud Environments," *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, pp. 277-284, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[94] Dan Boneh et al., "Public Key Encryption with Keyword Search," *International Conference on the Theory and Applications of Cryptographic Techniques*,"pp. 506-522, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[95] Rouzbeh Behnia, Attila Altay Yavuz, and Muslum Ozgur Ozmen, "High-Speed High-Security Public Key Encryption with Keyword Search," *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 365-385, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[96] Zhangjie Fu et al., "Semantic Keyword Search Based on Trie over Encrypted Cloud Data," *Proceedings of the 2nd International Workshop on Security in Cloud Computing*, pp. 59–62, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[97] Saripalli Vinod Manikanta, and Kondapalli Varaprasad, "A Secure Privacy Preserving Information Retrieval Model in Cloud Computing," *International Journal of Computer and Organization Trends*, vol. 9, no. 1, pp. 16-19, 2019. [Publisher Link]

[98] Jihoon Ko et al., "Keyword Based Semantic Search for Mobile Data," *IEEE 15th International Conference on Mobile Data Management*, pp. 245–248, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[99] R. ChinnaSamy, and S. Sujatha, "An Efficient Semantic Secure Keyword Based Search Scheme in Cloud Storage Services," *International Conference on Recent Trends in Information Technology*, pp. 488–491, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[100] Ping Li et al., "Privacy-Preserving Outsourced Classification in Cloud Computing," *Cluster Computing*, vol. 21, pp.277-286, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[101] M.B. Smithamol, and Rajeswari Sridhar, "PECS: Privacy Enhanced Conjunctive Search Over Encrypted Data in the Cloud Supporting Parallel Search," *Computer Communications*, vol. 126, pp. 50–63, 2018. [CrossRef] [Google Scholar] [Publisher Link]