IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

A Survey on Efficient and Secure Techniques for Storing Sensitive Data on Cloud

Supriya J.[1], Srusti K.S.[2], Gamana G[3], S. Sukhaniya Ragani[4], Raghavendra S.[5*], Venugopal K.R.[6]

[1,2,3,4,5]Dept. of Computer Science and Engineering, Vivekananda College of Engineering and Technology, Puttur, India
[6]Bangalore University, Bangalore, India

**Corresponding Author: raghush86@gmail.com, Tel.: +91 9591276777*

DOI: https://doi.org/10.26438/ijcse/v7i5.17661777 | Available online at: www.ijcseonline.org

Accepted: 21/May/2019, Published: 31/May/2019

Abstract**—** Cloud computing, being the most recent emerging paradigm, is a technological advancement that aims at turning the vision of computing utilities into a reality. Simply, it is an approach of making technology available to the users, by the usage of Internet servers for data storage and processing. More specifically, cloud computing offers users benefits such as scalability, availability, reliability and global accessibility. Being a radical mechanism, the major obstacles for massive adoption of cloud computing are security, trust and privacy issues. With some defensive procedures like using a combination of methods that include encryption, authentication, and authorization, users are still concerned about the risks associated with their stored data. In this survey, many efficient and secured claiming techniques are investigated for end users to access the data stored in the cloud. The focus is here much on securing the data residing in cloud and privacy in accessing them. The study will throw lights upon keyword search, indexing, file splitting, encryption, and multi-cloud. Further, various methodologies in the existing system and performance of algorithms together with their pros and cons are discussed. Also, cloud security challenges, privacy and communication issues are considered and addressed here.

Keywords**—** Keyword Search, Secure Data, Data Privacy, Cloud Computing, Splitting Techniques, Encryption.

I. Introduction

Cloud computing is one of the biggest utility resources that will make life even easier than it is in the present day concerning Information technology. It aims at facilitating IT as a service to the user's on-demand basis with greater availability, scalability, flexibility, and reliability in the cloud. It is now a challenging opportunity for big online businesses to implement cloud computing technologies in their corporate to raise the value of work and drop the production cost. Now people don't need a greater hard disk drive, memory card in their devices like mobile and computers. They can save data straightaway on the cloud with the service of the internet and later, can access and share data and information with greater speed and accuracy. A new world of openings for businesses has been opened up, but varied with these opportunities are the number of security challenges that have to be essentially considered and addressed before obligating to a cloud computing strategy. Hence, data security serves as one important aspect to look into as we see in [1], [2] and [3].

Data and computation integrity together with security are the key concerns for users of cloud computing services. Data Protection is effecting a cloud computing strategy by placing sensitive data in the hands of a third party, by this means ensuring that the data remains protected both at rest as well as when in transit which is of utmost importance [4]. Data requires to be encrypted at all times. Generally, for the client to own and manage the data encryption key is the only approach to truly certify confidentiality of encrypted data that exists on a cloud provider's storage servers. [5]. As soon as the encryption is complete, the next is about the access to data stored in the cloud. The data residing in the cloud should be made accessible only to those who are authorized, making it critical to both monitor and restrict who will be accessing the firm's data through the cloud. The companies should be able to view data access audit trails and logs to confirm that only authorized users are accessing the data, which intents ensuring the integrity of user authentication [6]. Counting some key security advantages, there are some if not more security challenges that prevent clients from committing to a cloud computing technique, even though there are some real benefits of using cloud computing. Restricting and monitoring access to that data through user authentication and access logging, and effectively planning for the true possibilities of inaccessible or compromised data due to the natural disasters or data breaches, are all the significant security challenges that a business needs to address when making an allowance for cloud computing providers.

Further, we are presenting a secure and dynamic approach that is, the splitting techniques, to prevent the attacks that occur on the cloud data. One of the methods for securing data over a computer network is through data splitting. This approach includes splitting the data into smaller units, encrypting it, and allocating those smaller units to various storage locations. The data is secured from security breaches with this process. Since it is combined with decrypted data components from various other locations, even if an intruder is successful to retrieve and decrypt a single data unit, the information would be useless.

For the user to easily access the required files from the storage, indexing the fragmented files helps. The process of indexing is performed along with encrypting file fragments, then uploading to the assigned clouds [7]. A multi-cloud server consists of encrypted file fragments and the index file, and it generates trapdoor to access index files from the cloud. The level of sensitivity of the data being hosted and the cloud encryption capabilities of the service provider is to be matched. An authorized user can process keyword search over encrypted cloud data, once the data is stored on multi-clouds. To address the problem of secure search functions over encrypted data, various schemes with similarity-based ranking are presented [8]. The data user submits the search query. The user can enter the multiple words query, based on which the server will split that query into a single word after which, search that word file in the database. Lastly, the matched word list from the database is displayed and the user gets the file from that list. The multi-keyword retrieval over the outsourced data is processed by the authorized data user. The cloud server searches the index file and returns the top-k search results. The user selects a file from the top-k results and the selected file will be decrypted and merged into a single file that will be retrieved by the data user. Hence, secure stored data is easily accessed from the multi-clouds. Here, we investigate a few privacy acts to demonstrate that they are outdated.

The contributions of cloud computing have been increased recently in the technological development phase. The effects are reflected in many fields since flexibility, efficiency and strategic value stands as major benefits. Concentrating more on significant prevailing issues here, the contributions to the study has been made:

1. The efficient and various techniques of keyword search are presented.
2. An emerging concept, multi-cloud has given thoughts on its applications.
3. Securing the cloud data by the process of encryption, implemented through various algorithms.
4. The indexing concepts.

Chuang et al., [12] states a new method called Effective Privacy Protection Scheme (EPPS) which aims at providing

5. Comparison of different models.

The organization of the paper is as follows, Section I contains the introduction to the Cloud Computing and fundamentals on basic concepts involved, Section II contains the related work carried out so far, Section III contains the conclusion and future work to be carried out.

II. Related Work

Kawser et al., [9] have proposed security design for cloud computing platforms, ensuring the secure communication system. In this model, to exchange information or data, AES based file encryption system and asynchronous key system is included. For the user authentication process, the one-time password system has been involved, where the security system of the whole cloud computing platform is dealt with. The deterministic RSA encryption system has been used which makes the model fragile in the long run process. The arrangement can be effortlessly implemented with main cloud computing structures.

Jin et al., [10] while maintaining keyword privacy, has explained the problematic effective fuzzy keyword search over encrypted cloud data. The fuzzy keyword search greatly improves system usability by returning the matching files, when the user's search inputs precisely match the predefined keywords or the likely matching files based on keyword similarity semantics. The edit distance to calculate keyword similarity is broken in this solution and for the construction of fuzzy keyword sets, two advanced techniques are developed that accomplishes the optimized representation overheads and storage. Further, a new symbol-based tree traverse searching scheme, which is different from a multi-way tree structure built using symbols converted from the obtained fuzzy keyword sets, is proposed.

Prashant et al., [11] proposed a three protection scheme, i.e. data security, authentication and verification, all at the same time, through a three-way mechanism. This mechanism is contributed by the combination of a key exchange algorithm together with an encryption algorithm and an authentication technique. The use of digital signature and Diffie Hellman key exchange along with (AES) Advanced Encryption Standard encryption algorithm is proposed to protect the confidentiality of data stored in the cloud. If at all, the key in the program is hacked, the facility of Diffie Hellman key exchange renders it useless since the key in transit is not useful without the user's private key. The proposed architecture prevents hackers from cracking the security arrangement, in so doing, protecting the data stored in the cloud.

the suitable privacy protection which satisfies the user demand privacy requirement and sustains system performance simultaneously. Above all, the privacy level users require and quantify the security degree and performance of encryption algorithms. At that point, a suitable security composition is derived from the results of analysis and quantified data. To conclude, the user-demand privacy is fulfilled by EPPS as shown by the simulation results which also preserve the cloud system performance in different cloud environments.

Rongmao et al., [13] presented a familiar cryptographic primitive, namely, PEKS framework- public key encryption with a keyword search. This suffers from inherent insecurity termed inside keyword guessing attack (KGA) launched by the harmful server. To address this vulnerability, a new PEKS framework named dual-server PEKS (DS-PEKS) is projected. Additionally, to build a generic scheme, a new Smooth Projective Hash Function (SPHF) is introduced and used. An efficient DS-PEKS scheme without pairings is given by an efficient instantiation of the new SPHF based on the Diffie-Hellman problem.

Zhang et al., [14] discuss cloud computing data, safety model. The cloud computing data application mode is summarized by the system and the data application system model in a cloud computing system is offered. The evaluation of the basic safety of the cloud computing data platform is also performed. A multi-dimension architecture of three layers' defense is held by the model. Through authentication, the user can get access to relative operations on the user data. The data of the user is in encrypted form and therefore, ensures security.

Volker et al., [15] presented a new methodology to cloud computing entitled cloud networking adds networking functionalities, that permits flexible and dynamic assignment of virtual resources by crossing provider borders. The security goals of service users are preserved through this architecture, while at the same time, at different virtual infrastructure providers, the flexible and dynamic placement of virtual resources advances. The key concepts of the system are formed by the conversion of security parameters in security constraints and the management of service users and virtual infrastructure providers by service providers.

Sudhansu et al., [16] projected a new security architecture that implements RSA for secure communication purposes and encryption, then for digital signature and hiding key information, MD5 hashing is used. The user can acquire secure communication and also hide the information from illegal users by this mechanism. In this, the slow functioning of the system is overcome by implementing each algorithm in different servers. Since the algorithms are implemented in different servers at different locations in the proposed system, an intruder cannot easily access or upload the file.

Wassim et al., [17] has presented Privacy as a Service (PaaS) which is a collection of security protocols for guaranteeing the privacy and legal agreement of data of the customer in cloud computing architectures. The solution for the security relies on the cryptographic coprocessors which provide an isolated and trusted execution environment in the computing cloud. PaaS central design goal is to maximize users' control in managing the several aspects related to the privacy of sensitive data which is achieved by data privacy mechanisms and applying for user-configurable software protection.

Dongxi et al., [18] offered a preserving the order scheme for indexing the encrypted data and facilitating the range queries over encrypted databases. The indexing is built simple since it is based on linear expressions. The randomized indexes are order-preserving, since controlling the number of noises is given away. For improving the robustness of the indexing programs, the elementary indexing expressions are collected together and the scattering of input values from indexes is hidden.

Jiadi et al., [19] has said that cloud potentially causes privacy problems and hence, should be handled wisely. Here, the objective is to solve data privacy concerns using searchable symmetric encryption (SSE), by expressing the privacy issue from the piece of relevance, similarity, and scheme robustness. A two-round searchable encryption (TRSE) scheme is proposed to get rid of the data leakage, which also supports top-k multi-keyword retrieval. For providing sufficient search accuracy, the vector space model is implemented and also, users are allowed to involve in the ranking through the homomorphic encryption, while the widely held computing work is completed on the server side by processes imparted on cipher text only.

Ning et al., [20] a multi-keyword ranked search over encrypted data (MRSE) procedure is used to solve the challenging problem of privacy-preserving in cloud computing. For a secured cloud data utilization system, a set of strict privacy requirements is being recognized. Among several multi-keyword semantics, to capture the relevance of data documents to the search query, selection of proficient similarity measure of coordinate matching is performed. To attain various rigorous privacy requirements, two improved MRSE schemes are set in two different threats models.

Ning et al., [21] has defined and solved the problem of a privacy-preserving query over encrypted graph-structured data in cloud computing (PPGQ). A set of firm privacy requirements is established for such a secure cloud data utilization scheme. Filtering-and verification is the principle employed here. An index that is feature-based is pre-built to deliver feature-related information about the respective encrypted data graph. Then to carry out the filtering procedure, the effective inner product is selected as the pruning tool.

Congetal et al., [22] offered a privacy-preserving public auditing structure in Cloud Computing for the security of data storage. During the efficient auditing process, the homomorphic authenticator and random masking are utilized to guarantee that TPA would not pick up any knowledge about the data stored on the cloud server. This removes the burden of a user from the tiresome and probably expensive auditing task. The multi-user setting is extended with the privacy-preserving public auditing protocol, where TPA can achieve the multiple auditing tasks consecutively.

R. H. Sakr et al., [23] has introduced a hybrid encryption algorithm based on the two security algorithms, the Rivest-Shamir-Adleman (RSA) and the Advanced Encryption Standard (AES) which is implemented on a cloud platform called eyeOS. The result for both computation time and security is optimized by this hybrid encryption algorithm. Following the hybrid algorithm, for a small amount of data, the slower but scalable algorithm should be used for encryption, and the bulk data, the faster algorithm should be used. A secure system hence has been fulfilled which would deliver speed, scalability and more security.

Qian et al., [24] studied the problematic integrity ensuring data storage in Cloud Computing. To guarantee cloud data storage security, a third party auditor (TPA) seems to be critical to estimate the quality of service from an objective as well as an independent perspective. In Cloud Computing, the difficulty of providing data dynamics for remote data integrity check and simultaneous public verifiability is explored. The structure is intentionally designed to come across the two important goals where efficiency is being considered very much important. An elegant Merkle hash tree construction is used to accomplish fully dynamic data operation which has extended the system to the PoR model.

Cong et al., [25] demonstrated applications on data storage security in the cloud, where the quality of service stands as an important feature. The distributed scheme which is flexible with data support open dynamically, including block update, deletes, and append is proposed to ensure the correctness of user's data residing in the cloud. The integration of storage accuracy insurance and data error localization of the system is achieved employing the homomorphic token along with distributed verification of erasure-coded data. The data blocks are supported with additional security and efficient dynamic operations in the new system.

Zhang Qian et al., [26] proposed an algorithm for load balancing task scheduling built on a feedback mechanism. It gives us ideas about how we can avoid the system bottleneck and balance load efficiently. In the beginning, the needed resources are chosen by the selected cloud scheduling host. The algorithm chosen is sorted by weight which then acquires the dynamic filter and sorts the left. Peer to peer cloud computing environment is the basic idea. It will not over-abound for the nodes with excellent performance.

Burhan et al., [27] discussed about Secure-Split-Merge Data Distribution in Cloud Infrastructure. The SSM scheme which is proposed here uses a special technique of splitting the data. The various rack servers of cloud zones maintain the parts of encrypted splits. Comparatively, the proposed system stretches effective results as per the relative analysis.

Anshika et al., [28] presented Data Security in the Cloud. The triple DES, AES are some of the symmetric algorithms. Here, the proposed techniques are used in different mathematical functions and further make use of a split algorithm for splitting the log file. Later, the future work becomes easy as the split files are stored in a different cloud. They use a folder lock approach in this program to check whether the folder has an XML file or not and checks for password insertion. If not, it creates password insertions with XML to enhance the security.

Goce et al., [29] proposed Block Encryption Ciphers based on Chaotic Maps. Brute force is the most organized attack to the ciphers, says extensive cryptanalysis hypothesis. The advantages of this algorithm are encryption, which provides security and integrity are maintained by the encrypted data. The disadvantages are forgetting passwords and developing a false sense of security.

Shucheng et al., [30] offered the Key Policy Attribute-Based Encryption (KP-ABE) algorithm which highlights security over the data. In this, most of the computation overhead is transferred to cloud servers by the data user. The advantage of this algorithm is non-negligible and the disadvantage is that it is designed for one to many communications.

Hongwei et al., [31] presented Identity-Based Authentication for Cloud Computing. In this, based on the identity based ranked model and corresponding encryption along with signature schemes, identity-based authentication for cloud computing is implemented. SSL authentication protocol is low efficient for cloud services as well as for users. The disadvantage is that users will go through a heavily loaded point in computation and communication due to the Cloud computing complexity.

Ming et al., [32] presented Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing. Here, the author proposed an encryption algorithm for data security. Here, addressing of authorized private searches over the encrypted PHRs in cloud computing is carried out. Based on a recent cryptographic primitive, the system offers two ways out for APKS. The advantage is that the owner can exert fine-grained control on user's search accesses to PHR documents and the disadvantage is that the data is not secured.

Ines et al., [33] proposed Cloud Service Delivery across Multiple Cloud Platforms. Allowing the cloud agents to well split requests among many cloud providers thereby minimizing cost is the main aim of this system. The advantage is that the data remains secured and the disadvantage is that it takes more time to retrieve the data. Chuang et al., [34] proposed an Effective Privacy Protection Scheme for Cloud to enhance the security of the data on the cloud. The suitable privacy protection that accomplishes the user demand privacy requirement and also sustains system performance concurrently is delivered by the Effective Privacy Protection Scheme (EPPS). The advantage of this method is, it assures more data security and has its disadvantage in more time complexity.

Yan et al., [35] to support the scalability of service and data migration, proposed the construction of an efficient Provable data possession (PDP) scheme for distributed cloud storage. PDP is referred to as a technique for ensuring the integrity of data in storage outsourcing. All the security properties required are provided by a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy so that it can fight various attacks. Further, the periodic verification and probabilistic query is optimized to increase the audit performance.

Peng et al., [36] offers a solution to the keyword guess attack (KGA) where the malevolent third party compromises the keyword. Here, the problem is addressed with public-key encryption with a fuzzy keyword search (PEFKS). With this, an exact keyword search trapdoor and a fuzzy keyword search trapdoor correspond with each keyword. The third party is given only with the fuzzy keyword search trapdoor to search a specific keyword contained in a specific document. This outputs minimum entropy more any other fuzzy function.

Sven et al., [37] presented a design for the externally protected source of data and erratic computations to an untrusted cloud. A Commodity Cloud and a Trusted Cloud are the two clouds (twins) that the construction comprises of. In the untrusted cloud, the data stored and operations accomplished are confirmed once the user communicates with a trusted cloud that encrypts. In a trusted cloud, the computations are split in such a way that it is mostly used for security-critical operations in a lesser amount of time-critical set-up phase. In parallel to this, the commodity clouds on encrypted data process the queries to the externally sourced data.

Bryan et al., [38] presented Pinocchio, a structure that is built for verifying the computations efficiently while depending only on cryptographic assumptions. To attain both asymptotic and concrete efficiency, a highly efficient cryptographic protocol grouped with quadratic programs is used. A natural cryptographic protocol is an outcome for efficiently signing computations. Verifiable computation is brought much closer to the practicality by Pinocchio.

Raghavendra et al., [39] propose an encryption technique here. For a dynamic group in the cloud, a secure multi-owner data sharing with RSA Chinese Remainder Theorem (RSACRT) is built. In this, to encrypt and store the data in the cloud, the Master key generation is used. An efficient index building algorithm is used for cost-efficient and speed file retrieval from the cloud. The storage space of the index file and key size is reduced in this key generation algorithm. The master-key is updated in the algorithm with every revocation or membership change, keeping the surviving group members private and public keys unaltered.

Bhavani et al., [40] presents a system for a secure share of the huge amount of data in the cloud, allowing cooperating organizations. By the usage of Hadoop, it also ensures the organizations to have a more common storage area. Besides, to present users of the system with a structured view of the data, Hive is used and also a SQL like a language is used to enable them to query the data. Lastly, using XACML policies, fine-grained access control has been provided on the shared data.

Raghavendra et al., [41] presents a search technique, Fast Result Object Retrieval using Similarity Search (FRORSS) on Cloud. This works without allowing the server occupies the privacy of the data residing in the cloud in its environment. The build phase, the data transformation, and the search phase are the three phases of this model. The process uploads data transform it before giving in the data for resemblance queries to the service provider on the transformed data and examines for same concerning query object in the respective phases.

Tonny et al., [42] for secure communication in the cloud computing environment, presented an innovative security structure that included the EL Gamal cryptosystem and DES file encryption system. The use of lightweight security ensuring algorithms ensures both securities to the uploaded file as well as less execution time. In this system, with the help of a unique encryption key, the user authentication system executes each algorithm individually on every single server which helps in the proper user interaction. The algorithm results are then transmitted from one side to the other side.

Abid et al., [43] in order to protect user data from hackers and make sure a more secured communication system in cloud computing platform, proposed security architecture. In this model, the integration of the asynchronous key system for the exchange of data and AES based file encryption system is performed. For safe communication between client and cloud storage system, the one-time password (OTP) system for user authentication ECC (Elliptic curve cryptography) has been proposed in the model. The SHA2 algorithm is used for hiding data from attackers.

Pruthviraj et al., [44] came up with the solution to perform encryption revocation based on identity in cloud computing storing sensitive and confidential data, which is a challenging task because it requires more security. In this model, dynamic groups are supported and they can be shared securely with others, once added to the group without contacting the admin always. Here, without updating keys users can easily remove the users and also, any user from another group can request file to the other group user. High security is provided for each user and the identity of the user can be shown by admin. In the AES algorithm, each cipher encrypts and decrypts the data and in AddRoundKey step, the matrix is XORed with the round key. Finally, for the reason of security, user can send data anonymously with others.

Payal et al., [45] carried out a Survey of Various Homomorphic Encryption algorithms and Schemes. It is the encryption scheme for the user to process data and to preserve privacy employing operations on the encrypted data homomorphic encryption. Based on the homomorphic encryption scheme for giving security, the public key cryptographic algorithms are emphasized. Encryption, Evaluation, and Decryption are the three functions of Homomorphic Encryptions. There are plans like Algebra Homomorphic Encryption Scheme and Non-Interactive Exponential Homomorphic Encryption Scheme. This survey is useful for applying a homomorphic algorithm for privacy preservation.

Guojun et al., [46] proposed a schema that helps enterprises to efficiently share confidential data on cloud servers. This was known as the Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. At first, the goal is accomplished by merging the cipher text-policy attribute-based encryption (CP-ABE) system and the hierarchical identity-based encryption (HIBE) system. Then, the performance-expressing trade-off is done and lastly, to offer fine-grained access control and full delegation, proxy re-encryption and lazy re-encryption HIBE system and a CP-ABE system is applied. Its future work is to design a more expressive design to provide full security.

Maha et al., [47] proposed a new idea, Homomorphic Encryption Applied to the Cloud Computing Security. The major need of organizations is the usage of cloud that includes low cost and easy to maintain. Here, the process goes on with the method applied for the execution of operations on encrypted data and that is done without decrypting the data which will provide us with the same results after calculations. The operations on encrypted data without knowing the private key (without decryption) is performed based on homomorphic encryption. The secret key will be held by the client who will be the only key holder.

Takahiro et al., [48] offers a general technique for creating Public key Encryption known as Simple CCA-Secure Public Key Encryption from any Non-Malleable Identity-Based Encryption. The cloud attacks are made tough by providing security which is obtained under identity “f(r)” by encrypting (m—r) with the encryption algorithm of the known IBE scheme. The IBE scheme is dissimilar and ‘f’ is one-way. Also, the user cannot see the direct variations from the previous techniques since it is non-malleable.

Levent et al., [49] proposed a scheme that helps in the reduction of data redundancy and increases in durability of the network by using Homomorphic Encryption Schemes in Wireless Sensor Networks (WSNs) through Computing Aggregation Function Minimum/Maximum. It relies on comparison operation. Some of the homomorphic encryption schemes were explained and how the known data is encrypted is shown using these schemes. In WSNs, by performing addition operation, the minimum or maximum of the aggregation function can be computed at the aggregator node. The elimination of the encryption cost at the sensor node is also demonstrated in this scheme.

Rachna et al., [50] proposed a technique that uses the RSA algorithm, namely Secure User Data in Cloud Computing Using Encryption Algorithms. In order to make cloud data secure, encryption algorithms have been proposed. RSA is the most powerful encryption algorithm used today. The advantage is to secure the data residing in cloud computing. The disadvantage is that it is very slow in cases where large data needs to be encrypted by the same computer. Ji et al., [51] performs an analysis that includes data encryption approaches for giving security to e-commerce applications on the privacy requirements for the applications of the cloud. The data encryption causes performance penalties whose quantitative estimation is to be delivered. A standard for an online marketplace application as a case study is done here. Furthermore, it discusses that both critical business transaction data and user related data must be mandatorily encrypted.

Suli et al., [52] presents a wide-ranging set of a hands-on way out based on the RSA algorithm for file encryption, by finding the feasibility of using it for file encryption. For encrypting smaller files, this algorithm is used, where, it is more convenient to manage and communicate because it has asymmetric key encryption into its texts. Taking into account, the efficiency and re-usability, this application was structured which has broad developmental prospects.

Rakesh et al., [53] presents a scheme that directly applied queries associated with comparison operators to the encrypted numeric columns. This was named as an order-preserving encryption scheme, OPES. To easily integrate the prevailing database indexes construction is allowed over encrypted tables by this scheme. It is designed for operating in environments where an intruder may be accessible to the encrypted database. It is strong since it is made difficult for anyone to acquire a tight estimation of an encryption rate.

Deyan et al., [54] deals with the privacy protection and data security concerns related to all phases of the data life cycle by delivering concise and overall analysis. To construct a collection of combined identity supervision and privacy protection frameworks across cloud computing services or applications stands as the main objective. In the cloud environment, the strict partition of sensitive and non-sensitive data is done, later which sensitive elements will be encrypted through the idea of the key to privacy protection.

Cheng et al., [55] offers a Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. They let us know about cryptography techniques here. This is all about efficiently securing the shared data with other users in cloud storage which also describes the newly found public-key cryptosystems. A compact single key can be made by gathering the collection of secret keys from constant-size cipher texts. By the usage of smart cards having limited secure storage, these close-packed collected keys can be sent to others. This approach seems flexible for saving spaces if the same set of privileges is shared among the key-holders.

Emily et al., [56] proposed Predicate Privacy in Encryption Systems. In this, the owner is given control over the encrypted key property. A new idea called predicate privacy is considered. In the symmetric-key setting, the predicate encryption is considered and asymmetric-key predicate encryption scheme supporting the inner product queries is presented. This scheme proves that it achieves plain text privacy as well as predicate privacy.

Jinbao et al., [57] proposed a new system where an important role is played by database systems indexes for the improvement of performance, named Indexing Multidimensional Data in a Cloud System. Here, for query processing on different applications efficiently, different types of indexes are used. To provide efficient multi-dimensional query processing in a Cloud system, RT-CAN which is a multi-dimensional indexing system and R-tree based indexing system are used. Point Query Processing, QUERY PROCESSING, are many types of query processing used.

Sai al., [58] proposed an efficient system knowing the need for handling the large volume of data. The B-tree Based Indexing for Data Processing in Cloud Computing satisfies the current need. A novel and scalable B+-tree based indexing scheme are presented for efficient data processing in the Cloud. For the organization of compute nodes as a structured overlay that helps in efficient query processing, a portion of the local B+tree nodes to the overlay is published. Lastly, following the query patterns, the published B+-tree nodes are selected using an algorithm adapted. This indexing scheme is dynamic.

Stepan et al., [59] proposed the Secure Metric-Based Index for Similarity. They presented a similarity index that makes sure the data privacy. So, it is fit for search systems this system can replace the existing metric indexes this encrypted m-index tested on datasets. The data owner creates the MS objects from the original data and these send MS objects to the same cloud for indexing and also for the raw data to data storage. At the server side resource demanding process is formed again. Communication cost is less after data is stored in the server side securely and further, they are going to study about the various types of distance transformations.

Raghavendra et al., [60] proposed an indexing technique for the cloud environment, the Most Significant index Generation technique. The MSIGT is one of the simpler and faster techniques for sorting array list. It supports index generation by Most Significant Digit. To encrypt the indexed keyword, a mathematical model is developed which reduces the cost on the owner side with a simple calculation of 0(Nt). Reducing the search time and index storage generation is referred to as future work.

Raghavendra et al., [61] presented a technique that solves the problematic synonym and fuzzy based keyword index generation over the data stored in the cloud. Here, the user is allowed to search through keywords in the encrypted cloud data which can be retrieved by selecting the files. Using the split factor for keyword search over encrypted cloud data in the cloud, the index generation method is implemented. For the ranking mechanism, the technique TF*IDF is used. The advantage of IGSK system is that it takes a smaller amount of storage space and less index generation time than any other schemes.

Raghavendra et al., [62] to maintain privacy and security, the confidential data is to be encrypted previously before uploading to the cloud server. Here, the Domain and Range Specific Index Generation (DRSIG) scheme are proposed, which aims at minimizing the Index Generation time. For splitting the index file into D Domains and R Ranges, the structure acquires collection sort technique. Based on the length of the keyword, Domain D is sort and based on the first character of the keyword, Range R is sorted. For encrypting the indexed keyword, a mathematical model is used which removes the data leakage.

Wenhai et al., [63] has given a verifiable privacy preserving multi-keyword text search (MTS) scheme with similarity-based ranking. This was developed to address the problem of secure search functions over encrypted data. A tree-based index system and different approaches for the multi-dimensional (MD) algorithm is projected to improve the search efficiency. Besides, to enable authenticity and to check over the returned search results, a scheme upon the proposed index tree structure is devised. Therefore, through extensive experimental evaluation, the efficiency and effectiveness of the proposed scheme is demonstrated.

Rakesh et al., [65] presents a study on the usage of services and privacy in Cloud computing. Addressing the concerns that can stand up during the deployment of a cloud services model, this paper provides the foundation for the deeper investigation on the security deployment of cloud computing. It checks for various cloud vulnerabilities and briefs the solution for each of them.

Chi et al., [64] has projected a method named hierarchical clustering for supporting additional search semantics which also aims at meeting the request for fast cipher text search in a big data environment. In the search phase, a linear computational complexity can be reached against an exponential size increase of document collection by this proposal. To verify the authenticity of the search results, a system called the minimum hash sub-tree is constructed. Over many traditional methods in the rank of privacy and retrieved documents relevance, this has many more advantages.

Raghavendra et al., [66] offered a technique that supports efficient and accurate search over encrypted cloud data. In the index file, to sort the keywords, the MSD radix sort algorithm is used. For clustering the keywords with the same ASCII value into a bucket, usage of counting sort algorithm is performed. Compared to the other existing systems, the efficiency of the proposed system is found to be more efficient supporting a vast number of data files which also diminishes the overhead on computation.

Bing et al., [67] discussed Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud which allows keyword search over encrypted data. In this system, a well-worn multi-keyword fuzzy search is proposed to attain fuzzy searching through the algorithmic design. Here the proposal is to construct the file index providing a solution to the secure fuzzy search of multiple keywords.

Yanbin et al., [68] proposed Privacy-Preserving Logarithmic-time Search on Encrypted Data in Cloud privacy preserving database in a cloud environment. The data owner will be keeping a record then the user can use this to search. They introduce range predicate encryption (RPE) that is used as a cryptographic building block. The data owner, the data user and the cloud server are the three entities that the cloud storage LSED system comprises of. Encrypted data is stored by the data owner. The search token is used by the cloud server to perform a logarithmic search to obtain the matching data. This system is to reinforce query authentication and provable data update. Raghavendra et al., [69] offers a solution to the problematic fuzzy based keyword search and multi-keyword ranked search and synonym over the encrypted cloud data. The synonym queries with higher accuracy and synonym-based search are reinforced by the multi-keyword ranked search using this system. For indexing, we use a method named inverted index while wild-card based technique for indexing keywords and the TF*IDF technique for ranking mechanism. The fuzzy-based queries are strengthened by the SKFS scheme which outperforms the B-tree scheme.

Sahin et al., [70] introduces a scheme on public-key encrypted data for privacy-preserving ranked keyword search. For processing queries in a privacy-preserving manner, a simple indexing structure, impact homomorphic encryption and private information retrieval protocols is set. Additionally, for the cryptographic primitives of this approach, several optimizations are introduced. These optimizations are used for diminishing the query response time by several orders of magnitude. Lung Yiu et al., [71] by the introduction of approaches that shift search functionality to the server, presented resemblance search methods for sensitive metric information. To store the relative information on the distance at the server under the private set of anchor objects, Metric Preserving Transformation (MPT) is proposed. An interesting trade-off among accuracy and query cost is given by this approach.

Hemant et al., [72] proposed a flexible and effective scheme associated with dynamic data, supported explicitly to assure the user data correctness in the cloud. The integration of localization of data error and storage correctness insurance is attained by the exploitation of homomorphism token using distributed verification ensuring the data coded. The scheme is highly resourceful and robust to server conniving occurrences, malicious data modification outbreak and various failures like Byzantine.

Table 1. Comparison of previously published research works

Authors	Splitting	Indexing	Encryption	Searching
Kawser et al., [9]	NO	NO	YES	NO
Jin et al., [10]	NO	YES	YES	YES
Prashant et al., [11]	NO	NO	YES	NO
Chuang et al., [12]	NO	NO	YES	NO
Rongmao et al., [13]	NO	NO	YES	NO
Zhang et al.,[14]	NO	YES	YES	YES
Volker et al., [15]	NO	NO	YES	NO
Sudhansu et al., [16]	NO	NO	YES	NO
Wassim et al., [17]	YES	NO	YES	NO

Padmapriya et al., [73] discusses security mechanisms in cloud computing and presents the comparison of three algorithms, namely, Homomorphic encryption, RSA and Data Encryption Standard (DES). Based on the stability of key used, applied security and the type of authentication, the algorithms are compared since these are important cloud computing security characteristics.

Kapoor et al., [74] proposed the algorithm on data encryption and decryption by modifying the RSA algorithm. The modification involves multiple public keys and 'n' prime numbers, thus, enabling secure data transfer on the transmission medium and high security over the network. As in the RSA algorithm, an extremely large number with four prime factors is taken and also, two public keys and 'n' prime numbers are used, making it difficult for the attacker to get the keys and decrypt the data. This algorithm provides more security but less speed comparatively.

Raghavendra et al., [75] developed a scheme Domain and Range Specific Multi keyword Search (DRSMS) where the search time and index storage space is minimized. The scheme holds the technique collection sort for splitting the index file into D domains and R ranges where the domain is according to the specified length of the keyword. The range is split within the domain following the efficient letter of the given keyword. A secure search on the index file is given by this model without any data outflow since the DRSMS algorithm is involved to give effective indexing and searching on data encrypted.

Vivek et al., [76] proposed a solution for performance improvement of SaaS and PaaS in the cloud environment. The study is all about the Cloud computing system consisting of virtualized computers and interconnected computers. Based on the service-level agreement established through negotiation between the service provider and clients, these computers are dynamically provisioned and presented as one or more unified computing resources. The comparative study of data center challenges of different cloud vendors is carried out here for wider views.

Raghavendra et al., [77] briefs about the data storage and retrieval techniques over encrypted cloud data where various keyword search techniques are discussed based on different parameters. An overview is presented based on the scalability, efficiency, functionality and architecture, which can be classified for various requirements. It also comprises of comparison table of different models that can derive the basic strategic idea.

Raghavendra et al., [78] discusses about the emerging trends, challenges and issues in Big Data, IoT and Cloud Computing. It briefs about various challenges faced during management and processing and also, it provides novel approaches related. It also suggests that IoT domain can make best use of both Cloud Computing and Big Data Analytics.

III. Conclusion and Future Scope

Cloud computing is Internet-based computing where central remote servers maintain all the data and applications. The benefits of cloud computing are widely accepted and enterprises are moving fast to experience the transformation. Although, it is seen that there are some crucial issues to be solved regarding the successful deployment of cloud computing, cloud computing remains a developing paradigm of distributed computing. This far-reaching survey paper targets to elaborate and investigate the number of uncertain issues threatening cloud computing adoption. Here, several papers regarding cloud computing have been surveyed. The security issues, privacy risks have been addressed and numerous methodologies to solve the risks with each of their pros and cons, ensuring safety and reliability are presented. The existing solutions to address the security issues of the Cloud are looked into while finding some open problems. It opens up space for further research, to extend prevailing techniques and to explore new techniques for privacy and security in the cloud. This paper throws light on only some of the focused concepts like keyword search, indexing, file splitting, encryption, and multi-clouds. As a part of future work, more complex topics can be surveyed that might help the research works.

REFERENCES

[1] M. Almorsy, J. Grundy, and I. M¨uller, “An analysis of the cloud computing security problem,” arXiv preprint arXiv:1609.01107, 2016.

[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multikeyword ranked search scheme over encrypted cloud data.” IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340–352, 2016.

[3] P.Arora,A.Singh,andH.Tyagi,“Evaluationandcomparisonofsecurity issues on cloud computing environment,” World of Computer Science and Information Technology Journal (WCSIT), vol. 2, no. 5, pp. 179–183, 2012.

[4] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.

[5] S. El-etriby, E. M. Mohamed, and H. S. Abdul-kader, “Modern encryption techniques for cloud computing,” in ICCIT, 2012, pp. 800–805.

[6] S. S. Khan and R. Tuteja, “Security in cloud computing using cryptographic algorithms,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 1, pp. 148–155, 2015.

[7] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[8] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[9] K. W. Nafi, T. S. Kar, S. A. Hoque, and M. Hashem, “A newer user authentication, file encryption and distributed server based cloud computing security architecture,” arXiv preprint arXiv:1303.0598, 2013.

[10] 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.

[11] P. Rewagad and Y. Pawar, “Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing,”in Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013, pp. 437–439.

[12] I.-H. Chuang, S.-H. Li, K.-C. Huang, and Y.-H. Kuo, “An effective privacy protection scheme for cloud computing,” in Advanced Communication Technology (ICACT), 2011 13th International Conference on. IEEE, 2011, pp. 260–265.

[13] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “Dual-server publickey encryption with keyword search for secure cloud storage,” IEEE transactions on information forensics and security, vol. 11, no. 4, pp. 789–798, 2016.

[14] Z. Xin, L. Song-qing, and L. Nai-wen, “Research on cloud computing data security model based on multi-dimension,” in Information technology in medicine and education (itme), 2012 international symposium on, vol. 2. IEEE, 2012, pp. 897–900.

[15] V. Fusenig and A. Sharma, “Security architecture for cloud networking,” in Computing, Networking and Communications (ICNC), 2012 International Conference on. IEEE, 2012, pp. 45–49.

[16] [16] S. R. Lenka and B. Nayak, “Enhancing data security in cloud computing using rsa encryption and md5 algorithm,” International Journal of Computer Science Trends and Technology, vol. 2, no. 3, pp. 60–64, 2014.

[17] W. Itani, A. Kayssi, and A. Chehab, “Privacy as a service: Privacyaware data storage and processing in cloud computing architectures,” in Dependable, Autonomic and Secure Computing, 2009. DASC’09. Eighth IEEE International Conference on. IEEE, 2009, pp. 711–716.

[18] D. Liu and S. Wang, “Programmable order-preserving secure index for encrypted database query,” in 2012 IEEE Fifth International Conference on Cloud Computing. IEEE, 2012, pp. 502–509.

[19] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, “Toward secure multikeyword top-k retrieval over encrypted cloud data,” IEEE transactions on dependable and secure computing, vol. 10, no. 4, pp. 239–250, 2013.

[20] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data,” IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.

[21] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, “Privacy-preserving query over encrypted graph-structured data in cloud computing,” in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 393–402.

[22] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Infocom, 2010 proceedings ieee. Ieee, 2010, pp. 1–9.

[23] R. Sakr, F. Omara, and O. Nomir, “An optimized technique for secure data over cloud os,” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume, vol. 3.

[24] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in European symposium on research in computer security. Springer, 2009, pp. 355–370.

[25] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security i.n cloud computing,” in Quality of Service, 2009. IWQoS. 17th International Workshop on. Ieee, 2009, pp. 1–9.

[26] ZQian, G.Yufei, L.Hong, and S.Jin, “A load balancing task scheduling algorithm based on feedback mechanism for cloud computing,” International Journal of Grid and Distributed Computing, vol. 9, no. 4, pp. 41–52, 2016.

[27] B. U. I. Khan, A. M. Baba, R. F. Olanrewaju, S. A. Lone, and N. F. Zulkurnain, “Ssm: Secure-split-merge data distribution in cloud infrastructure,” in Open Systems (ICOS), 2015 IEEE Confernece on. IEEE, 2015, pp. 40–45.

[28] A. Negi, M. Singh, and S. Kumar, “An efficent security farmework design for cloud computing using artificial neural networks,” International Journal of Computer Applications, vol. 129, no. 4, p. 1721, 2015.

[29] G. Jakimoski and L. Kocarev, “Chaos and cryptography: block encryption ciphers Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, no. 2, pp. 163–169, 2001.

[30] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Infocom, 2010 proceedings IEEE. Ieee, 2010, pp. 1–9.

[31] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in IEEE International Conference on Cloud Computing. Springer, 2009, pp. 157–166.

[32] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted data in cloud computing,” in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 383–392.

[33] I. Houidi, M. Mechtri, W. Louati, and D. Zeghlache, “Cloud service delivery across multiple cloud platforms,” in Services Computing

(SCC), 2011 IEEE International Conference on. IEEE, 2011, pp. 741–742.

[34] I.-H. Chuang, S.-H. Li, K.-C. Huang, and Y.-H. Kuo, "An effective privacy protection scheme for cloud computing," in Advanced Communication Technology (ICACT), 2011 13th International Conference on. IEEE, 2011, pp. 260–265.

[35] Y.Zhu, H.Hu, G.-J.Ahn, and M.Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE transactions on parallel and distributed systems, vol. 23, no. 12, pp. 2231–2244, 2012.

[36] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Transactions on computers, vol. 62, no. 11, pp. 2266– 2277, 2013.

[37] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, "Twin clouds: An architecture for secure cloud computing," in Workshop on Cryptography and Security in Clouds (WCSC 2011), vol. 1217889, 2011.

[38] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in 2013 IEEE Symposium on Security and Privacy. IEEE, 2013, pp. 238–252.

[39] S. Raghavendra, K. Meghana, P. Doddabasappa, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Index generation and secure multi-user access control over an encrypted cloud data," Procedia Computer Science, vol. 89, pp. 293–300, 2016.

[40] B. Thuraisingham, V. Khadilkar, A. Gupta, M. Kantarcioglu, and L. Khan, "Secure data storage and retrieval in the cloud," in Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on. IEEE, 2010, pp. 1–8.

[41] S. Raghavendra, K. Nithyashree, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Frorss: Fast result object retrieval using similarity search on cloud," in Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), IEEE. IEEE, 2016, pp. 107–112.

[42] S.Kar,M.P.Mahmud,S.H.Farjana,K.W. Nafi,andB.C. Karmokar, "A newer secure communication, file encryption and user identification based cloud security architecture," International Journal of Computer Applications, vol. 52, no. 4, 2012.

[43] A. Hussain, C. Xu, and M. Ali, "Security of cloud storage system using various cryptographic techniques."

[44] P. S. Patel, K. Patidar, M. Yadav, R. Kushwah, and S. SSSIST, "A result paper on outsourced revocation of encryption based on identity in cloud computing," International Journal of Engineering Science, vol. 16078, 2018.

[45] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of various homomorphic encryption algorithms and schemes," International Journal of Computer Applications, vol. 91, no. 8, 2014.

[46] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.

[47] M. Tebaa, S. El Hajji, and A. El Ghazi, "Homomorphic encryption applied to the cloud computing security," in Proceedings of the World Congress on Engineering, vol. 1, 2012, pp. 4–6.

[48] T. Matsuda, G. Hanaoka, K. Matsuura, and H. Imai, "Simple ccasecure public key encryption from any non-malleable identity-based encryption," in International Conference on Information Security and Cryptology. Springer, 2008, pp. 1–19.

[49] E. Vaidehi, "Computing aggregation function minimum/maximum using homomorphic encryption schemes in wireless sensor networks (wsns)," California State University, East Bay Hayward, CA, USA, vol. 14, 2007.

[50] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International journal of engineering research and applications, vol. 3, no. 4, pp. 1922–1926, 2013.

[51] J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," in Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on. IEEE, 2009, pp. 735–740.

[52] S.Wangand G.Liu, "File encryption and decryption system based on rsa algorithm," in Computational and Information Sciences (ICCIS), 2011 International Conference on. IEEE, 2011, pp. 797–800.

[53] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563– 574.

[54] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1. IEEE, 2012, pp. 647–651.

[55] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Keyaggregate cryptosystem for scalable data sharing in cloud storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 468– 477, 2014.

[56] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Theory of Cryptography Conference. Springer, 2009, pp. 457–473.

[57] J. Wang, S. Wu, H. Gao, J. Li, and B. C. Ooi, "Indexing multidimensional data in a cloud system," in Proceedings of the 2010 ACM SIGMOD International Conference on Management of data. ACM, 2010, pp. 591–602.

[58] S. Wu, D. Jiang, B. C. Ooi, and K.-L. Wu, "Efficient b-tree based indexing for cloud data processing," Proceedings of the VLDB Endowment, vol. 3, no. 1-2, pp. 1207–1218, 2010.

[59] S. Kozak, D. Novak, and P. Zezula, "Secure metric-based index for similarity cloud," in Workshop on Secure Data Management. Springer, 2012, pp. 130–147.

[60] S. Raghavendra, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Msigt:Most significant index generation technique for cloud environment," in India Conference (INDICON), 2015 Annual IEEE. IEEE, 2015, pp. 1–6.

[61] S. Raghavendra, S. Girish, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Igsk: index generation on split keyword for search over cloud data," in Computing and Network Communications (CoCoNet), 2015 International Conference on. IEEE, 2015, pp. 374–380.

[62] S. Raghavendra, G. Mara, R. Buyya, V. K. Rajuk, S. Iyengar, and L. Patnaik, "Drsig: Domain and range specific index generation for encrypted cloud data," in Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on. IEEE, 2016, pp. 591–596.

[63] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025–3035, 2014.

[64] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Y. Zomaya, "An efficient privacy-preserving ranked keyword search method," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 951–963, 2016.

[65] R. Sarang and R. Bunkar, "Study of services and privacy usage in cloud computing," International Journal of Scientific Research in Computer Science and Engineering, vol. 1, no. 6, 2013.

[66] S. Raghavendra, C. Geeta, K. Shaila, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Msss: most significant single-keyword search over encrypted cloud data," in Proceedings of the 6th Annual Intrernational Conference on ICT: BigData, Cloud and Securit, 2015.

[67] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 2112–2120.

[68] Y. Lu, "Privacy-preserving logarithmic-time search on encrypted data in cloud." in NDSS, 2012.

[69] S. Raghavendra, S. Girish, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, "Split keyword fuzzy and synonym search over encrypted cloud data," Multimedia Tools and Applications, vol. 77, no. 8, pp. 10135–10156, 2018.

[70] S. Buyrukbilen and S. Bakiras, “Privacy-preserving ranked search on public-key encrypted data,” in High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC EUC), 2013 IEEE 10th International Conference on. IEEE, 2013, pp. 165–174.

[71] D. Liu and S. Wang, “Programmable order-preserving secure index for encrypted database query,” in 2012 IEEE Fifth International Conference on Cloud Computing. IEEE, 2012, pp. 502–509.

[72] H. T. Dhole, P. C. Papade, and S. B. Bhosale, “Ensuring data storage security using cloud computing,” Intl. Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 1, 2014.

[73] A. Padmapriya and P. Subhasri, “Cloud computing: security challenges and encryption practices,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, 2013.

[74] V. Kapoor, “Data encryption and decryption using modified rsa cryptographybasedonmultiplepublickeysand‘n’primenumber,” International Journal of Scientific Research in Network Security and Communication, vol. 1, no. 2, pp. 35–38, 2013.

[75] S. Raghavendra, C. Geeta, R. Buyya, K. Venugopal, S. Iyengar, and L. Patnaik, “Drsms: Domain and range specific multi-keyword search over encrypted cloud data,” International Journal of Computer Science and Information Security, vol. 14, no. 5, p. 69, 2016.

[76] V. Raich, P. Sharma, S. Mewada, and M. Kumbhkar, “Performance improvement of software as a service and platform as a service in cloud computing solution,” ISROSET-International Journal of Scientific Research in Computer Science and Engineering, vol. 1, pp. 13–16, 2013.

[77] Raghavendra, S., et al. "Survey on data storage and retrieval techniques over encrypted cloud data." International Journal of Computer Science and Information Security 14.9 (2016): 718.

[78] Kobusińska, Anna, et al. "Emerging trends, issues and challenges in Internet of Things, Big Data and cloud computing." (2018): 416-419.

Authors Profile

Supriya J, Computer Science and Engineering in Vivekananda College of Engineering and Technology, Puttur.

Her fields of interest are Artificial Intelligence and Internet of Things.

Srusti K S, Computer Science and Engineering in Vivekananda College of Engineering and Technology, Puttur.

Her fields of interest is Internet of Things and Cloud Computing.

Gamana G, Information Science and Engineering in Vivekananda College of Engineering and Technology, Puttur.

Her fields of interest is Artificial intelligence and Cloud Computing.

S Sukhaniya Ragani, Computer Science and Engineering in Vivekananda College of Engineering and Technology, Puttur.

Her fields of interest is Artificial intelligence and Big Data Analytics.

Dr. Raghavendra S received his Bachelor degree in Computer Science and Engineering from BMS Institute of Technology, Visvesvaraya Technological University, Bangalore and Master degree from R V College of Engineering, Visvesvaraya Technological University, Bangalore. and Ph.D. degree from the University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He is currently a Associate Professor at Vivekananda College of Engineering and Technology, Puttur. He has 8 years teaching and research experience in various institutes. Dr. Raghavendra S has authored over 25 publications and his research interests include Cloud Computing, applied cryptography and Internet of Things. He is serving as editorial board member, Reviewer and Guest editor for a number of prestigious journals, like IEEE, Elsevier, Springer, Wiley, Taylor and Frances, KJIP. He was a organizing committee member for conferences like ICCN-14, ICCN 15, ICCN-16, ICInPro-18, DISCOVER-19 and ICInPro-2019. He is a Executive committee member of IEEE and IEEE Mangalore Sub-Section Website Co-Chair. He delivered few technical talk related to BigData, IoT, Data Storage and retrieval techniques and Latex.

K. R. Venugopal received the Bachelor of Engineering degree from the University Visvesvaraya College of Engineering (UVCE), the master’s degree in computer science and automation from the Indian Institute of Science Bangalore, and the Ph.D. degree in economics from Bangalore University and in computer science from the Indian Institute of Technology Madras. He is currently the Vice Chancellor, Bangalore University, Bangalore. He has served as the Principal with the University Visvesvaraya College of Engineering, Bangalore University, Bengaluru for more than one decade. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science, and Journalism. He has authored and edited 72 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++, and Digital Circuits and Systems. He has filed 101 patents. During his three decades of service at UVCE he has over 800 research papers to his credit. His research interests include computer networks, wireless sensor networks, parallel and distributed systems, digital signal processing, and data mining. He is a Fellow of IEEE and a ACM Distinguished Educator.