InternationalJournal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 1, January-February (2024)

RESEARCH ARTICLE

EFFICIENT DATA SEARCH AND RETRIEVAL IN CLOUD ASSISTED IOT ENVIRONMENT

K. Paul Joshua [1,*] and A. Jenice Prabhu [2]

[1]Professor, Department of Computer Science and Engineering, SCAD College of Engineering and Technology, Tirunelveli-627414, Tamil Nadu, India.

[2]Assistant Professor, Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai Tamil Nadu, India.

Corresponding e-mail: k.pauljoshua@gmail.com

Abstract –Internet of Things (IoT) is expanding across a number of industries, including the medical field. Such a scenario might easily reveal sensitive information, such as private digital medical records, presenting potential security issues. Symmetric Searchable Encryption has been widely considered due to its promise to allow well-organized search on encoded data. Nevertheless, most SSE techniques ignore malicious cloud servers and need the data owner to provide the entire key in order to query users. In this paper, a novel technique has been proposed to solve these restrictions. Normalization, tokenization, word removal and stemming are used for preprocessing the data from the data owner and preprocessed data is divided into k-number of clusters using k-means clustering algorithm. The clustered data is encrypted using a Damgard-Jurik encryption algorithm. The efficiency of the proposed P2ADS technique has been determined using assessment metrics such as accuracy, encryption time, and decryption time. The proposed method's decryption time is 7.56%, 5.01%, 4.41%, and 3.50% quicker than that of the existing VPSL, ABKS, PERT, and PP-DSA methods respectively.

Keywords *– Data Search, Encryption, Damgard Jurik, Decryption, Internet of Things.*

1. INTRODUCTION

Cloud-based IoT has become more well-known as an emerging technology as using the cloud to manage massive amounts of IoT data can greatly improve the performance of IoT applications [1]. Several cloud services leverage consumer location, private data, and identity, such as Cloud [2] and Amazon's basic storage service. Since cloud models are addressing various data security and privacy issues, the biggest conflict in recent cloud services has emerged. The primary right to data security belongs to consumers or cloud users who keep private information such as bank account details, health information, and so forth.

The process of searching for data typically involves multiple procedures. First, the types of data that IoT [3] devices continuously collect vary depending on the application. These data sets could contain information about human behavior, machine status, environmental variables, or other features. After that, the raw data will be sent to and stored on the cloud for additional processing. Large databases housed on cloud servers hold these data, enabling the preservation of historical records for analysis, projection, and decision-making [4].

Security and privacy are critical components of IoT data search. Many times, data from the Internet of Things contains sensitive information about individuals, systems, or vital infrastructure. Certifying the security and honesty of this statistics is essential to stop unwanted contact and data openings [5]. Here, encryption is crucial for both data transmission and storage. When combined with secure connection protocols like SSL/TLS, encrypted database and storage technologies in the cloud protect data while it is at rest [6].

Furthermore, all of the aforementioned schemes with the exception of one assume that the clouds are sincere in their adherence to the rules of protocol but also sufficiently interested to attempt deriving useful information from the encrypted data [7]. Because of things like financial incentives, technical malfunctions, or cyber-attacks, this assumption doesn't seem to be enough. Consequently, the clouds might only carry out a portion of the search process. As a result, our goal is to create a more reliable and safer search engine that guarantees the return of real search results even in the occurrence of malevolent clouds [8]. To overcome these issues, a novel Data Search strategy for the cloud-assisted IoT has been proposed. The main structures of this paper are listed below:

- The data is first preprocessed utilizing stemming, tokenization, normalization, and word removal techniques from the data owner. The k means clustering algorithm is then applied to divide the preprocessed data into k number of clusters.
- Subsequently, the data is clustered and encrypted using the damgard-jurik encryption algorithm.
- Once the data has been encrypted, it is stored on a cloud server and the user's identity is verified. The decrypted data is sent to the user as a search result

by the cloud server in response to the data user's search request.

- The efficacy of the suggested methodology has been assessed through the utilization of multiple factors, such as precision, encryption duration, and decryption duration.

The following explanation pertains to the remaining half of this research: In Section II, the research is examined with reference to the literature. In Section III the proposed system is detailed in detail. The conclusion is found in Section V, whereas the result and discussion are found in Section IV.

2. LITERATURE SURVEY

In 2020, Tong, Q., et al., [9] designed a cloud-assisted Internet of Things Verifiable Privacy-preserving data Search strategy with Limited key-disclosure (VPSL). VPSL uses the k-means clustering technique and the Merkle hash tree structure to provide effective search processing and result verification, respectively. Real-world datasets were used for performance evaluation, which revealed the true effectiveness and accuracy of VPSL or VPSL+ in terms of search.

In 2021, Zhang, K., et al., [10] suggested attribute-based keyword search (ABKS) to provide cloud-assisted IoT with fine-grained search control and data confidentiality. By tracing and canceling abusive users, these two structures prevent private key abuse in addition to reducing privacy leaks caused by hidden access policies. Formal security analysis demonstrates that the system can ensure the traceability of hostile users in addition to ensuring the confidentiality of keywords and access regulations.

In 2021, Wang, T., et al., [11] suggested PERT, a cloud-assisted Internet of Things retrieval technology with improved privacy. By using a hierarchical retrieval model and an implicit index that is controlled by edge servers, this architecture safeguards data privacy by hiding the specifics of data flow between the cloud and edge servers. When the number of users is reasonably high, this method's time cost is much lower than that of the benchmark cloud encrypted storage model.

In 2022, Deebak, B.D., et al., [12] suggested a PPP-MKRS phrase for multi-keyword ranked searches that protects privacy. It makes use of conjunctive keyword search, a binary tree index structure, and an optimal filtering approach to ensure the efficacy of secure searching. The results of the experimental research demonstrate that compared to previous searching encryption systems, the proposed PPP-MKRS system requires less processing, storage, and verification time.

In 2022, Li, X., et al., [13] suggested VRFMS, a ranking fuzzy multi-keyword search technique that is both efficient and verifiable. Using bloom filters and locality-sensitive hashing, VRFMS implements fuzzy keyword search. The outcomes are organized according to TF-IDF. VRFMS's primary flaw is that it struggles to handle confusing terminology. Formal security analysis and practical testing, respectively, have demonstrated the security and efficacy of VRFMS in real-world applications.

In 2023, Kirubakaran, S.S., et al., [14] introduced the Privacy-Preserved Data Security Approach (PP-DSA) to guarantee the information integrity and security of data that is outsourced in a cloud environment. The work's primary goal is to improve cloud security, which will raise Quality of Service (QoS). Based on the model's efficacy, security, and dependability, the outcomes validate that the suggested model beats previous efforts in terms of output.

In 2023, Gupta, I., et al., [15] introduced a revolutionary effective, privacy-preserving, secure communication model (SeCoM) that reduces the hazard of information leaking, detects, and terminates malevolent entities to prevent data leakage, and handles security risks to protect healthcare data in cloud and IoT systems. The suggested model considerably enhances privacy, security, and detection efficiency as well as data usage of up to 43.25%, 83%, 77.17%, and 9.49%, according to experimental results and comparison with existing methodologies.

3. PROPOSED SYSTEM

In this section, a novel Data Search strategy for the cloud-assisted Internet of Things has been proposed. The data is first preprocessed utilizing stemming, tokenization, normalization, and word removal techniques from the data owner. The k means clustering algorithm is then used to divide the preprocessed data into k number of clusters. Subsequently, the data is clustered and encrypted using the damgard-jurik encryption algorithm. Once the data has been encrypted, it is stored on a cloud server and the user's identity is verified. The decrypted data is sent to the user as a search result by the cloud server in response to the data user's search request. The efficacy of the suggested methodology has been assessed through the utilization of multiple factors, such as precision, encryption duration, and decryption duration. The overall block diagram for the proposed technique is given in Figure 1.

3.1 Data Collection

The process of data collection involves acquiring raw data from the data owner, which may encompass various sources such as databases, sensors, or user interactions. Once obtained, the data undergoes preprocessing to ensure its quality, completeness, and relevance for subsequent analysis.

3.2 Pre-Processing

Preprocessing is the grouping of steps and techniques used to adjust unprocessed data prior to additional analysis. The goal of preprocessing is to format data such that it is suitable for the task at hand. Preprocessing procedures like as normalization, tokenization, word removal, and stemming are used to the data owner's data to ensure that it is in an appropriate format.

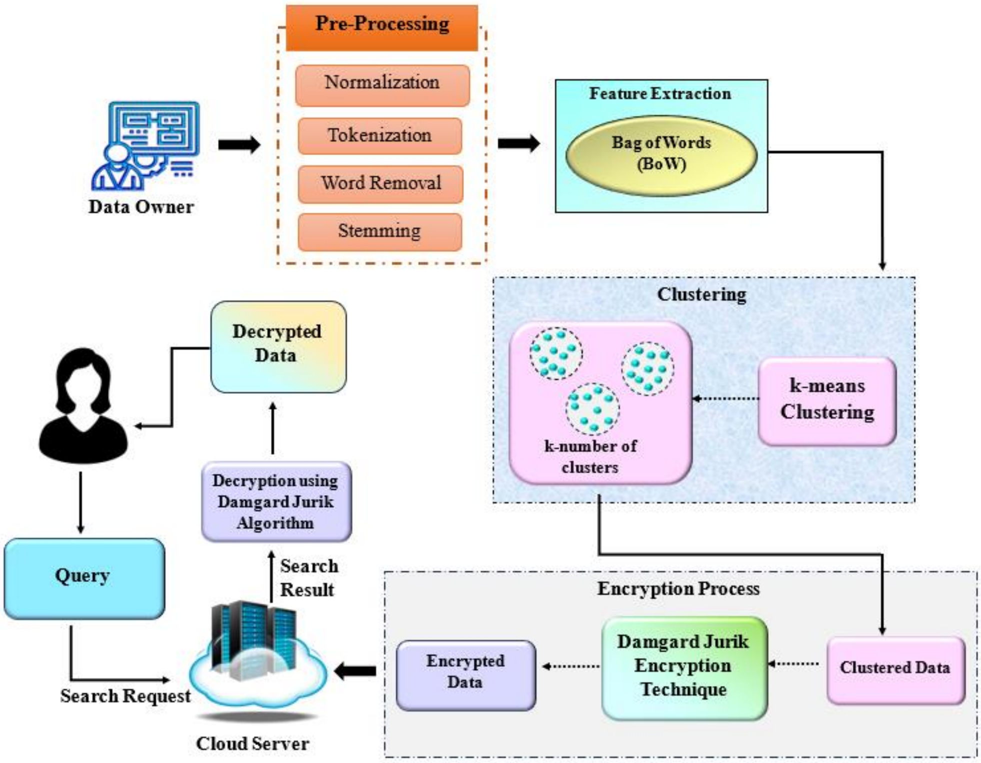

Figure 1. Overall work flow of proposed method

3.2.1. Normalization

Normalization requires the simultaneous completion of multiple tasks. Punctuation must be eliminated, all text must be transformed to uppercase or lowercase, and numbers must be translated to words. Every text will therefore experience more uniform pre-processing.

3.2.2. Tokenization

Tokenization divides a text into meaningful pieces while maintaining its meaning. Long paragraphs, also known as text chunks or chunks, are split into tokens in this stage, which are sentences. You can break these statements down into their component words as well.

3.2.3. Word Removal

Recurring arguments are eliminated from the text throughout this phase. Many stop words are used, including "are," "of," "the," and "at." These have to be taken out of the text as a result.

3.2.4. Stemming

By stemming words in many tenses, unnecessary computations are eliminated and words are reduced to their most fundamental forms. Words with similar meanings should be grouped together via stemming, even if their derivations or inflections differ.

3.3. Feature Extraction

The preprocessed data undergoes feature extraction using Bag of Words (BoW) techniques. The goal of feature extraction is to provide a set of pertinent and instructive characteristics that can be utilized as input for clustering technique from the preprocessed input data.

3.3.1. Bag of Words (BoW) technique

In natural language processing (NLP), the Bag of Words (BoW) is a straightforward and widely used feature extraction tool. The BoW algorithm ignores word order and focuses exclusively on word frequency in order to convert a text passage into a numerical vector. A machine can understand text by first understanding its representation. In order to match and count each element of a text separately and produce its vector representation, the BoW model ignores a significant amount of correlation information between words. The formula for the bag of words representation of a document is given in (1)

$$bow(q_o) = [count(w_{o_1}, q_o), count(w_{o_2}, q_o) \ldots\ldots., count(w_{o_m}, q_o)] \tag{1}$$

Where m represents vocabulary size and the query as q_0, $bow(d_o)$ represents the bag of words representation. Text tokenization is the process of segmenting text into words by utilizing white space and punctuation as delimiters. A vocabulary is formed by treating each word as a unique entity. Using the Bag-of-Words (BoW) technique, every input query is represented by a numerical vector, resulting in a fixed feature set. Word frequency in the query is indicated by values in the vector. Formula (2) expresses the BoW design.

$$y_i = [y_1, y_2, y_3, \ldots \ldots y_{ni}] \tag{2}$$

Let, n denote the general quantity of distinct words in the vocabulary. n_i be the text's frequency count for the i-th word.y_i be the feature vector's element with index i.

3.4. Clustering

A popular unsupervised machine learning technique that divides data into clusters according to similarity is K-means clustering. In this analysis, K-means clustering is applied to pre-processed data to identify inherent patterns and group data points into distinct clusters.

The Euclidian distances serve as the primary foundation for the k-means algorithm, which clusters nodes based on the separation between centroids and data points. The number of clusters is taken to be constant during the k-means clustering process. Adjust one of the n inputs patterns $(m_1 \dots m_n)$ with one of the k prototypes $(pr_1, pr_2 \dots pr_k)$. Therefore,

$$pr_s = m_p, s \in \{1, \dots, k\}, p \in \{1, \dots, n\} \quad (3)$$

The method finds the shortest path between the k centers and the sensor to identify the node in the band with the closest center. When the group stabilizes, the algorithm comes to an end. For every band, the new center of gravity is calculated by the algorithm. reducing a squared error function, an objective function, by

$$S(J) = \sum_{y=1}^{d} \sum_{x=1}^{d_y} \left(\left\| V_y - U_x \right\| \right)^2 \quad (4)$$

Where, $\left(\left\| V_y - U_x \right\| \right)^2$ represents the Euclidean distance between $v_y - u_x$. d_x is the amount of data facts in y^{th} group and $d_y$is the amount of group middles. Table 1. Represents the algorithm for k-means clustering.

Table 1. Algorithm for K-means Clustering

Algorithm of K-means Clustering

1. Begin the K-means algorithm.

2. Randomly place 'k' centroids to initiate clustering of the nodes.

3. Compute the Euclidean distance between each node and its closest centroid, then assign the node to that centroid's cluster.

4. Update the positions of centroids within each cluster and assess for changes.

5. If any centroid has moved, return to step 3; otherwise, proceed to step 6.

6. Conclude the algorithm.

3.5.Damgard Jurik Encryption Algorithm

The Damgård–Jurik encryption algorithm is a versatile cryptographic scheme designed to offer both efficiency and security. Building upon the foundation of the RSA cryptosystem, it incorporates homomorphic properties, allowing for secure computation on encrypted data. It a hybrid encryption approach blending elements of RSA and homomorphic encryption, is employed to secure data prior to storage on cloud servers.

Using the RSA architecture, this approach first creates the public and private keys, allowing for effective key exchange while maintaining homomorphic features. These keys are used to convert each data segment into an encrypted format during encryption, guaranteeing secrecy and integrity both during transmission and storage. The following is the definition of the asymmetric Damgard-Jurik cryptosystem. Let $((q, KY_a), KY_s)$ be the public/private key pair.

$$KY_a = ab \text{ and } KY_s = LCM\big((a-1),(b-1)\big) \quad (5)$$

where a and b are two huge prime integers, and LCM stands for the least common multiple function. $\mathbb{Z}_{KY_a^m} = \{0,1, \dots., KY_a^m - 1\}$ and $\mathbb{Z}^*{}_{KY_a^m}$ indicates the integers with modulo multiplicative inverses KY_a^m where m is a ordinary amount and choice $q \epsilon \mathbb{Z}^*{}_{KY_a^2}$ which is given in equation (6)

$$q = (1 + KY_a)^i y \, mod \, KY_a^{m+1} \quad (6)$$

Where, i is a recognized mutable that moderately prime with KY_a and $y \in \mathbb{Z}^*{}_{KY_a^2}$. The Damgard-Jurik encryption of a plain-text $n \in \mathbb{Z}_{KY_a^m}$ into the cipher-text $c \in KY_a^{m+1}$ using the public key KY_a is given in equation (7).

$$c = F[n,r] = q^n r^{KY_a^m} mod \, KY_a^{m+1} \quad (7)$$

Where, $r \in \mathbb{Z}^*{}_{KY_a^m}$ is the Damgard-Jurik encryption system stochastic or semantically secure, given a random number associated with n..More specifically, depending on the value of r, the encryption of the same plain-text message will produce different cipher-texts using the same encryption key. Selecting $g = 1 + KY_a$ will enable a speedy implementation of this cryptosystem without compromising algorithm security. In this way, n's encryption into c is provided by in equation (8)

$$c = F[n,r] = q^n r^{KY_a^m} mod \, KY_a^{m+1} \quad (8)$$

There are two processes involved in decrypting c using the private key KY_s, based on the premise that $g = 1 + KY_a$. Initially, the decoder calculates:

$$c^{KY_s} = (1 + KY_a)^{KY_s n} \, mod \, KY_a^{m+1} \quad (9)$$

To get access to the message n from c^{KY} , the decipherer has to compute $KY_s n$. To do so, Damgard-Jurik proposed a reiterative process to find n from $(1 + KY_a)^n \, mod \, KY_a^{m+1}$. The decoding of the cipher-text c into n is given in equation (10)

$$n = E(c^{KY_s}). KY_s^{-1} mod KY_a^m \quad (10)$$

By combining the strengths of RSA encryption with homomorphic properties, the Damgård–Jurik algorithm safeguards sensitive data within cloud environments, fortifying against unauthorized access or manipulation.

The cloud server receives a query from the data owner in the form of a search request. Blockchain technology is used in the cloud server to verify the identity of the data user. The data deposited in the cloud server in the encrypted form is decrypted using the Damgard-Jurik method, and if the data user is authorized to deliver the search result, the search result is then safely sent to the data user.

4. RESULTS AND DISCUSSION

The proposed novel technique’s experimental results are analyzed and a discussion of performance is done in terms of numerous evaluation metrics within this section. The dataset NACC is used for the evaluation of the proposed technique. The proposed method is developed and assessed using the Python programming language along with libraries (such as sci-kit-learn, TensorFlow, Keras, Numpy, and HDF5) on a Windows operating system with an Intel Core i7 CPU and 16GB RAM.

4.1. Comparative Analysis

The proposed model's effectiveness is contrasted with VPSL [9], ABKS [10], PERT [11], and PP-DSA [14] in terms of accuracy, encryption time, decryption time, search accuracy, search complexity, and query time.

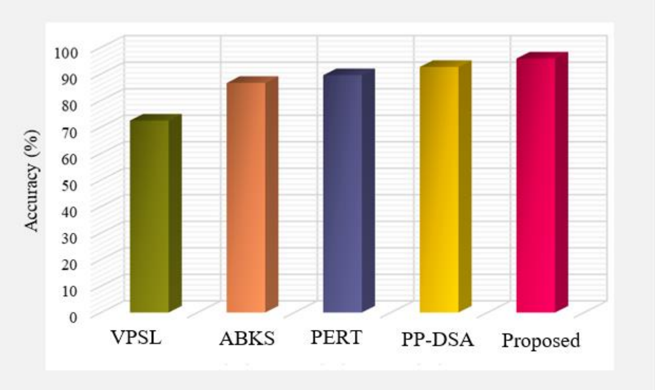

Figure 2. Comparison in terms of accuracy

Figure 2 shows the comparison in terms of accuracy with the proposed technique and the existing techniques like VPSL [9], ABKS [10], PERT [11], and PP-DSA [14] techniques. The accuracy of the proposed method is increased by 9.60%, 6.575 and 3.34% correspondingly. It shows that the proposed method has tall accuracy compared to the existing VPSL, ABKS, PERT, and PP-DSA techniques.

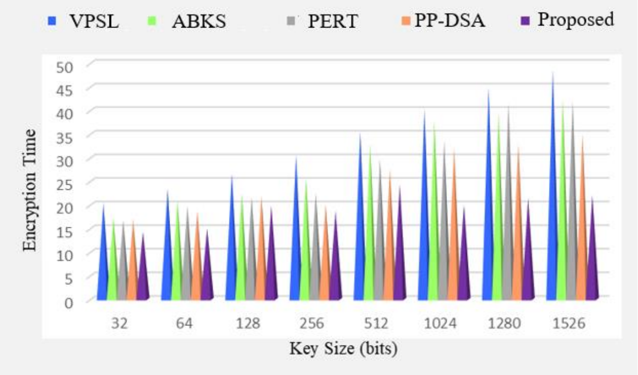

Figure 3. Comparison in terms of encryption time

Figure 3 shows a contrast among a proposed technique and already-in-use methods like VPSL [9], ABKS [10], PERT [11], and PP-DSA [14] in terms of encryption time. The encryption time is the length of time required to employ an encryption algorithm to encrypt a piece of data. The time booked to encode the data is quicker using the proposed approach when compared to other current solutions. The encryption times of the proposed approach are 73.77%, 53.59%, 46.20%, and 31.81% quicker than those of the current techniques.

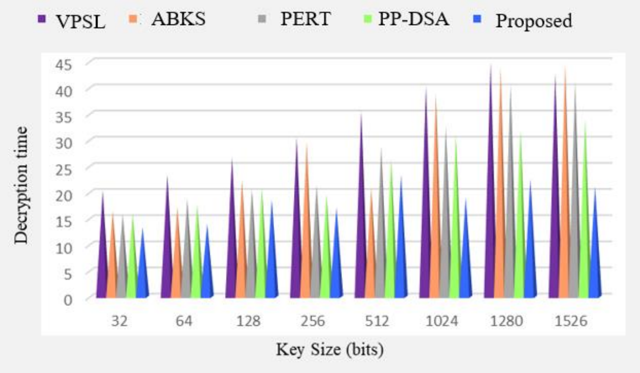

Figure 4. Comparison in terms of decryption time

Figure 4 compares the decryption times of a suggested approach with those of techniques presently in use, such as VPSL [9], ABKS [10], PERT [11], and PP-DSA [14]. The length of time needed to use a decryption method to convert encrypted data back into plaintext is known as the decryption time. Figure 3 shows that when comparing the proposed approach to the current technique, it decrypts data more quickly. The suggested method's decryption time is 7.56%, 5.01%, 4.41%, and 3.50% quicker than that of the existing methods.

5. CONCLUSION

In this paper, a novel technique for the cloud-assisted Internet of Things has been proposed. Normalization, tokenization, word removal and stemming are used for preprocessing the data from the data owner and Preprocessed data is split using the k-means clustering technique into k number of clusters. The clustered data is encrypted using a Damgard Jurik encryption algorithm. The proposed method is developed and assessed using the Python programming language. Evaluation measures like encryption time, decryption time, and accuracy have been used to gauge how effective the suggested technique is. The suggested method's decryption time is 7.56%, 5.01%, 4.41%, and 3.50% quicker than that of the existing VPSL, ABKS, PERT, and PP-DSA methods. In the future, concentrate on reducing the encryption time so that real-time apps can perhaps employ it.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] S. Mishra, and A.K. Tyagi, “The role of machine learning techniques in internet of things-based cloud applications”, *Artificial intelligence-based internet of things systems*, pp.105-135, 2022.[CrossRef] [Google Scholar] [Publisher Link]

[2] M. Prabhu, G. Revathy and R. Raja Kumar, “Deep Learning Based Authentication Secure Data Storing in Cloud Computing”, *International Journal of Computer and Engineering Optimization*, Vol. 01, no. 01, pp. 10-14, 2023.[CrossRef] [Google Scholar] [Publisher Link]

[3] M. Amanullakhan, M. Usha and S. Ramesh, “Intrusion Detection Architecture (IDA) In IOT Based Security System”, *International Journal of Computer and Engineering Optimization*, Vol. 01, no. 01, pp. 33-42, 2023.[CrossRef] [Google Scholar] [Publisher Link]

[4] H. Demirkan, and D. Delen, “Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud”, *Decision Support Systems*, vol. 55, no. 1, pp.412-421, 2013.[CrossRef] [Google Scholar] [Publisher Link]

[5] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, *Computer networks*, vol. 57, no. 10, pp.2266-2279, 2013.[CrossRef] [Google Scholar] [Publisher Link]

[6] A. Mishra, T.S. Jabar, Y.I. Alzoubi, and K.N. Mishra, “Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework”, *Concurrency and Computation: Practice and Experience*, pp. e7831, 2023.[CrossRef] [Google Scholar] [Publisher Link]

[7] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance”, *Computer Networks*, vol. 191, pp.108005, 2021.[CrossRef] [Google Scholar] [Publisher Link]

[8] Z. Shi, X. Fu, X. Li, and K. Zhu, “ESVSSE: Enabling efficient, secure, verifiable searchable symmetric encryption”, *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 7, pp.3241-3254, 2020.[CrossRef] [Google Scholar] [Publisher Link]

[9] Q. Tong, Y. Miao, X. Liu, K.K.R. Choo, R.H. Deng, and H. Li, “VPSL: Verifiable privacy-preserving data search for cloud-assisted Internet of Things. IEEE Transactions on Cloud Computing, vol.10, no. 4, pp. 2964-2976, 2020.[CrossRef] [Google Scholar] [Publisher Link]

[10] K. Zhang, Y. Li, and L. Lu, “Privacy-preserving attribute-based keyword search with traceability and revocation for cloud-assisted iot”, *security and communication Networks*, 2021, pp.1-13, 2021.[CrossRef] [Google Scholar] [Publisher Link]

[11] T.Wang, Q.Yang, X.Shen, T.R.Gadekallu, W. Wang, and K.Dev, A privacy-enhanced retrieval technology for the cloud-assisted internet of things. *IEEE transactions on industrial informatics*,vol. 18, no. 7, pp.4981-4989, 2021.[CrossRef] [Google Scholar] [Publisher Link]

[12] S.S.Kirubakaran, V.P.Arunachalam, S. Karthik, and S. Kannan, Towards Developing Privacy-Preserved Data Security Approach (PP-DSA) in Cloud Computing Environment. Computer Systems Science & Engineering, vol. 44, no. 3, 2023.[CrossRef] [Google Scholar] [Publisher Link]

[13] X. Li, Q. Tong, J. Zhao, Y. Miao, S. Ma, J. Weng, J. Ma, and K.K.R. Choo, “VRFMS: verifiable ranked fuzzy multi-keyword search over encrypted data”, IEEE Transactions on Services Computing, vol. 16, no. 1, pp.698-710, 2022.[CrossRef] [Google Scholar] [Publisher Link]

[14] I.Gupta, D.Saxena, A.K. Singh, and Lee, C.N., 2023. SeCoM: An Outsourced Cloud-Based Secure Communication Model for Advanced Privacy Preserving Data Computing and Protection. IEEE Systems Journal.[CrossRef] [Google Scholar] [Publisher Link]

[15] B.D. Deebak, F.H. Memon, K. Dev, S.A. Khowaja, and N.M.F. Qureshi, “AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT”, Ad Hoc Networks, 125, p.102740, 2022.[CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

K. Paul Joshua received a B.E. degree in EEE from the Government College of Technology, Coimbatore, affiliated with Anna University, Chennai, Tamil Nadu, in 2005. M.E. Degree in VLSI Design from Francis Xavier Engineering College, Tirunelveli, affiliated to Anna University, Chennai, Tamil Nadu, in 2008, and PhD Degree in Information and Communication Engineering from Anna University, Chennai, India, in 2020. His research interests include soft computing applications in power system Engineering. Currently, he is working as Professor and Head of the Department of Computer Science and Engineering at SCAD College of Engineering and Technology, Tirunelveli-627414, Tamil Nadu, India.

A. Jenice Prabhu was born in Nagercoil, Kanyakumari District, Tamilnadu, India. He received him bachelor degree of Engineering in Computer Science and Engineering from C.S.I Institute of Technology, and Master of Engineering in Computer Science and Engineering in St. Xavier Catholic College of Engineering, Nagercoil, India in 2006 and 2012 respectively. He doing Ph.D. in information and Communication Engineering from Anna University, Chennai, India. He has 8 years of teaching experience in Engineering College. His research interests include Networking and Communication, Cloud computing, Wireless sensor Networks, Adhoc Networks and Data analytics

Arrived: 25.11.2023

Accepted: 11.01.2024