Ad Hoc Networks 125 (2022) 102740

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT

B D Deebak [a,*], Fida Hussain Memon [b,c], Kapal Dev [d], Sunder Ali Khowaja [e], Nawab Muhammad Faseeh Qureshi [f,*]

[a] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632 014, India
[b] Department of Mechatronics, AMM Lab Jeju National University, South Korea
[c] Department of Electrical Engineering Sukkur IBA University, Pakistan
[d] Department of Institute of Intelligent Systems, University of Johannesburg, South Africa
[e] Department of Mechatronics Engineering, Korea Polytechnic University, Republic of Korea
[f] Department of Computer Education, Sungkyunkwan University, Seoul, South Korea

ARTICLE INFO

Keywords:
Industrial internet of things
Multi-keyword searching
Data privacy
Protection
Cloud computing
Secure searching efficiency

ABSTRACT

The integration of sensing technologies and cloud computing signifies the design perspectives of electronic healthcare systems. It has its own application domain to upload the clinical data of the patients and treatment procedures to the cloud server. Moreover, the data user may process the queries with suitable sensing parameters to obtain an appropriate medical record. As a result, the development of the Industrial Internet of Things (I-IoT) demands practical insights, trustworthiness, and reliability of intelligent automation to prevent the occurrence of potential risks in the process of production. In the past, multi-keyword searching (MKS) over encrypted cloud data has attracted researchers' attention. As cloud computing is highly practicing, data owners may easily outsource any kind of system data to commercial sites using the Industrial Internet of Things (I-IoT). However, data privacy and protection should be ensured using encryption techniques before any sensitive data is outsourced over insecure public networks. Providing cloud data encryption and secure keyword searching still exist as challenging issues. In I-IoT, cloud computing deals with a large amount of data users and documents, thus a technique like MKS is highly necessitated to process the search request and secure query processing. Thus, this paper presents a privacy-preservation phrase with multi-keyword ranked searching (PPP-MKRS) that introduces optimized filtering, binary tree index structure, and conjunctive keyword search to achieve secure searching efficiency. The experimental analysis shows that the proposed PPP-MKRS scheme consumes less computation, storage, and verification time in comparison with other searching encryption techniques.

1. Introduction

The industrial IoT exploits the features of the physical world to state the proposal of industrial standards. It can include multi-level security approaches to stream the system data over trusted authorities. Each approach has its own encryption strategy to interoperate the system heterogeneity in terms of software and hardware to protect industrial equipment and technological development. An I-IoT ecosystem considers an appropriate countermeasure to identify security vulnerabilities, risks, and threats. Most of the systems reform the paradigm structure of IoT to meet the industrial standards which evolve smart intelligence to make life easier. It can even emerge with artificial intelligence to manage the issues of IoT applications such as intelligent production, energy management, and organizational services. Moreover, the AI-enabled IoT systems demand a decision-making process to offer adaptable features including effectiveness, smart services, and reliability.

The IoT applications possess multi-dimension structures to explore the functionalities of remote servers and networks to solve real-time problems. To exploit accessible resources, smart computing devices apply diversified techniques. It uses multi-dimensional structures to signify the role of the decision-making process. Most computing devices integrate AI and IoT to design a systematic framework to regulate the evolution of the digital markets. An AI-enabled IoT deals with a three-

* Corresponding authors.
E-mail addresses: deebak.bd@vit.ac.in (B.D. Deebak), faseeh@skku.edu (N.M.F. Qureshi).

https://doi.org/10.1016/j.adhoc.2021.102740
Received 18 June 2021; Received in revised form 21 September 2021; Accepted 31 October 2021
Available online 14 November 2021

tier strategy to exploit the core features of smart application systems. The system has a reliable edge-tier architecture to transfer and control the communication between the end computing devices through a dedicated edge-gateway. An edge-gateway utilizes a proximity network to connect sensing components, actuator, and control system to provide inter-level communication. Moreover, the middleware applications such as data transformation and integration interface with a platform tier to offer high-level services.

Of late, the fifth generation (5 G) has standardized the technological standards of broadband cellular networks for the evolution of IoT-enabled wireless devices (IoT-EWD). Global commercialization engrosses the network initiatives towards sixth-generation (6 G) to determine performance requirements, technological innovation, and key drivers. International Telecommunication Union (ITU) discovers a new horizon to enable digital society and network innovation by 2030 [1]. An academic institute so-called the University of Oulu, Finland allies with a telecom research institution to launch a 6 G flagship project [2]. The university research partnership focuses on the evolution of networking architecture to enable new technological services such as critical and holographic communication. The united states collaborate with the federal communications commission to operate the 6 G network in the spectrum of TeraHertz $\langle THz \rangle$ [3]. It applies blockchain technology to offer a feature of dynamic spectrum sharing.

Also, the next-generation communication systems such as aerial, terrestrial, maritime, and satellite integrate the feature of the 6 G network to discover a space-air-ground integrated network (SAGIN) to propose various cutting edge technologies including quantum machine learning and Millimeter and Terahertz Waves Communication [4]. The generation of mobile communication systems generally drives the fundamental features of the 6 G network to empower digital technologies. The advancement of the Internet of Things (IoT) deals with system intelligence to connect the environmental object which utilizes the services such as enhanced mobile broadband (eMBB) and massive machine type communication (mMTC) to perform intensive computing, data collection, processing, and analysis [5]. Moreover, the communication technologies such as high-order modulation and low-density parity coding consider an eMBB scenario to achieve a peak data rate ~ 10 *Gbps*. However, the massive growth of IoT devices consumes a longer time to process the environmental data to the cloud storage system.

As a result, future networking system including 5 G/6 G makes a discovery of edge intelligence to minimize processing delay and to perform a power computation at mobile edge computing (MEC) [6]. It may converge computing, communication, and caching to standardize the vision of beyond 5 G (B5G) networks. Most networking scenarios present a predictive technical framework, three-dimension radio connectivity, cell-less architecture, and resource allocation to fulfill the system-level perceptive of 6 G applications. The emerging communication system utilizes sensitive sensors, immersive media, autonomous vehicles, and IoT to fulfill the key dimensions of digital society. The massive volume of physical objects centralizes the operational demands of 6 G to coordinate with intelligent networks which offer efficient interaction over a dedicated network infrastructure. An effective binding can vary the limits of the network latency and amplitude to support convenient access and edge computing. Moreover, this technical feature may effectively control the usage of network resources to meet the requirements of new communication services. Of late, cloud computing has rapidly been developed for various application services that deal with a massive amount of data over cloud-server [7].

To provide better storage efficiencies, private and public clouds are blended. It may involve a joint operation to develop a hybrid cloud. It is emerging as a new paradigm to perform storage and service computation. As a result, more individual users and enterprises are motivating to outsource the private data over a cloud server. It has several benefits such as high-quality services, greater flexibility, quick deployment, faster computation, and effective resource usage. The recent development makes a double-edged sword to address various challenging issues. Therefore, data security and privacy issues have attracted researches attention for the protection of cloud data [8]. To offer effective data retrieval and utilization, encrypted data over the cloud is stimulating more interest. In a cloud environment, data upload plays a significant role to ensure the security of sensitive data i.e. for data-owner. On the other hand, cloud servers should provide adequate protection from outsider attack. However, there may be a serious threat to the user data when the cloud server is compromised. Thus, the cloud server is usually a semi-trusted component to perform honest user requests when any data content is attempting to gain quality services [9].

Of late, encryption over cloud data has enhanced the development aspects of data security and user protection. Since the cloud server has high-quality data storage, on-demand service, data accessibility, shareability, and consistent data backup of massive data, the storage technologies and network environment include hardware resources and software management to minimize the maintenance cost and service response time. The emerging technologies advance the development of cloud computing to improve the quality of user experience and application services [10]. As a result, it allows computing devices to access cloud data remotely which adopts system resources such as computation, communication, and storage to enable large-scale data processing [11]. The intelligent system integrates a cloud storage service to manage extensive datasets of industrial applications. However, the applications are still challenging to offer better security and privacy in the management of remote data services [12]. A large quantity of datasets generated by IoT devices demands efficient shareability among different computing devices. The real-time entities utilize trusted third parties to store their data files on a cloud server.

Unfortunately, in a real-time application, cloud storage or third parties gain device access to collect the sensitive information of the users [13]. Thus, it is evident that sensitive data can easily be intruded under any mission-critical infrastructure by illegal users. By accessing the file, the entities such as cloud servers and an illegal user may acquire the information restricted to a particular data. In order to preserve data integrity, a straightforward approach is highly preferred. This approach can encrypt the user data before outsourcing it to the cloud server. However, a user wants relative searching techniques such as semantic, privacy-preserving, identity-based, etc. to solve the problem of intractability [14]. Zeng and Choo [15] designed a proxy re-encryption scheme for secure cloud storage systems. Their scheme constructs a conditional process to minimize computation cost and key size of the ciphertext. Hussain et al. [16] applied a sequence of binary bit and an XOR operation to develop an efficient encryption scheme. In their scheme, the IoT includes several stages to encrypt the data which consumes less time than traditional RSA.

Fan et al. [17] considered multi-linear mapping to design a proxy re-encryption with the dynamic condition. Their scheme allows the data owners to share the encrypted data using proxy on to the cloud. As a result, the data security issue is a key factor of the data owner to verify whether the outsourcing data is private to the cloud-server or not. Of late, the researchers have proposed various data encryption techniques [18–21] that guarantee secure data outsourcing. Lian et al. [18] utilized access control factors to design a proxy re-encryption scheme. Their scheme tries to build a system model to generate a key with multi-factor and weight value. Maiti et al. [19] employed a strategy of proxy re-encryption to present a privacy-preserving scheme. In their scheme, Lagrange interpolation is preferred to solve the computation cost of re-generation keys. Wu et al. [20] proposed identity-based proxy re-encryption using lattice-based cryptography. This mechanism applies pre-image sampling and double private-key to separate the execution of ciphertext transformation and decryption in order to generate a valid re-encryption key. Kim et al. [21] designed a proxy re-encryption scheme to optimize the resource usages including storage and network capacity.

This scheme enables data sharing and management to design a

lightweight device. However, the existing re-encryption techniques are still unavailable to construct a conventional keyword-based technique. Therefore, a searchable encryption technique is chosen which allows data users to execute the encrypted queries over stored data remotely. It provides security efficiency and flexibility to strengthen the verification process in the ciphertext environment. Of late, cloud computing has been more prevalent to examine the searching techniques such as multi-keyword ranking, fuzzy keywords, and similarity over encrypted data outsourcing. The authorized data users have sufficient network access to search outsourcing files that allow the users to search arbitrary keywords. It can obtain the eligible data files without applying for any control data access. In a real-time scenario, the data owner wishes to access the keyword queries to grant the privileges to the different data users. As an instance, a technical manager allows searching techniques to obtain the development process of the documents. Moreover, the developers rely on the current projects to prevent the company from accessing the financial statements.

The fine-grained data access control is not trivial to process by the data owner as the data can be outsourced to the remote cloud server in the form of encryption. Moreover, the provision of ciphertext retrieval considers the role of keyword trapdoor to complete a ciphertext search without accessing the entire documents of ciphertext. As a result, the bandwidth consumption can be preserved to accelerate the execution of ciphertext queries. However, most of the existing techniques cannot resist indistinguishable attack as they use a strategy of the deterministic trapdoor to complete ciphertext retrieval. Most importantly, searchable encryption techniques such as single keyword, multi-keyword, and fuzzy keyword linearly increase the complexity over the size of the encrypted/decrypted document. The storage systems such as public, private, and hybrid integrate searchable encryption to gain data security and privacy. It is worthy to note that hardware storage and system maintenance may cause severe physical threats to cloud storage. As to strengthen the security features of the storage systems, people prefer encrypted cloud before uploading sensitive data. At present, privacy preservation is treating as a serious issue to outsource cloud data.

1.1. Edge-Cloud in I-IoT

To provide a substantial solution, an edge-cloud design is preferred that has a comparable platform among energy computation and industrial applications i.e. based on the Internet of Things (IoT) [22]. To optimize the system computation, edge computing is suited that may closely associate with IoT objects to acquire the cloud services. This systematic process may offer instant caching to analyze the online data efficiently to meet the industrial demand i.e. Industry 4.0. [23]. Fig. 1 shows the architecture of edge-cloud in I-IoT that traditionally collects the raw data to synchronize with a cloud computing platform. Most IoT devices utilize edge applications to transmit industrial data to a central storage unit. The edge applications locate their own cloud center to process any real-time data which demands minimum latency to fulfill the requirements of cloud computing. The computing system prefers the edge of the network to build a robust infrastructure. It is widely comprised of industrial IoT devices, software applications, and network protocols to deliver any intellectual services. The industrial IoT includes sensing units, actuators, and smart devices to establish seamless interaction with data users. The edge of the network manages IoT devices to locate centralized access in the cloud. The centralized cloud solves the issue of data placement to minimize service latency. It uses a strategy of service allocation to manage the cloud services using software-defined networking.

Moreover, to analyze a huge amount of industrial data, the architecture of Edge-Cloud integrates on-demand computing services over a dedicated Internet such as a database, server, and web-based tools. This architecture handles a massive amount of data generated by IoT devices to manage the consumption of bandwidth, storage, and processing costs. It uses a technology of edge computing to offer service continuity and to manage the cloud networks. The computing tools such as edge device, control access, communication, and storage are legally distributed to process the system functions namely query task, delegate, collect data, and upload. However, a data manager may authorize the user to retrieve the cloud data due to storage limitations. In general, communication latency may involve a significant role between data managers and IoT devices to analyze the data services. Each IoT device may typically store the online data over an edge platform to authorize the data owner. Most of the applications include online data services over the flow of data such as transmission latency and data redundancies. A typical win-win strategy may be applied to mitigate the communication cost that restricts unnecessary data upload over a cloud platform. Therefore, cloud and edge computing may usually be honest but more curious. Traditionally, edge computing devices have fewer capabilities of intelligence

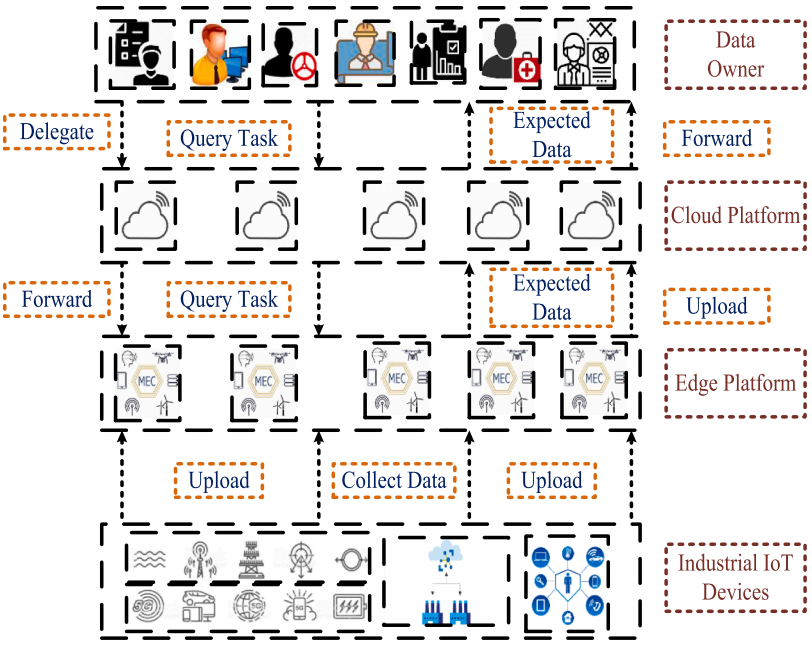

Fig. 1. An Architecture of Edge-Cloud in I-IoT.

to process local data such as data transmission, and feature extraction to the cloud servers.

1.2. Motivation

Edge computing devices demand machine learning techniques to improve system intelligence. It can offer a proper decision-making process without cloud intervention to protect sensitive data. To retrieve on-demand data precisely, the encryption technique is highly preferred. It can guarantee data confidentiality to improve the efficiency rate of the searching techniques including document frequency, word frequency, and vector model that makes the edge platform to distribute the computing nodes over a dedicated network. However, major issues such as data privacy and keyword search are yet to be solved. Opportunely, a technique known as public-key encryption with keyword search (PEKS) is widely used to address privacy and searching issues. Due to expensive computation costs, most of the existing schemes are still incongruous for industrial IoT devices. In the past, the diagnostic industries have practiced rapid development involving IoT and cloud computing. The technological objective is to enable cloud assistance efficiently that forms a set of wearable sensors to aggregate personal health information (PHI). The healthcare service providers (HSPs) associate with a medical patient to find the health status whereby a timely diagnosis may be provided. The integration of cloud edge with wearable IoT may significantly improve healthcare to mitigate the storage and computation cost.

Nevertheless, data privacy and file security play a major role due to the nature of sensitive data. File encryption i.e. PHI may preserve the medical file before transferring to the cloud server. But, it may not provide a complete solution for privacy preservation [24]. As a result, searching keywords i.e. medical data need to be in the form of encryption to offer a promising solution. A technology known as searchable encryption [25] may allow the user to search the keywords on encrypted files that convert the search index into encrypted form. Of late, several searchable encryption schemes [26] have been proposed that can only process a static dataset. Thus, it cannot be applied to the electronic healthcare (e-Health) system as it is dynamic. On the other hand, various dynamic searchable encryption schemes [27,28] may not directly support the e-Health system as the medical files are periodically generated to upload the data into the cloud. Generally, keyword partition has a high relevance but query processing relevant to keyword search plays an important role to examine the target partition.

Therefore, to enhance the search efficiency, a privacy preservation phrase with multi-keyword ranked searching (PPP-MKRS) is presented that introduces optimized filtering, binary tree index structure, and conjunctive keyword search. The major contributions are as follows:

1 Use a bisecting $k-Mean$ clustering, to generate a balanced keyword partition and index bit-vectors
2 Use a vector space model adopts to examine the metrics such as term frequency TF, and inverse document frequency I_{DF} over encrypted cloud data
3 Utilize secure $k-NN$ to analyze a high execution efficiency without loss of accuracy.
4 To attain the execution cost, a system with a multi-core processor is preferred that builds a balanced multi-mode searching.
5 To mitigate the computation overhead, the index vectors of all documents are separated level-wise before storing them in the tree.

The rest of the paper is prepared as follows: Section 2 discusses the relevant works of searchable and privacy-preservation-based authentication schemes. Section 3 shows a systematic model and the design requirements for the e-Health system. Section 4 presents the proposed PPP-MKRS scheme. Section 5 analyzes the important security properties of searching schemes. Section 6 demonstrates the experimental analysis using Phyton 3.6. Section 7 summarizes the outcomes of the state-of-the-art approaches. Section VII concludes the research work.

2. Related works

This section studies the relevant works of searchable and privacy-preservation-based encryption schemes. Of late, a network of the electronic healthcare system has been set up as a reliable application domain for the development of sensory technologies, cloud computing, and IoT. Healthcare applications significantly improve the availabilities of the networks to manage massive amounts of medical records. Most computing applications utilize a practical query service so-called pay-as-you-go to improve the quality of cloud-based services. A paradigm of service-oriented computing highly motivates the usages of data outsourcing to address the performance issues such as computation and reliability. However, the existing studies show that the cloud service models are vulnerable to several security threats such as phishing, spyware, account hijacking, and data breaches. The existing works are focused on keyword searches, multi-keyword searches, and searching based on access control to achieve s state of user personalization. Pitchai et al. [29] presented a file-sharing technique to address searchable encryption. Wang et al. [30] proposed multiuser encryption to provide a private secret key and to generate a trapdoor without the activities of the data owner or trusted third parties. Unfortunately, their schemes cannot trace the malicious activities that may leak the information of the decryption key to other users.

Xia et al. [31] employed an authorized and multi-keyword searching scheme using asymmetric encryption techniques. Their scheme may satisfy document confidentiality, collision resistance, and trapdoor unlinkability. Li et all. [32] presented a multi-keyword searching scheme to provide secure searching and accuracy over the mobile cloud data. Moreover, their scheme uses $k-nearest$neighbor and relevance score to meet the objective of multi-keyword searching. Jiang et al. [33] developed a verification searching scheme for a single keyword search that uses a specific data structure to achieve searching efficiency. Sun et al. [34] proposed an attributed-based keyword search that has search authorization and user revocation to outsource multiple data owners. Fan et al. [35] presented a verifiable scheme using an authentication tag that controls the server access. Wu et al. [36] developed a verifiable searching scheme using homomorphic encryption. Their scheme may generate an encrypted index structure to validate the searching results. Li et al. [37] addressed the issue of searchable encryption over a medical cloud. Cao et al. [38] utilized a bilinear mapping to build the access control list that uses a proxy server to generate the encrypted data.

Ren et al. [39] shown the technical challenges of privacy-preservation searching to address the significance of thing-fog-cloud architecture i.e. for IoT. Their architecture shares the secret key to authorize the user and to generate a query token. Since a user may gain access to recover the entire database, an access-control policy is tactfully set to update the secret key periodically by data owners. The searching results execute the query to return the most relevant files, which may apply a probabilistic trapdoor to resist a distinguishability attack. Xu et al. [40] designed a two-step ranking scheme that adopts ordered-preserving encryption over cloud encrypted data. Li et al. [41] developed a fine-grained multi-keyword searching over cloud encrypted data. Fortunately, their scheme can only operate boolean queries to improve the searching accuracy. Yang et al. [42] presented a fast privacy-preserving scheme to exploit the security features of multi-keyword searching. Their scheme can offer dynamic updates to maintain a better relevancy score between a query and a document. Xia et al. [43] adopted a balanced binary-tree index to explore the algorithmic strategies of dynamic multi-keyword searching schemes. Chen et al. [44] proposed privacy-preserving ranked searching to explore the clustering mechanism which can improve the searching efficiency. Fu et al. [45] designed a fuzzy-based multi-keyword searching scheme that uses location-sensitive hashing to adopt the technical feature of WordNet.

Wang et al. [46] developed a multi-keyword searching to explore the queries which order the privacy-preserving using locality-sensitive hashing. Fu et al. [47] presented a synonyms-based multi-keyword searching to realize the expansions of document keywords. Xia et al. [48] designed a semantic multi-keyword searching scheme to relate the libraries including document index and semantic relationship. Fu et al. [49] introduced several semantic-aware ranked searching schemes to adopt the features of semantic relationships. Most of the existing works introduce state-of-the-art approaches for public clouds. Yang et al. [50] proposed a searching scheme for hybrid clouds including public and private. In general, the public cloud acts as a trusted entity whereas the private cloud presumes to be honest but curious. The document keywords divide into several partitions to obtain unique document index vectors. The private cloud uses the document index vectors to hold the document identities. Accordingly, the public cloud finds the identities of the encrypted documents to classify the efficiency rate of the search keywords. Importantly, the coverage keywords influence the proportionality of searching efficiency over the number of partitions.

Wang et al. [51] introduced a secure keyword ranking scheme to record top-k relevant scores. Also, several ranked searching schemes have been introduced for key factors such as security and efficiency. However, their schemes cannot mitigate the computation cost to apply multi-keyword searching. Cao et al. [52] presented an asymmetric scalar privacy-preserving approach to support multi-keyword searching. However, their scheme cannot consider a weight for each keyword to improve the searching efficiency. Peng et al. [53] developed a keyword-balanced binary tree to construct an index structure. Moreover, it uses a multi-keyword searching scheme to meet the configuration setup of multi-ownership. Since the server of the semi-trusted cloud can easily snoop the keywords and trapdoor privacy, it can be prone o equivalence tests and keyword guessing attacks. Moreover, the malicious user may infer the receiver's public key to capture the generated ciphertext including trapdoor and keyword ciphertext. To provide better analysis, the key issues of searching such as single keyword, multi-keyword, single-owner, multiple owners, proxy, trapdoor privacy protection, and unlinkability are considered in Table 1. It is shown that the proposed PPP-MKRS scheme can support multi-keyword searching without the establishment of a proxy (Figs. 2 and 4).

Zhong et al. [54] introduced locality-sensitive hashing to achieve a privacy-aware system. Their scheme proposes a multi-dimensional ensemble-driven approach that prefers a set of candidate services to achieve a better quality of services such as response time and throughput. Guan et al. [55] discovered a cross-lingual multi-keyword searching to signify the use of language profiling. This scheme includes personalized searching to accelerate the sorting process. Xiao et al. [56] designed multi-keyword searching based on a mapping set that includes a private cloud server to match the keyword set over the query vectors. It may segment document index vector and query vector to minimize the processing cost. Cui et al. [57] presented an attribute-based multi-keyword searching to secure the encrypted cloud data. This scheme linearly scales the growth of service functionality to minimize the computation overhead of encrypted keywords. Najafi et al. [58] utilized symmetric searchable encryption to provide an optimal solution in terms of searching time, storage, and communication. Sangeetha et al. [59] applied attribute-based encryption to secure the personal health record of the patients. This scheme effectively retrieves the health data file to secure trustworthiness while any sensitive data is being shared in the cloud.

Niu et al. [60] developed a data-sharing scheme using multi-keyword searching. In their scheme, the techniques such as proxy re-encryption and searchable encryption are analytically unified to protect the private information of the patient. Hozhabr et al. [61] presented a dynamic secure multi-keyword searching to authorize document access in any operational environment. It can generate an index tree-based cluster technique to improve search efficiencies and to ensure the trustworthiness of the retrieving documents. Xu et al. [62] applied a modified Paillier encryption and secure k-NN computation to match and rank the diagnostic data files. It uses weighted Euclidean distance to obtain the Top-k files in diagnostics.

Table 1
Comparison of Multi-Keyword Searching Schemes.

Existing Schemes	KI_1	KI_2	KI_3	KI_4	KI_5	KI_6	KI_7
Fu et al. [45]	X	√	X	√	√	X	X
Wang et al. [46]	X	√	X	√	√	√	X
Fu et al. [47]	X	√	X	√	√	X	X
Fu et al. [49]	X	X	X	X	√	X	X
Yang et al. [50]	X	X	X	X	√	X	X
Wang et al. [51]	√	X	√	X	√	X	X
Cao et al. [52]	X	√	X	√	X	X	X
Peng et al. [53]	X	√	X	√	X	X	X
Xiao et al. [56]	X	√	X	√	X	√	X
Cui et al. [57]	X	√	√	√	X	√	X
Niu et al. [60]	X	√	X	X	√	X	X

KI_1: Single keyword searching; KI_2: Multi-keyword searching;.
KI_3: Single owner; KI_4: Multiple owners; KI_5: Proxy;.
KI_6: Trapdoor privacy protection; and KI_7: trapdoor unlinkability.

3. Models and design requirements

This section shows a systematic model for the e-Health system that defines different model elements and design goals.

3.1. System model

In e-Health, the wearable sensor devices collect the generated data in the encrypted medical files over IoT-gateway. Then, the medical files are forwarded to cloud storage i.e. *ServerA*. Importantly, this model obtains the files and their related queries to store in another cloud storage i.e. *ServerB*. This is to note that privacy preservation may be ensured in the use of multiple cloud servers. It comprises six real-time entities: 1. Data Owner $\langle D_O \rangle$; 2. IoT-Gateway $\langle G_{IoT} \rangle$; 3. *Cloud* − *ServerA*; 4. *Cloud* − *ServerB*; 5. Data Users $\langle D_U \rangle$; and 6. Trusted Authority $\langle T_A \rangle$. The real-time entities including IoT-gateway, cloud-server, data owner, and user guarantee data confidentiality to outsource the encrypted data files. It can build searchable indexes to enable efficient and secure access control over encrypted data. Each index creates a secure searching index to define the user types and policies. It authorizes data users that execute query trapdoor, which is based on encrypted keywords. Moreover, it uses attribute sets to infer the interested medical files from the cloud server. Upon execution of the query trapdoor, the searching index explores the cloud server to extract the encrypted data file. However, the associated attributes are verified with the access control policy to perform the query execution over the search index. Eventually, the cloud server returns the query response to the data users.

Data Owner $\langle \boldsymbol{D_O} \rangle$**:** Data owner outsources private and sensitive data to achieve convenient access, reliability, and on-demand data access to authorized users. To provide data privacy, D_O encrypts the medical documents using symmetric encryption techniques [12]. Each document creates the index vector that is based on the dictionary using a term frequency T_F. BMS index tree may be constructed using index vectors and document pool to enhance searching efficiency. To protect index tree privacy, the data owner encrypts the index tree before uploading them to *Cloud* − *ServerB*. D_O generates a query vector based on a dictionary and inverse document frequency (IDF) values that are linked to query keywords of D_U. To protect data and consumer privacy, D_O encrypts query vector, forms trapdoor, sends trapdoor and document decryption keys to D_U.

Data Users $\langle \boldsymbol{D_U} \rangle$**:** D_U sends the searching keywords to D_O and obtains a trapdoor corresponding to the searching keywords from D_O. D_O sends the trapdoor to *Cloud* − *ServerA* that obtains the top-ranking from the encrypted documents. Then, D_O decrypts the downloaded documents using decryption keys.

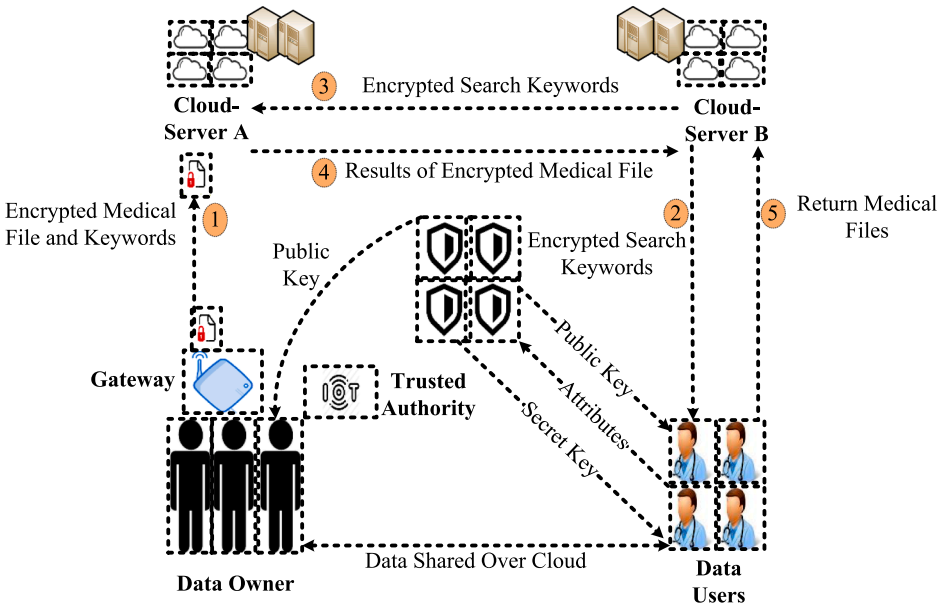

Fig. 2. Model of e-Health System.

Trusted Authority $\langle T_A \rangle$***:*** T_A collects the D_U attributes to generate the public keys and distribute the keys to other entities.

IoT-Gateway $\langle G_{IoT} \rangle$***:*** G_{IoT} collects the medical files from D_O to aggregate the medical data. Additionally, the keywords are extracted from the medical files to encrypt both files i.e. medical and keywords.

Cloud $-$ ***Server****: A*and *B* store the encrypted documents and the corresponding encrypted BMS tree received from D_O. *A*and *B* offer data access to authorized D_U. When the D_U sends trapdoor to *A*and *B, A*and *B* then search the trapdoors over BMS tree to yield top-ranked encrypted documents to D_U.

3.2. Threat model

T_A is assumed to be a trusted entity whereas the cloud servers i.e. *ServerA*and *ServerB* are designated to be honest but more curious to sense the private information of D_O. G_{IoT} considers as a secure entity to generate an encrypted medical file. Moreover, D_U acts as a medical professional to evaluate the medical data. *ServerA*and *ServerB* may be susceptible to compromise the integrity of real-time entity i.e. D_U. Hence, D_U should verify the veracity of medical files to claim that the real-time entities do not conspire. To acquire the supplementary information, the trapdoor and secure indexes utilize the phrase searching protocol. As a result, it would analyze the document to infer the location and keyword index. We consider two different threat models, which are already employed in [13].

Known Cyphertext Model: In this model, *ServerA*and *ServerB* may only identify the encrypted documents and the index vectors that are outsourced by D_O and the trapdoors provided by D_U. Moreover, they are capable to record the search history in the encrypted document.

Known Background Model: This model uses *ServerA*and *ServerB* to retain more knowledge rather than known ciphertext models, such as the relation between trapdoors and statistical information about the datasets. Also, they may infer query phrasing to collect the keyword frequencies.

3.3. Design requirements

In this paper, important design requirements are defined as follows:

Searchable Keywords: The proposed PPP-MKRS scheme achieves multi-keyword searching and their related frequencies. In opposition to other e-Health systems, the proposed PPP-MKRS may obtain frequency gaps in keyword ranges.

Data Sharing: D_O may periodically upload the medical files into *ServerA*. Later, the files may be shared to D_U to provide a proper medical diagnosis.

Data Verifiability: To extract the incorrect medical data, D_U should verify the document integrity and conformity of encrypted file contents.

Confidentiality of document pool: Using *ServerA*and *ServerB, *D_O stores the document pools whereas D_U accesses them. As a result, proper data confidentiality may be maintained among D_O and D_U to provide document privacy.

Index and trapdoor privacy protection: Assume that *ServerA*and *ServerB* are used to identify the content of the index and trapdoor in turn to learn the documented subjects. Importantly, the secure index cannot be inferred by *ServerA*and *ServerB* as it is subjected to the representation of an encrypted document. Therefore, the privacy of the document may be guaranteed once the keyword locations are well protected.

Trapdoor Unlinkability: *Cloud* $-$ *Server* cannot associate with the trapdoors to perform the phrase searching as it has a similar phrase for multiple queries. The documents storing in *ServerA*and *ServerB* may have searched for several times. However, *ServerA*and *ServerB* may not be learning about the search keyword information, which is accessed from trapdoors. Therefore, D_O use different trapdoors to generate the same set of search keywords.

4. Proposed PPP-MKRS

This section presents the vector space model, search model, relevance score, secure $k-NN$ computation, and dictionary formation to protect data authorization.

4.1. Fibonacci heap F_H

A mergeable-heap with a set of a heap-ordered tree is chosen to exploit the operations such as node insertion and extraction with the minimum keys [63]. It is used to implement the process effectively that introduces several key operations. They are as follows:

- Make-Heap () – Create a new heap without any key elements
- Insert () – Add a key element $\{x\}$ with a key to H, which takes constant storage time

- $EX_{MIN}(H)$ – Use to perform a deletion of a node $\{x\}$, which has a minimum key to return the pointer $\{x\}$ i..e. from the heap. It is a complex operation for a Fibonacci Heap F_H.

Shorter execution time may appeal to select a minimum number of elements from the given set.

4.2. Pseudo-Random permutation and function

A pseudo-random number may generate a fixed length to express the function as F: $\{0, 1\}^{\lambda} \times \{0, 1\}^* \rightarrow \{0, 1\}^*$. The adversaries use probabilistic polynomial-time to distinguish the pseudo-random permutation and function to build and protect the privacy of the nodes in the graph. Table 2 defines the important notations used in the proposed PPP-MKRS.

4.3. Paillier cryptosystem

It is an additive homomorphic cryptosystem to enable the arithmetic operation on the encrypted medical data that may result in operation consistency. Assume that two computation integers i.e. x_1 and x_2 are encrypted using the same secret-key k into the ciphertexts $E_k(x_1)$ and $E_k(x_2)$. As a result, additive homomorphism can be expressed as follows:

$$E_k(x_1).E_k(x_2) = E_k(x_1 + x_2)$$

In formal, three Paillier algorithms are shown below:

KeyGen: Two independent prime integers such as r_1 and $r_2$are randomly selected to obtain $N = (r_1.r_2)$; and $\phi(P_K) = (r_1 - 1).(r_2 - 1)$. Lastly, public key $P_K$and private key $\langle P_K,\phi(P_K)\rangle$are chosen.

Encryption: A random integer $r \in Z_N^*$ is chosen for a message $M_G \in Z_N$ that obtains the encrypted results as:

$$C = (1 + N)^{M_G}.r^N \left(mod\ N^2\right)$$

Decryption: Assume that $C = E_k(M_G)$ is selected to perform the encryption. As to decrypt the results, C with $\langle P_K,\phi(P_K)\rangle$is carefully chosen:

$$M_G = \left\langle \left(\left(C^{\varphi(P_K)}\ mod\ N^2\right) - 1\right) / N \right\rangle .\varphi(P_K)^{-1} (mod\ N)$$

$$MS\left(\overline{F}_{d,i}\right) = \sum_{t=1}^{i} S_t + \sum_{j=i+1}^{h} R_i \tag{1}$$

Where h is the total number of levels in the index tree; L_k is a list to store the top-ranked K document files in descending order i.e. S_d; DL_i is the list of index vectors storing the documents at i^{th} level; and A_k is the similarity score of K^{th} document file in L_k. Fig. 3 shows the flow structure of the proposed PPP-MKRS including vector space modeling, keyword relevance score, and query computation.

4.4. Vector space model

A vector space model adopts a secure multi-keyword search to examine the metrics such as term frequency TF, and inverse document frequency I_{DF}. The former term defines the number of times the keywords existing in the given document, whereas the latter divides the overall documents by many available documents in the existence of keywords or terms. Each medical document D_i describes n dimension vectors where n is the ordered reference of the keyword dictionary. $V_{D_i}[j]$ is used to store the normalized TF value of the keyword W_j as defined in Eq. 1.

$$V_{D_i}[j] = TF_{D_i,W_j} \Bigg/ \sqrt{\sum_{W_j \in D_i \wedge D_i \in D} \left(TF_{D_i,W_j}\right)^2} \tag{2}$$

For an execution query Q, n dimension query vector $V_Q$is used to store the normalized I_{DF}. The expression of $V_Q[j]$ is defined in Eq. 2:

$$V_Q[j] = I_{DF_{W_j}} \Bigg/ \sqrt{\sum_{W_j \in Q} \left(I_{DF_{W_j}}\right)^2} \tag{3}$$

4.5. Relevance score R_C

In a document, the term *'relevance'* signifies the number of times the query searching in a searchable document. It is widely employed in the searchable encryption technique, which retrieves the ranked search results. The metric for relevance score is meant as $TF_{I_{DF}}$. To measure the R_C among documents and searching requests, D_i and Q is assumed. It can be defined to calculate the inner product between V_{D_i} and V_Q:

$$R_C\langle V_{D_i}, V_Q\rangle = (V_{D_i}.V_Q) = \sum_{j=1}^{n} (V_{D_i}[j] \times V_Q[j]) \tag{4}$$

However, this paper deliberately uses TF to compute the size of keyword frequency which is completely depending on synonyms frequency from the searching documents. As referred to [15], the keyword relevance score is defined as follows:

$$R_C\left(W_j, TF_{D_i,W_j}\right) = \frac{1}{\left|TF_{D_i,W_j}\right|}\left(1 + \ln TF_{D_i,W_j}\right)\ln\left(1 + \frac{W_j}{TF_{D_i,W_j}}\right) \tag{5}$$

$$R_C\left(W_j, I_{DF_{W_j}}\right) = \frac{1}{\left|I_{DF_{W_j}}\right|}\left(1 + \ln I_{DF_{W_j}}\right)\ln\left(1 + \frac{W_j}{I_{DF_{W_j}}}\right) \tag{6}$$

4.6. Secure k − NN query computation

A secure k − NN Query Computation discusses a key specific feature of query protocol that initializes *ServerA* with Fibonacci-Heap $F_H$resulting in a heap list H_L. Specifically, it is used to store the encrypted k − NN that initiates a result with counter $M = 1$. It has an adjacent

Table 2
Important Notation Used in Proposed PPP-MKRS.

Parameter	Description
D_P	A document pool i.e. set of m documents denoted as $D_P = (d_1,d_2,\ldots\ldots, d_m)$
PD_i	Medical document
D_i	A collection of medical documents, comprising $D_i = \{d_1,d_2,\ldots\ldots, d_m\}$
V_{PD_i}	An n dimensional vector of medical documents d_i
V_{D_i}	A set of document vectors in D_i, $V_{D_i} = \{V_{D_1}, V_{D_2}, \ldots\ldots, V_{D_m}\}$
W	A keyword dictionary consisting of n keywords, $W = \{w_1,w_2,\ldots\ldots, w_n\}$
P_L	A list of keyword partitions, $P_L = \{P_{L1},P_{L2},\ldots\ldots, P_{LM}\}$
$V_{\overline{F}_{d_i}}$	An n dimension document filtering bit (DFB) vector d_i
V_{F_D}	A set of DFB vectors in medical documents, $V_{F_D} = \{V_{F_{d_1}}, V_{F_{d_2}}, \ldots\ldots, V_{F_{d_m}}\}$
D	The keyword-synonym dictionary of size $n \times t$, where n refers to the number of keywords and t represents the number of synonyms of each keyword. It is denoted as $D_{n \times t} = (k_{11},k_{12},\ldots\ldots, k_{1t}$ $k_{21},k_{22},\ldots\ldots, k_{2t}$ $\vdots$ $k_{n1},k_{n2},\ldots\ldots, k_{nt})$
W	A subset of keywords and synonyms of D in the search query
TF	A sum of keyword frequency and corresponding synonyms (in the dictionary) frequencies in the document
Q	Query vector for keywords or synonyms of data consumers to search in the cloud
T	An encrypted trapdoor that forms the query vector Q
$\overline{F}_{d,i}$	An index vector of the document at i^{th} level
S_i	Equate similarity score with RelevanceScore ($F_{d,i}$, Q_i)
Q_i	A query vector at i^{th} level
R_j	An inner product of G_i and Q_i at query generation phase
V_Q	An n dimension query vector of Q
C_D	A set of candidate documents i.e. for query D
$MS(\overline{F}_{d,i})$	A function to predict the maximum conceivable final relevance score from the index vector $F_{d,i}$

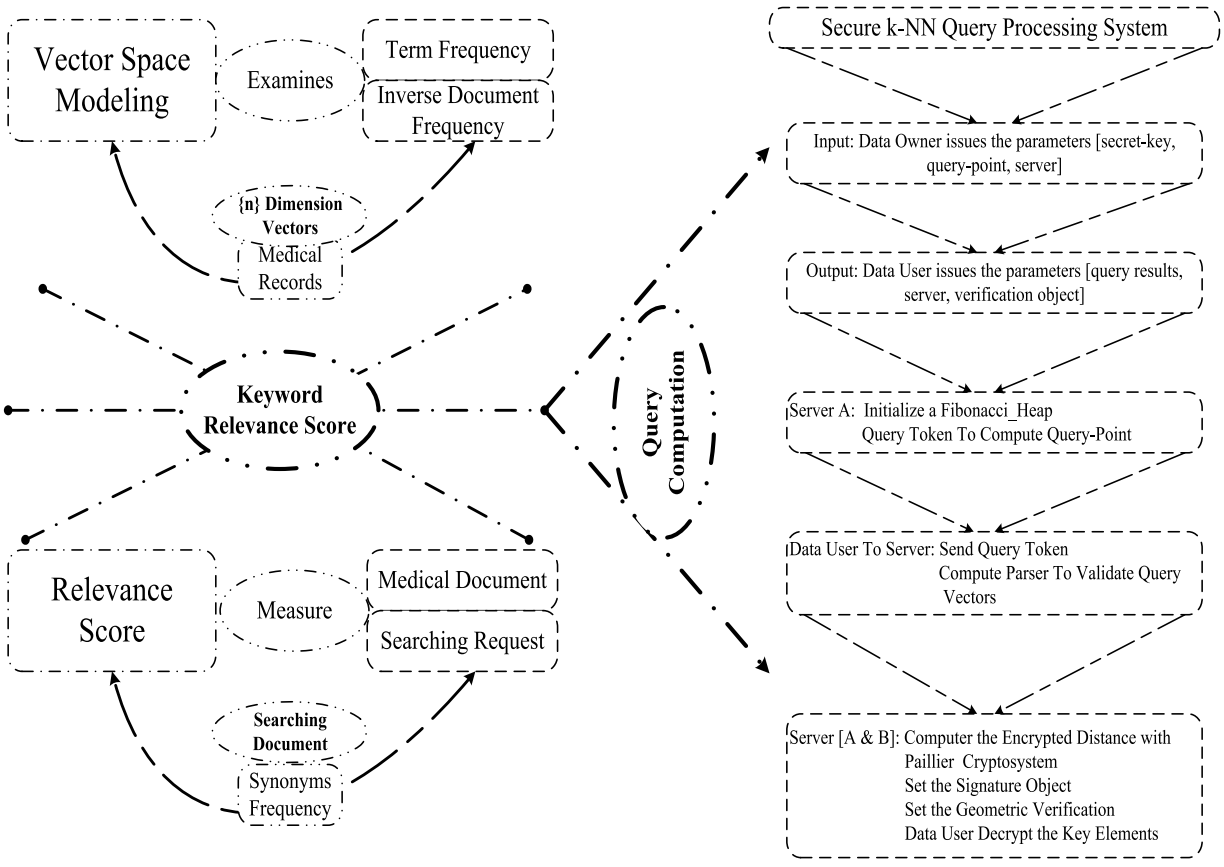

Fig. 3. Flow Structure of the Proposed PP-MKRS.

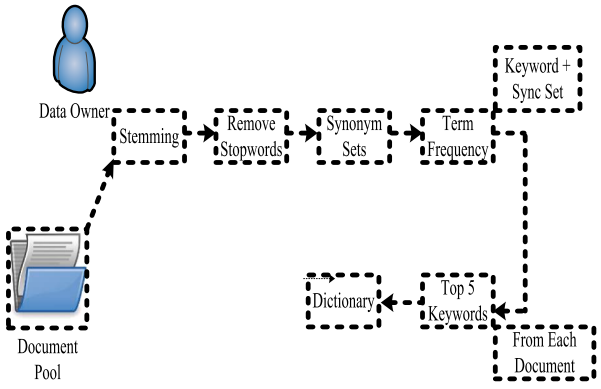

Fig. 4. Dictionary Formation – A Document Pool.

dictionary $D_{nbr}$with a size k, which stores the neighbor point of interest (PoI) in $k-$ NN.

To determine the initial PoI, the user may generate a query token i.e. q_{t1}, and q_{t2} with a query-point q_p. It will later send to *ServerA* to compute $q_{t1} \oplus q_{t2}$ that obtains $\langle x_1 \| x_2 \rangle$, where x_1 is the first encrypted NN of q. In the secure $k-$ NN query, the rest of the $(k-1)$ nearest PoI employs an iterative method to find $F_H$privately.

Each iteration involves a filtering mechanism to refine the M^{th} steps. They are as follows:

Step1: *ServerA* recovers the adjacency list involving the head pointer that may newly add the PoI i.e. M^{th} NN query.
Step2: The adjacency list retrieves the nodes to insert $F_H$with *Key* $(x_i \| y_i) = D_i$, where D_i defines encryption distance to the query.
Step3: *ServerA* runs $EX_{MIN}(H)$ to extract the nodes with minimum keys. It is set to encrypt $(M+1)^{th}$ NN query to add the set of encryption results H_L.
Step4: *ServerA* returns the authentic information to include k^{th} nearest PoI resulting in H_L. To verify the authentic data, the user should include V_{sign}, where V_{sign} is the modular signature multiplication of k nearest PoI i.e. for each vertex obtained from the adjacent neighbor.
Step5: Lastly, D_U collects the verification objects V to include the encryption results that correspond to the authentic information V_{sign} to validate H_L. This is to note that D_U may decrypt H_L with secret key s_k to collect the $k-$ NN query results. R, where $R = \{1^{st}NN, 2^{nd}NN, \ldots\ldots, k^{th}NN\}$.

The objective of the random vector generation is to guarantee the keyword anonymity of the document pool. The second step is to create two random invertible matrices M_1 and M_2 to encrypt the split vectors. Finally, (s_k, M_1, M_2) is used to act as a secret key. When a relevance score of a document file is computed for a query of data consumer, the index vector of a document and the query vector should be considered to use. To achieve privacy-preserving, the index vector and the query vector are encrypted using a secret key (s_k, M_1, M_2) and transfer to $Cloud-Server$. It computes the encrypted vectors without knowing the actual values including the document vector and query vector. Moreover, it provides the document score for the query.

It splits into two document vectors $\{d_i', d_i''\}$ and query vector q splits into two query vectors $\{q', q''\}$ based on bit-vector S. If j^{th} bit of S is equaled to 0, then $i'[j]$ and $i''[j]$ are set as the identical value as $i[j]$, whereas $q'[j]$ and $q''[j]$ are set as 0 and 1 respectively. The split index vectors may be encrypted as follows:

$$EN\ (i) = \left\{M_1^T.i',\ M_2^T.i''\right\} \tag{7}$$

The query vector pair may be encrypted as follows:

$$EN\ (q) = \ \left\{M_1^{-1}.q^{'},\ M_2^{-1}.q^{''}\right\} \tag{8}$$

Eq. (7) and Eq. (8) are used to compute the product of the index vector and the query vector that produces a document score to the query. It is as follows:

$$Score\ = EN\ (p)\ \times\ EN\ (q)$$

$$= \left\{M_1^T.i^{'},\ M_2^T.i^{''}\right\} \times \left\{M_1^{-1}.q^{'},\ M_2^{-1}.q^{''}\right\}$$

$$= M_1^T.i^{'}.\ M_1^{-1}.q^{'} + M_2^T.i^{''}.\ M_2^{-1}.q^{''}$$

$$= \left(i^{'T}.M_1 \times M_1^{-1}.q^{'}\right) + \left(i^{''T}.M_2 \times M_2^{-2}.q^{''}\right)$$

$$= \left(i^{'T}.q^{'}\right) + \left(i^{''T}.q^{''}\right)$$

$$= i^T.q$$

$$= RelevanceScore(i,q) \tag{9}$$

This is to note that the relevance score of unencrypted vectors is very similar to encrypted vectors. Algorithm 1 shows the execution steps of secure $k-$ NN query computation.

Algorithm 1
Secure $\boldsymbol{k-NN}$ *Query.*

: D_O provides the input parameters such as secret-key s_k, query-point q_p, and *ServerA*
O_P: D_U provides query results R, *ServerA*, and verification object V
ServerA: Initialize a Fibonacci-Heap $F_H$resulting in a
  heap list H_L
  Consider a counter $M = 1$ with an adjacent
  dictionary $D_{nbr}$with a size k
ServerA: Consider a query token i.e. q_{t1}, and q_{t2}
  with a query-point q_p to compute
  (q_{t1},q_{t2}): $=(P_{k1}(q_p),G_{k2}(q_p))$
D_U To *ServerA*: Send the query token $q_t = (q_{t1},q_{t2})$
D_U: Compute $\langle x_1 \| x_2 \rangle = D_{1\ -\ NN}(q_{t1} \oplus q_{t2})$
D_U: Set $P_{k1}(1^{st}NN) = x_1$
D_U: Insert $P_{k1}(1^{st}NN)$ into H_L
while $(M < k)$ do
ServerA: Compute $\langle Addr_1 \| k_p \rangle = D_{Head}[P_{k1}(1^{st}NN)] \oplus y$
ServerA: Parse $A_{rr}[Addr_1]$ as $\langle N_1^{'}, r_1 \rangle$
ServerA: Compute N_1: $=N'_1 \oplus H(k_p, r_1)$
while $Addr_1 \neq NULL$ do
ServerA: Parse N_i as $(x_i \| y_i \| Addr_{i+1})$
ServerA & *ServerB*: Compute the encrypted
  Distance with Paillier cryptosystem:
  $D_i = \min\{D_1.D_2 | (C,D_1) \in D_{H_L}\langle q_{t1}\rangle, (C,D_2) \in D_{H_L}\langle x_i\rangle\}$
ServerA & *ServerB*: Insert $\langle H, x_i \| y_i \rangle$ with $k\langle x_i \| y_i \rangle = D_i$
ServerA: Insert (x_i, D_i) to the neighbor dictionary $D_{nbr}$with $[P_{k1}(M^{th}NN)]$
ServerA: Parse $A_{rr}[Addr_{i+1}]$ as $\langle N_{i+1}^{'}, r_{i+1} \rangle$
ServerA: Compute N_{i+1}: $=N'_{i+1} \oplus H(k_p, r_{i+1})$
ServerA: Set $i = i + 1$
end while
ServerA & *ServerB*: Parse $EX_{MIN}(H)$ as $\langle x \| y, Key(x \| y) \rangle$
ServerA: Set $M = M + 1$
ServerA: Set $P_{k1}(M^{th}NN) = x$
ServerA: Insert $P_{k1}(M^{th}NN)$ into H_L
end while
Each operation demands a security comparison between *ServerA* & *ServerB* to choose two minimum encrypted data. It is used to process the interaction between *ServerA* & *ServerB*.
ServerA: Set the signature object:

$$V_{sign} = \prod_{M=1}^{k} S_{Pol}[P_{k1}(M^{th}\ NN)]\ [mod\ N]$$

ServerA: Set the geometric verification:
  $V_{geo} = [S_{1\ -\ NN}(q_{t1}), D_{nbr}]$
ServerA: Return $V = \langle H_L, V_{sign} \rangle$ to D_U
D_U: Decrypt the key elements in H_L to collect the $k-NN$ results in R

4.7. Verify $k-$ NN query

In $k-$ NN verification, *Cloud* $-$ *Server* may attempt to return some incorrect results. Therefore, query verification is highly demanded to validate the expected outcome. In general, $k-$ NNquery has a significant procedure such as signature verification, where D_U creates an encrypted query to provide a verification object V i.e. for *ServerA*. V contains the encrypted H_L to apply an authentic signature V_{sign}. Algorithm 2 shows the verified $k-$ NN query.

4.8. Dictionary formation D_{nbr}

We consider a publicly available document pool that finds the root of every term with a well-known stemming method called the Porter stemming algorithm [64]. Each document pool shows a regular set of important keywords. It extracts the important keywords to increase the searching efficiency as shown in Fig 3. It is observed that the first step is to translate each term into a lower case to determine the root of each term. The second step is to remove the stop words. Next, we find the synonym set of each term using WordNet. In the next step, to extract keywords in each document, we compute $TF_{I_{DF}}$ of each term provided in Eq. (6). The TF is used to calculate the sum of the frequencies i.e. for term and frequency of corresponding synonyms in the document pool. Importantly, the keywords are sorted in descending order to select the first 5 words as the main keywords of the corresponding document. Eventually, the dictionary with all selected keywords is created to represent the whole document pool with the corresponding synonyms.

4.9. Trapdoor generation

$$(V_{D_i}, V_Q) \leftarrow T_G\left(R_C,\ W_j\right)$$

With the query keywords of the data consumer, D_O engenders the query vector based on the generation of query keywords, When the keyword is available in D_{nbr}, I_{DF} values of the keyword are placed in the corresponding dimension of the query vector. Otherwise, it is set to be zero. The query vector is encrypted using Eq. (2) and Eq. (3) to send the search access control i.e. for D_O. T_G has the highest relevance score $R_C(W_j, I_{DF_{W_j}})$ at each level of an index vector to D_U. lastly, D_U submits query vector to *cloudserver*.

5. Security analysis

This section analyzes the important security of the proposed PPP-MKRS to enrich the privacy constraint.

5.1. Document confidentiality

The document and the corresponding vectors are forcibly encrypted to outsource the data over an encrypted cloud. The secure $k-NN$ query is intellectually created to sense the encrypted data that authorizes the activities of D_O. It uses a specific signature algorithm to secure the internal product operation with k^{th} nearest PoI resulting in H_L to verify the data authenticity. Since the secret key s_k is privately shared to D_O through D_U authorization, the *ServerA*, and *ServerB* cannot collect any confidential parameters to infer s_k. Therefore, it is computationally infeasible to determine the information of medical files over *cloudserver*. Hence, the proposed PPP-MKRS guarantees data confidentiality.

5.2. Index and trapdoor privacy protection

Trapdoor may be generated periodically to perform a secure $k-NN$ query that uses secret-key s_k and query-point q_p to determine the secret key s_k shared by D_O and D_U. Moreover, several random integers such as x, y, and r are chosen to generate the trapdoor process, which may add

more random values in index vectors. Without knowing the secret key s_k, it is more complex to deduce the actual query vector. Hence, the proposed PPP-MKRS can achieve the privacy of the query vector and trapdoor.

5.3. Trapdoor unlinkability

A trapdoor may generate a similar query to analyze the probability under a known-background model that can extend the query vector into $\langle n + H_L + 1 \rangle$ bit dimension. Moreover, it uses parameters such as P_{k_r}, s_k, and s_{k_p} to perform the multiplication i.e. $(S_{1\ -\ NN}[P_{k1}(q)])^e \neq H(q\|1 - NN)(modN)$. It has a possible query to generate $P_{k_r} = 1/(x \times 2^q)$ that determines whether it can achieve a larger denominator and smaller P_{k_r}. Assume that q is a parameter whose size is 1024 bits. Then, the size of the query i.e. $P_{k_r} < 1/2^{1024}$, which is considered to be negligible. Therefore, the proposed PPP-MKRS can achieve the property of unlinkability.

6. Result analysis

This section demonstrates the experiential analysis of the proposed PPP-MKRS scheme with other searchable encryption schemes [6,8,17] over encrypted cloud data. An $1024 - bits$ Paillier cryptosystem has been implemented using Python 3.6 that compares the performance metric such as verification time among the proposed and existing schemes [25,27,36,61,62]. The system is capable of a $3.60GHz$ Intel Core i7–4790 processor, and Windows 8.1 operating system with 16 GB RAM. We have conducted an extensive analysis of the public dataset [65] that uniformly distributes the densities d i.e. 1% to 10% [18]. As to analyze the public dataset, an average execution time of ~ 100 is chosen. Each file has the number of keywords in the dictionary $\langle d \rangle$ and trapdoor $\langle n \rangle$ to examine the computation and storage costs.

Fig 5[A] shows the comparison of computation overhead over the number of keywords in terms of the trapdoor. When $d = 100$ and $n = 10 \sim 50$ are considered to analyze the computation cost, it is observed that the proposed PPP-MKRS has less execution time to operate the encryption process including trapdoor and retrieval than other existing schemes [25,27,36,61,62]. Moreover, we can observe that the execution time including encryption and retrieval is linearly growing over the number of keywords for the analysis of trapdoor and dictionary. It considers the time cost to examine the trapdoor and encryption algorithm to verify whether there is a relationship with the available keywords in the trapdoor or not. Fig 5[B] shows the comparison of computation overhead over the number of keywords in terms of dictionary. When $d = 10 \sim 50$ and $n = 10$ are utilized to analyze the execution time such as encryption, and trapdoor, it is observed that the proposed PPP-MKRS has less computation time to learn the encryption process including trapdoor than other existing schemes [25,27,36,61,62]. Moreover, we can observe that the operational processes such as encryption and trapdoor linearly grow with the available number of keywords in the dictionary. However, it can be more stable irrespective of the keywords available in the dictionary.

Fig 6[A] and 6 [B] show the comparison of storage overhead over the number of keywords in terms of the trapdoor. The examination result reveals that the proposed PPP-MKRS has less storage cost than other existing schemes [25,27,36,61,62]. Moreover, it has the operational parameters such as trapdoor size, parameter size, and ciphertext size to examine the given settings such as $d = 100$, $n = 10 \sim 50$, $d = 10 \sim 50$, and $n = 10$. Moreover, it is evident that the proposed PPP-MKRS linearly grows over the number of keywords in terms of trapdoor and dictionary to realize the storage sizes such as trapdoor and ciphertext. Above all, the proposed PPP-MKRS has less computation and storage efficiencies to meet the practical constraints of big data applications. Fig 6[B] shows the verification time over a number of users.

From Fig. 7, it is observed that a survey was conducted on the given dataset i.e. $k = 16$ search. According to query processing, the medical files are returned. In the experiment, the PoI densities are chosen to be 5% to acquire the verification time over V_{sign}. In the proposed PPP-MKRS, the time for trapdoor generation completely depends on the number of keywords in the dictionary and the query but not the number of documents in the document pool. Therefore, the proposed scheme can execute the queries in parallel in the multicore system in comparison with other existing schemes [6,8,17]. Assume that one processor executes on the root, then the other nodes may execute on the other processors in parallel without any queueing delay, whereby improves the search efficiency.

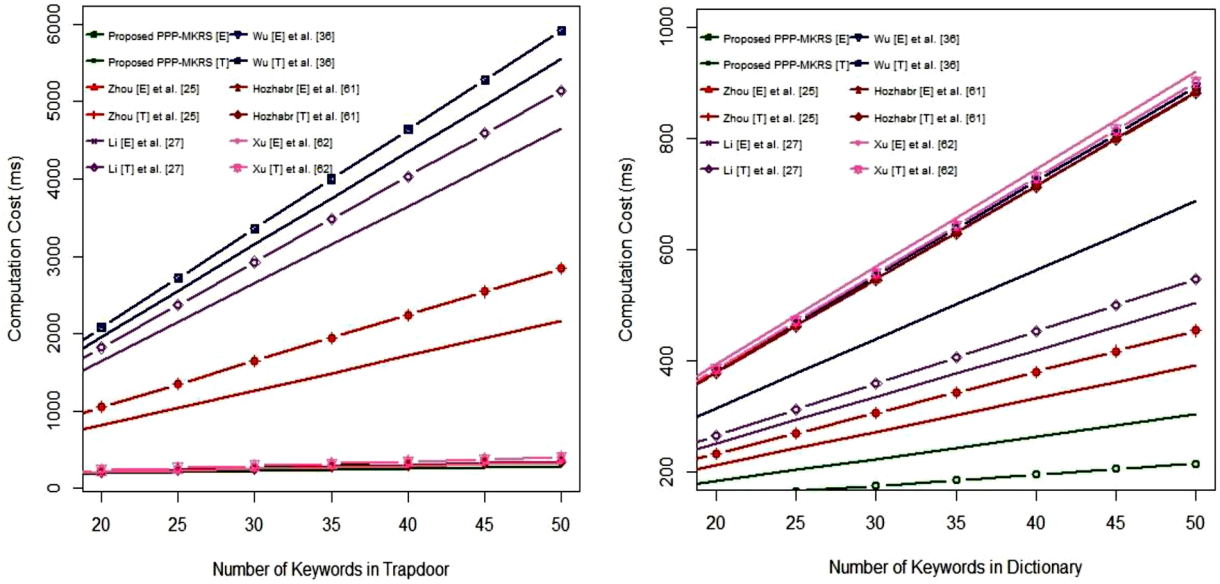

Fig. 5. [A] Computation cost $\langle ms \rangle$ versus the number of keywords in the trapdoor. [B] Computation cost $\langle ms \rangle$versus the number of keywords in the dictionary.

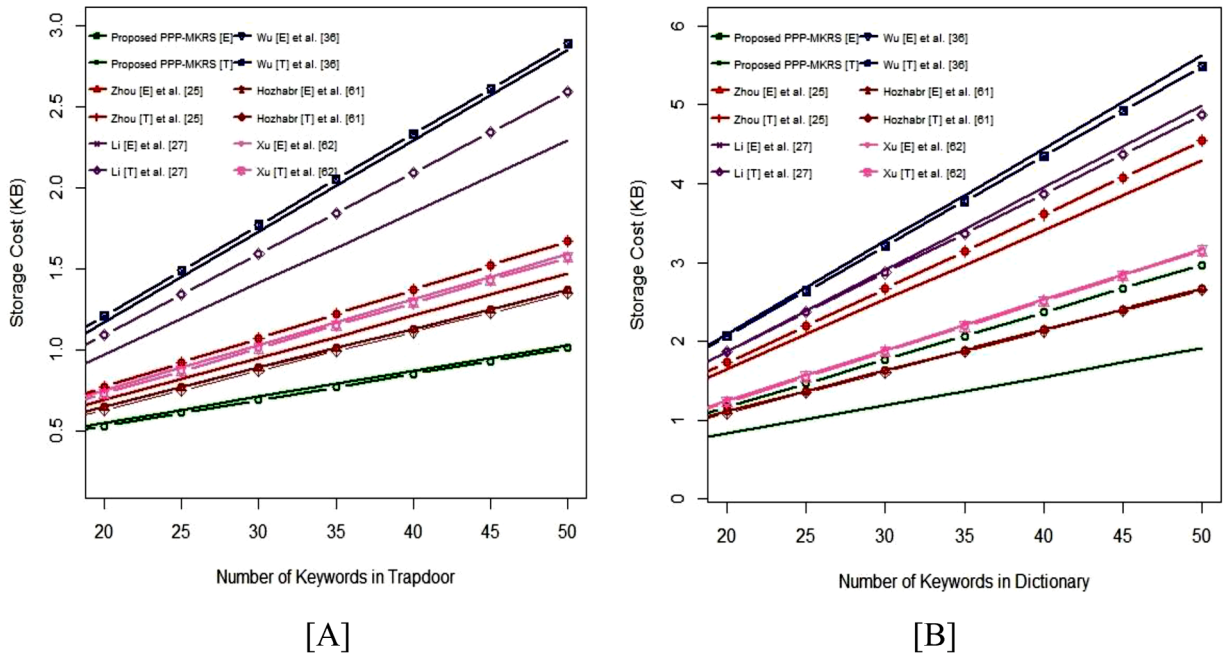

Fig. 6. [A] Storage cost $\langle KB \rangle$ versus the number of keywords in the Trapdoor. [B] Storage cost $\langle KB \rangle$ versus the number of keywords in the Dictionary.

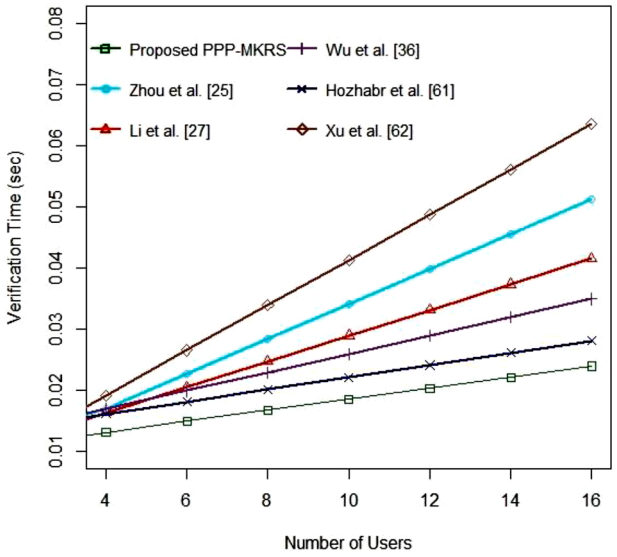

Fig. 7. Verification time $\langle sec \rangle$ versus the number of users.

7. Discussion

The evolving technologies including wireless personal and local area networks, wireless wide area networks, and unlicensed long-range technologies signify the roles of IoT to promote smart intelligence, tracking, and monitoring [66]. Of late, I-IoT has played a crucial role to offer a powerful computing system. The system may exploit the features of the distributed system to evolve a paradigm known as 'computing-as-a-service' to realize resource utilization. Due to the increasing demand for computing resources, the data owners prefer to upload their computed data to the cloud servers. The emerging technologies can handle massive computation and storage to process the user requests dynamically [67]. Users may use computational resources to process the industrial data in real-time. They use sensing devices such as radio frequency identification and global positioning system to optimize resource utilization and to improve the quality of experiences. I-IoT standardizes the technological guidance to develop a potential application system [68]. Nowadays, it is growing exponentially to manage and utilize the massive amount of industrial data. It may use a cloud service provider to improve storage capacity and analytical capabilities.

The service providers can effectively analyze and mine the industrial data to offer better intelligence to the industrial sectors such as logistics and manufacturing. Moreover, the data users may exploit the features of cloud service providers to offer better scalability and resource optimization [69]. However, data security and privacy are seriously challenged over an insecure network. As an instance, an adversary may overhear on any transmitted data to infer the intricacy of the production units. On the other hand, the service providers may misuse the sensitive data of data users to gain some illegal profits or to restrict the privileges of data outsourcing. As a result, a privacy-preserving strategy is highly demanded to optimize the data utilization of I-IoT [70,71]. In order to protect the information about an enterprise, the service providers exploit a technique of data encryption. Unfortunately, the traditional encryption techniques cannot guarantee data privacy to process and submit confidential data to the cloud servers. It is worthy to note that the original data structure will be altered once the encryption technique is applied. Therefore, a searching algorithm for plaintext will not be preferable for encrypted data contents. To address the issue effectively, this paper prefers multi-keyword searching with privacy-preserving. It uses secure k-NN computation, vector spacing, and relevance score not only to minimize computation cost but also to enhance the storage capacity of healthcare service providers.

8. Conclusion

The cybersecurity applications for IoT demand the development of an AI-enabled trustworthy model. The trustworthy models can integrate with sensors, actuators, and medical diagnostics to fulfill the security goals including data confidentiality,integrity, and confidentiality. Thus, in this paper, the PPP-MKRS scheme has been proposed for e-Health systems. To examine the metrics such as term frequency *TF*, and inverse document frequency I_{DF} over encrypted cloud data, a vector space model was adopted. Moreover, a secure $k - NN$ was constructed to analyze a high execution efficiency without loss of accuracy. To attain better verification costs, a system with a multicore processor was built. The

security analysis proves that the proposed PPP-MKRS fulfills the desirable properties such as confidentiality, privacy, and trapdoor unlinkability. Finally, the performance analysis demonstrates that the proposed PPP-MKRS can execute the queries in parallel in the multicore system without queueing delay to enhance efficiency factors such as computation, storage, and verification cost. In the future, superior functionalities such as optimization problems and context-aware models will be incorporated with multi-keyword searching techniques to achieve the standard requirements of cybersecurity applications. In addition, we will utilize a weighted Euclidean distance through secure k-NN to find the Top-k diagnostic data files. As to restrict the injection of uncorrected file formats, a technique known as message authentication codes will be employed. It will verify the integrity of data files and proof of correctness to examine the properties of privacy preservation.

Conflict of interest and authorship conformation form

Please check the following as appropriate:

- Deebak B D has participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.
- Fida Hussain Memon, Nawab Muhammad Faseeh Qureshi, Kapal Dev, and Sunder Ali Khowaja have participated in (a) system model, or analysis and interpretation of the data; (b) revising the drafting of research article or revising it critically for important intellectual content; and (c) approval of the final version.
- This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.
- We do have affiliations with organizations with direct or indirect financial interest in the subject matter discussed in the manuscript:

Declaration of Competing Interest

None.

References

[1] Han, C., Wu, Y., & Chen, Z. (2018). Network 2030 a blueprint of technology, applications and market drivers towards the year 2030 and beyond.

[2] M. Katz, M. Matinmikko-Blue, M. Latva-Aho, 6Genesis flagship program: building the bridges towards 6G-enabled wireless smart society and ecosystem, in: 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), IEEE, 2018, pp. 1–9.

[3] K.M.S. Huq, S.A. Busari, J. Rodriguez, V. Frascolla, W. Bazzi, D.C. Sicker, Terahertz-enabled wireless system for beyond-5G ultra-fast networks: a brief survey, IEEE Netw. 33 (4) (2019) 89–95.

[4] P. Yang, Y. Xiao, M. Xiao, S. Li, 6G wireless communications: vision and potential techniques, IEEE Netw. 33 (4) (2019) 70–75.

[5] Parus Khuwaja, Sunder Ali Khowaja, Kapal Dev, Adversarial Learning Networks for FinTech applications using Heterogeneous Data Sources, IEEE Internet of Things J. (2021).

[6] K. Dev, S.A. Khowaja, P.K. Sharma, B.S. Chowdhry, S. Tanwar, G. Fortino, DDI: a novel architecture for joint active user detection and IoT device identification in grant-free NOMA systems for 6G and beyond networks, IEEE Internet of Things J. (2021).

[7] T. Wang, Y. Quan, X.S. Shen, T.R. Gadekallu, W. Wang, K. Dev, A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things, IEEE Trans. Ind. Inf. (2021).

[8] Z. Xu, D. He, H. Wang, P. Vijayakumar, K.K.R. Choo, A novel proxy-oriented public auditing scheme for cloud-based medical cyber-physical systems, J. Inf. Secur. Appl. 51 (2020), 102453.

[9] K. Inokuchi, K. Kourai, Secure VM management with strong user binding in semi-trusted clouds, J. Cloud Comput. 9 (1) (2020) 1–22.

[10] C. Li, J. Bai, Y. Chen, Y. Luo, Resource and replica management strategy for optimizing financial cost and user experience in edge cloud computing system, Inf. Sci. (Ny) 516 (2020) 33–55.

[11] Khowaja, S.A., Dev, K., Qureshi, N.M.F., Khuwaja, P., & Foschini, L. (2021). Towards Industrial Private AI: a two-tier framework for data and model security. arXiv preprint arXiv:2107.12806.

[12] S. Sicari, A. Rizzardi, A. Coen-Porisini, 5 G In the internet of things era: an overview on security and privacy challenges, Comput. Netw. 179 (2020), 107345.

[13] R. ALmarwani, N. Zhang, J. Garside, An effective, secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage, PLoS One 15 (11) (2020), e0241236.

[14] H.Y. Lin, Y.M. Hung, An Improved Proxy *Re*-Encryption Scheme for IoT-Based Data Outsourcing Services in Clouds, Sensors 21 (1) (2021) 67.

[15] P. Zeng, K.K.R. Choo, A new kind of conditional proxy re-encryption for secure cloud storage, IEEE Access 6 (2018) 70017–70024.

[16] I. Hussain, M.C. Negi, N. Pandey, Proposing an encryption/decryption scheme for IoT communications using binary-bit sequence and multistage encryption, in: 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), IEEE, 2018, pp. 709–713.

[17] C.I. Fan, Y.F. Tseng, Y.L. Huang, Key-aggregate proxy re-encryption with dynamic condition generation using multilinear map, in: 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, 2020, pp. 9–15.

[18] Z. Lian, M. Su, A. Fu, H. Wang, C. Zhou, Proxy re-encryption scheme for complicated access control factors description in hybrid cloud, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–6.

[19] S. Maiti, S. Misra, P2B: privacy preserving identity-based broadcast proxy re-encryption, IEEE Trans. Veh. Technol. 69 (5) (2020) 5610–5617.

[20] L. Wu, X. Yang, M. Zhang, L. Liu, New identity based proxy re-encryption scheme from lattices, China Commun. 16 (10) (2019) 174–190.

[21] S. Kim, I. Lee, IoT device security based on proxy re-encryption, J. Ambient Intell. Humaniz. Comput. 9 (4) (2018) 1267–1273.

[22] M.A. Jarwar, S.A. Khowaja, K. Dev, M. Adhikari, S. Hakak, NEAT: a resilient deep representational learning for fault detection using acoustic signals in IIoT environment, IEEE Internet of Things J. (2021).

[23] L.D. Xu, L. Duan, Big data for cyber-physical systems in industry 4.0: a survey, Enterprise Inf. Syst. 13 (2) (2019) 148–169.

[24] C. Liu, S. Zhou, H. Hu, Y. Tang, J. Guan, Y. Ma, CPP: towards comprehensive privacy preserving for query processing in information networks, Inf. Sci. (Ny) 467 (2018) 296–311.

[25] R. Zhou, X. Zhang, X. Du, X. Wang, G. Yang, M. Guizani, File-centric multi-key aggregate keyword searchable encryption for industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (2018) 3648–3658.

[26] M. Shen, B. Ma, L. Zhu, X. Du, K. Xu, Secure phrase search for intelligent processing of encrypted data in cloud-based IoT, IEEE Internet of Things J. 6 (2) (2018) 1998–2008.

[27] J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, W. Lou, Searchable symmetric encryption with forward search privacy, IEEE Trans. Dependable Secure Comput. (2019).

[28] Q. Liu, Y. Tian, J. Wu, T. Peng, G. Wang, Enabling verifiable and dynamic ranked search over outsourced data, IEEE Trans. Serv. Comput. (2019).

[29] R. Pitchai, S. Jayashri, J. Raja, Searchable encrypted data file sharing method using public cloud service for secure storage in cloud computing, Wirel. Pers. Commun. 90 (2) (2016) 947–960.

[30] H. Wang, X. Dong, Z. Cao, Secure and efficient encrypted keyword search for multi-user setting in cloud computing, Peerto-Peer Netw. Appl. (2017) 1–11.

[31] H. Li, D. Liu, K. Jia, X. Lin, Achieving authorized and ranked multi-keyword search over encrypted cloud data, in: IEEE International conference on in communications (ICC), 2015, pp. 7450–7455.

[32] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 27 (2016) 340–352.

[33] X. Jiang, J. Yu, J. Yan, R. Hao, Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data, Inf. Sci. 403 (2017) 22–41.

[34] W. Sun, S. Yu, W. Lou, Y.T. Hou, H. Li, Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud, IEEE Trans. Parallel Distrib. Syst. 27 (2016) 1187–1198.

[35] Y. Fan, Z. Liu, Verifiable attribute-based multi-keyword search over encrypted cloud data in multi-owner setting, in: IEEE Second International conference on data science in cyberspace (DSC), 2017, pp. 441–449.

[36] D.N. Wu, Q.Q. Gan, X. Wang, Verifiable public key encryption with keyword search based on homomorphic encryption in multiuser setting, IEEE Access 6 (2018) 42445–42453.

[37] H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, Y. Xiang, Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data, IEEE Trans. Cloud Comput. (2017).

[38] L. Cao, Y. Wang, X. Dong, Y. Liu, Y. Zhang, X. Guo, T. Feng, Multiuser access control searchable privacy-preserving scheme in cloud storage, Int. J. Commun. Syst. 31 (9) (2018) e3548.

[39] H. Ren, H. Li, Y. Dai, K. Yang, X. Lin, Querying in internet of things with privacy preserving: challenges, solutions and opportunities, IEEE Netw. 99 (2018) 1–8.

[40] J. Xu, W. Zhang, C. Yang, J. Xu, N. Yu, Two-step-ranking secure multi-keyword search over encrypted cloud data, in: 2012 International Conference on Cloud and Service Computing, IEEE, 2012, pp. 124–130.

[41] H. Li, Y. Yang, T.H. Luan, X. Liang, L. Zhou, X.S. Shen, Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data, IEEE Trans. Dependable Secure Comput. 13 (3) (2015) 312–325.

[42] C. Yang, W. Zhang, J. Xu, J. Xu, N. Yu, A fast privacy-preserving multi-keyword search scheme on cloud data, in: 2012 International Conference on Cloud and Service Computing, IEEE, 2012, pp. 104–110.

[43] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 27 (2) (2015) 340–352.

[44] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A.Y. Zomaya, An efficient privacy-preserving ranked keyword search method, IEEE Trans. Parallel Distrib. Syst. 27 (4) (2015) 951–963.
[45] Z. Fu, X. Wu, C. Guan, X. Sun, K. Ren, Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement, IEEE Trans. Inf. Forensics Secur. 11 (12) (2016) 2706–2716.
[46] J. Wang, X. Yu, M. Zhao, Privacy-preserving ranked multi-keyword fuzzy search on cloud encrypted data supporting range query, Arabian J. Sci. Eng. 40 (8) (2015) 2375–2388.
[47] Z. Xia, Y. Zhu, X. Sun, L. Chen, Secure semantic expansion based search over encrypted cloud data supporting similarity ranking, J. Cloud Comput. 3 (1) (2014) 1–11.
[48] Z. Fu, X. Sun, N. Linge, L. Zhou, Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query, IEEE Trans. Consum. Electron. 60 (1) (2014) 164–172.
[49] Z. Fu, L. Xia, X. Sun, A.X. Liu, G. Xie, Semantic-aware searching over encrypted data for cloud computing, IEEE Trans. Inf. Forensics Secur. 13 (9) (2018) 2359–2371.
[50] Y. Yang, J. Liu, S. Cai, S. Yang, Fast multi-keyword semantic ranked search in cloud computing, Chin. J. Comput. 41 (6) (2018) 1126–1139.
[51] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, Secure ranked keyword search over encrypted cloud data, in: 2010 IEEE 30th international conference on distributed computing systems, IEEE, 2010, pp. 253–262.
[52] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-preserving multi-keyword ranked search over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 25 (1) (2013) 222–233.
[53] T. Peng, Y. Lin, X. Yao, W. Zhang, An efficient ranked multi-keyword search for multiple data owners over encrypted cloud data, IEEE Access 6 (2018) 21924–21933.
[54] W. Zhong, X. Yin, X. Zhang, S. Li, W. Dou, R. Wang, L. Qi, Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment, Comput. Commun. 157 (2020) 116–123.
[55] Z. Guan, X. Liu, L. Wu, J. Wu, R. Xu, J. Zhang, Y. Li, Cross-lingual multi-keyword rank search with semantic extension over encrypted data, Inf. Sci. (Ny) 514 (2020) 523–540.
[56] T. Xiao, D. Han, J. He, K.C. Li, R.F. de Mello, Multi-Keyword ranked search based on mapping set matching in cloud ciphertext storage system, Conn. Sci. (2020) 1–18.
[57] Y. Cui, F. Gao, Y. Shi, W. Yin, E. Panaousis, K. Liang, An efficient attribute-based multi-keyword search scheme in encrypted keyword generation, IEEE Access 8 (2020) 99024–99036.
[58] A. Najafi, H.H.S. Javadi, M. Bayat, Efficient and dynamic verifiable multi-keyword searchable symmetric encryption with full security, Multimed Tools Appl. (2021) 1–20.
[59] D. Sangeetha, S.S. Chakkaravarthy, S.C. Satapathy, V. Vaidehi, M.V. Cruz, Multi keyword searchable attribute based encryption for efficient retrieval of health Records in Cloud, Multimed. Tools Appl. (2021) 1–21.
[60] S. Niu, W. Liu, S. Han, L. Fang, A data-sharing scheme that supports multi-keyword search for electronic medical records, PLoS One 16 (1) (2021), e0244979.
[61] M. Hozhabr, P. Asghari, H.H.S. Javadi, Dynamic secure multi-keyword ranked search over encrypted cloud data, J. Inf. Secur. Appl. 61 (2021), 102902.
[62] C. Xu, N. Wang, L. Zhu, C. Zhang, K. Sharif, H. Wu, Reliable and Privacy-preserving Top-k Disease Matching Schemes for E-healthcare Systems, IEEE Internet of Things J. (2021).
[63] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A.Y. Zomaya, An efficient privacy-preserving ranked keyword search method, IEEE Trans. Parallel Distrib. Syst. 27 (4) (2015) 951–963.
[64] E.M. Kornaropoulos, C. Papamanthou, R. Tamassia, Data recovery on encrypted databases with k-nearest neighbor query leakage, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 1033–1050.
[65] F. Li, D. Cheng, M. Hadjieleftheriou, G. Kollios, S.H. Teng, On trip planning queries in spatial databases, in: International symposium on spatial and temporal databases, Berlin, Heidelberg, Springer, 2005, pp. 273–290.
[66] Q. Tong, Y. Miao, X. Liu, K.K. Choo, R. Deng, H. Li, VPSL: verifiable privacy preserving data search for cloud-assisted internet of things, IEEE Trans. Cloud Comput. (2020).
[67] H. Yin, et al., CP-ABSE: a ciphertext-policy attribute-based searchable encryption scheme, IEEE Access 7 (2019) 5682–5694.
[68] B.D. Deebak, F. Al-Turjman, Robust Lightweight Privacy-Preserving and Session Scheme Interrogation for Fog Computing Systems, J. Inf. Secur. Appl. 58 (2021), 102689.
[69] B.D. Deebak, A.T. Fadi, Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing, Future Gener. Comput. Syst. 116 (2021) 406–425.
[70] P. Varga, J. Peto, A. Franko, D. Balla, D. Haja, F. Janky, L. Toka, 5G support for Industrial IoT applications—challenges, solutions, and research gaps, Sensors 20 (3) (2020) 828. ... &.
[71] M. Bhatia, S. Sharma, S. Bhatia, M. Alojail, Fog computing mitigate limitations of cloud computing, Int. J. Recent Technol. Eng. (IJRTE), SCOPUS (2020).

B D Deebak is presently working as Associate Professor in the department of Computational Intelligence, School of Computer Science and Engineering at Vellore Institute of Technology, Vellore, India. He has more than 12 Years of Teaching Experience, Research in various Engineering Institutions in India and Abroad. He received his Ph.D. under a research grant of TCS from SASTRA University-Thanjavur in 2016. His-areas of research include Multimedia Networks, Network Security and Machine Learning. He is an active member in professional societies like IE (I), CSI and ISTE. His-current research interests include network security, computer networks, wireless communication systems, wireless sensor networks, Multimedia Networks, Routing and Security. He has published 22 articles in well reputed publishers such as IEEE, Elsevier, Springer and Tubitak. He also serves as reviewer from IEEE Communications Letters, IEEE Access, IEEE Systems and IEEE Sensors Journal.

Fida Hussain Memon is currently serving as in the department of Electrical engineering at Sukkur Institute of Business Administration Pakistan. His-research interest are IoT, medical robotics, Analog and Digital communication, Measurement and instrumentation, Electronic devices and circuits, and FPGAs. He is in-charge person of FabLab at his university. He has teacnhing experience of more than 5 years in the deaprtment of electronics and computer engineering.

Kapal Dev is Senior Researcher at Munster Technological University, Ireland. Previously, he was a Postdoctoral Research Fellow with the CONNECT centre, School of Computer Science and Statistics, Trinity College Dublin (TCD). He worked as 5 G Junior Consultant and Engineer at Altran Italia S.p.A, Milan, Italy on 5 G use cases. He is also working for OCEANS Network as Head of Projects funded by European Commission. He was awarded the PhD degree by Politecnico di Milano, Italy under the prestigious fellowship of Erasmus Mundus funded by European Commission. His-research interests include Blockchain, 6 G Networks and Artificial Intelligence. He is very active in leading (as Principle Investigator) Erasmus + International Credit Mobility (ICM), Capacity Building for Higher Education, and H2020 Co-Fund projects. He is also serving as Associate Editor in Springer Wireless Networks, Elsevier Physical Communication, IET Quantum Communication, IET Networks, Topic Editor in MDPI Network, and Review Editor in Frontiers in Communications and Networks. He is also served(ing) as Guest Editor (GE) in several Q1 journals; IEEE TII, IEEE TNSE, IEEE TGCN, Elsevier COMCOM and COMNET, and Tech press CMC. He served(ing) as Lead chair in one of MobiCom 2021, Globecom 2021, IEEE PIMRC 2021 and CCNC 2021 workshops, TPC member of IEEE BCA 2020 in conjunction with AICCSA 2020, ICBC 2021, SCt 2021, DICG Co-located with Middleware 2020 and FTNCT 2020.

Sunder Ali Khowaja received the Ph.D. degree in Industrial & Information Systems Engineering from Hankuk University of Foreign Studies, South Korea. He is currently an Assistant Professor at Department of Telecommunication Engineering, Faculty of Engineering & Technology, University of Sindh, Pakistan. He had the experience of working with multi-national companies as Network and RF Engineer from 2008 to 2011. He is also a regular reviewer of notable journals including IEEE Transactions, IET, Elsevier, and Springer Journals. He has also served as a TPC member for workshops in A* conferences such as Globecom and Mobicom. His-research interests include Data Analytics & Machine Learning for Computer Vision applications.

Nawab Muhammad Faseeh Qureshi is an Assistant Professor at Sungkyunkwan University, Seoul, South Korea. He received Ph. D. in Computer Engineering from Sungkyunkwan University, South Korea and was awarded the 1st Superior Research Award from the College of Information and Communication Engineering based on his research contributions and performance during studies. He is an active Senior Member of IEEE, ACM, KSII (Korean Society for Internet Information), and IEICE (Institute of Electronics, Information and Communication Engineers). He has served 14 Guest Editorials. Also, he has served as General Chair Workshop NexGenRAN (Open-RAN: Open Road to Next Generation Mobile Networks) in IEEE Wireless Communications and Networking Conference (WCNC2020) 25th May, Seoul, South Korea and serving as Proceedings Chair in Global Conference on Wireless & Optical Technologies 2020 (GCWOT'20) and General Chair Workshop Open-RAN: Open Road to Next Generation Mobile Networks in IEEE Globecom 2020, Taiwan. He is a reviewer of various prestigious journals and has been a reviewer of various top-tier conferences such as IEEE GlobeCom, IEEE InfoCom, IEEE PIMRC, IEEE ICACT, AIIPCC, and ACM MobiCom. He has been a TCP in various prestigious conferences and performed role of session chairs with ICGCET Denmark, RTCSE19 USA, ICACT 2019 South Korea, and RTCSE 2020. He has evaluated several theses as external Ph.D. thesis evaluators. He has facilitated several institutes with Webinars on Big data analysis and Modern Technology convergence and served sessions with keynote talks on convergence with modern technologies. His research interests include big data analytics, context-aware data processing of the Internet of Things, and cloud computing.