Journal of Information Systems Engineering and Management
2025, 10(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Privacy-Preserving Analysis Technique for Secure, Cloud-based Data Mining with Cloud Service Provider

R. Ratheesh[1], M. Rajasekar[2*], Bhuvaneswari B[3], Jose P[4], Suhail Mubarak[5]

[1]*Associate Professor, Department of Electronics and Communication Engineering, Agni College of Technology, Chennai 600130 ratheesh.ece@act.edu.in*

[2*]*Department of Deep Learning, Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu, India. mrajasekarcse@gmail.com*

[3]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Bangalore Trunk Road, Varadharajapuram, Nazarathpet, Poonamallee, Chennai 600123. drbhuvanaramani@gmail.com*

[4]*Associate Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai. drjosep@veltech.edu.in*

[5]*Research Institute of Humanities and Social Sciences, University of Sharjah, University of Sharjah, Sharjah 27272, United Arab Emirates. suhailmubarak@gmail.com*

ARTICLE INFO

Received: 26 Oct 2024

Revised: 30 Dec 2024

Accepted: 18 Jan 2025

ABSTRACT

These days, data mining is commonly used to find relationships between the elements in large datasets. Frequent itemset mining is an essential component of association rule mining, one of the most widely used techniques for data mining. The truthful but inquisitive cloud service provider (CSP) receives large amounts of data. Encrypting data before uploading it to the cloud is generally acknowledged as a way to protect its privacy. This makes it difficult to analyze data, particularly association rule mining while maintaining data privacy. The smooth integration of information is also threatened by recent developments in data mining and knowledge discovery, which make it possible to uncover buried knowledge in massive amounts of data. We examine the challenge of developing privacy-preserving algorithms for association rule mining, one data mining technique. Technologies that enable privacy-aware outsourcing of sensitive data processing and storage to public clouds are covered in this survey to address this problem. Big data and cloud computing are two recent developments. Therefore, it is crucial to identify the connections between them and extract relevant patterns and knowledge from published publications in these disciplines. Additionally, we provide a list of numerous research initiatives and products that have made some of the ideas surveyed a reality. Lastly, we list unresolved research issues.

Keywords: Cloud service provider (CSP); secure; Data Mining; data processing; storage; data mining technologies;

INTRODUCTION

The outsourcing of data and computing services is gaining new relevance with the development of cloud computing and its paradigm for IT services based on the Internet and massive data centers, and it is anticipated to grow significantly shortly. It is anticipated that business intelligence and knowledge discovery services, including advanced analytics based on data mining technologies, will be among those that can be externalized on the cloud because of their data-intensive nature and the intricacy of data mining techniques. Therefore, it is likely that the paradigm of data as service administration and mining will expand along with the popularity of cloud computing. The goal of the data mining-as-a-service paradigm is to make it possible for businesses with little access to computing power and/or data mining know-how to contract with a third-party service provider to handle their data mining requirements.

The data-mining-as-a-service paradigm has several significant security flaws, even though it is beneficial to accomplish complex analysis of massive amounts of data economically. The server's access to the owner's valuable data and the potential to extract private data from it are among the primary security concerns [1]. The server (or a hacker with access to the client) can determine which things are consistently purchased, for instance, by examining the transactions. Nevertheless, the data owner owns the activities and the trends that have been mined, thus they should be protected from the server. The issue of safeguarding the private data of businesses or organizations is

known as corporate privacy. Corporate privacy demands that both individual objects and the patterns of data collection be considered assets of the company, which means they must be secured, in contrast to personal privacy [2], which solely takes into account the security of the private data gathered about individuals.

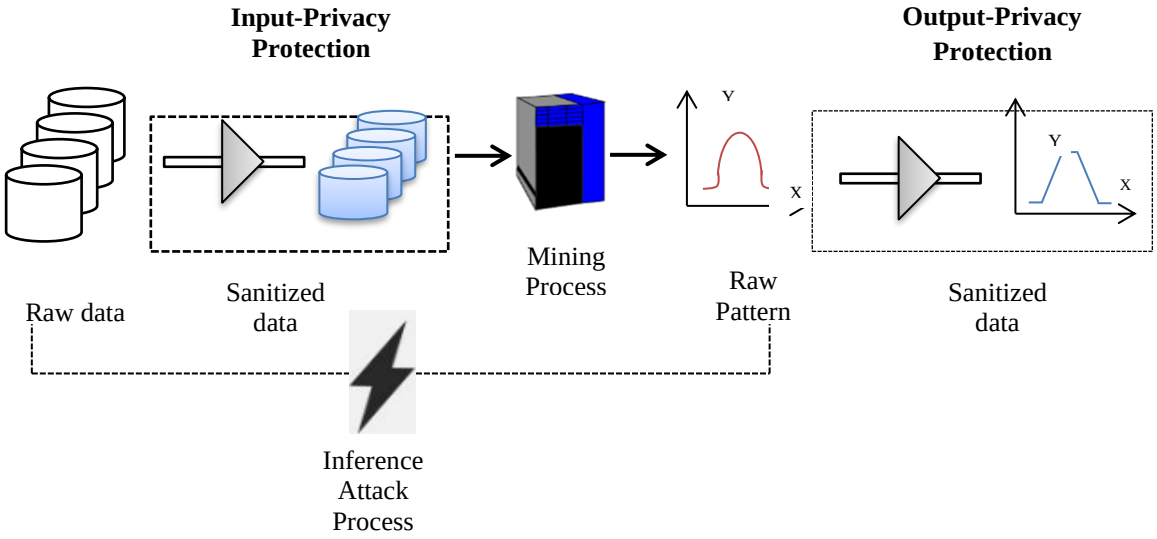

Figure 1.1: Framework of privacy preserving data mining

The architecture for data mining that protects privacy is shown in Figure 1.1. ETL tools are used to gather and pre-process data from various operational systems or data sources. The data warehouse houses this Level 1 data that has been cleaned and converted. Data warehouse data is utilized for mining. Level 2 involves using data mining techniques to identify trends and extract insights from past data. Following mining, methods for protecting privacy are employed to shield data from unwanted access. Individuals' sensitive information can be shielded from abuse.

Numerous applications have made substantial use of data mining techniques. On the other hand, improper use of these methods could result in the disclosure of private data. Sensitive association rules are being concealed by researchers.

However, the rule hiding process may result in undesirable side effects, such as spurious rules that are falsely generated and non-sensitive rules that are falsely hidden. Privacy has grown to be a major concern in data mining. Numerous approaches have been proposed to address this issue. The association rule mining technique, which maintains each database's confidentially, is the fundamental topic of this work. Each participant must provide their own data in order to determine the association rule. As a result, a lot of private information could be disclosed or utilized unlawfully. [3] "The process that attempts to discover patterns in large data sets" is one definition of data mining. Extracting information from a data set and transforming it into a comprehensible structure for future use is the main objective of the data mining process.

This is how the rest of the job is organized. Section 2 presents the inspiration for our paper and the relevant literature. The suggested methodology is presented in Section 3. The experimental setup utilized for the evaluation is described in full in Section 4. The work is concluded in Section 5 with some closing thoughts and suggestions for further study.

RELATED WORKS

These days, DM and ML are very relevant topics. These fields of study give entities, organizations, and people the means to analyze data and extract knowledge. As CC and Edge Computing continue to flourish [4], DM services are becoming more and more prominent in the provider catalog. A comprehensive specification that goes beyond technical or conceptual concerns is necessary due to the complexity of DM solutions. Therefore, the definition needs to incorporate important features of the offering into the CC environment. To obtain an accurate definition and modeling of services, there are a number of proposals for their definition that span a significant range of syntactic and semantic languages. Solutions built on the Linked Data (LD) approach can address the issue of service definition from a more thorough standpoint. LD uses Semantic Web concepts and buildings, a technology that

attempts to make data on the web accessible and compatible with other applications. By utilizing the Semantic Web, the LD proposal enables you to connect data and idea definitions from other areas.

The first real-time scoring engine on the market for commercial data mining software [5] is also offered on Amazon Cloud as a service, which is a comprehensive suite of analytical tools for non-technical marketers housed in a cloud computing environment that also includes optimization and modeling instruments. IBM provides its Smart Analytics System, which includes unstructured information analytics and data mining. The Biocep-R project, an open-source framework for virtualizing Scientific Computing Environments (SCEs) like R and Sci Lab that may be operated on powerful computers or in the clouds, is located in the charity sector. Other attempts along the same line offer data pre-processing functions, data mining algorithms, and visualization methods, all of which are wrapped using Web Services, just like we do. However, none of these initiatives fully encapsulate the process, which is our tool's objective.

The most talked-about topic among scholars and industry professionals is the smart city with the IoT paradigm. The network routing, quality of service, and security features of the smart city data monitoring Internet of Things system have been the main topics of this article. There are still some possible research gaps, such as defining the optimal network routing, enhancing quality of service (QoS), reaching high reliability or lifetime, obtaining the best adaptability, and offering high security, even though many researchers have extensively studied monitoring the conditions of smart cities with IoT [6]. Three possible research issues in smart city IoT wide area networks—network routing, quality of service, and security—have been covered in this study. The two main categories of blockchains are permission (independent) and unrestricted (visible). Any kind of blockchain integration with IoT allows for decentralized management, which improves network security and scalability.

The introduction of cloud computing into our daily lives has been seamless and transparent. The popularity of the Internet has grown due to its simplicity of use and the exponential rise in the number of connected devices [7]. Adopting the cloud computing phenomena entails a significant shift in how IT services are investigated, used, delivered, and consumed. Like energy or gasoline, among other commercial models, online computing is a way to offer services to businesses, organizations, and consumers. Therefore, the goal is a service delivery paradigm in which processing power and computer resources are rented over the Internet of companies. An organization can benefit greatly from internet services because they are accessible from any location and on a variety of devices, and they are also quite affordable when it comes to hardware, software, and technical upkeep. The capacity, a crucial component of any commercial service, is what makes it unique, though.

Clients or users might take advantage of various data mining services that cloud providers guarantee to offer by utilizing this strategy. The issue of sensitive data exposure and costly facilities that arise when a standard client-server model is employed or when the client's sensitive data is transferred to the cloud while using its offerings, as mentioned in the article, are crucial to the advancement of this type of model. These issues will no longer be confronted in the future thanks to this paradigm [8]. When connecting between the server and a client using the general client-server model, the client and the server must share a common library in order to interact using the same structures and formats. This created a dilemma because every client needed to know if they were aware of this library. This turned out to be expensive, time-consuming, and resource-wasting.

The challenge is that these two metrics—privacy and accuracy—are usually incompatible; meaning that enhancing one usually comes at the expense of the other. In this paper, we examine whether customers can be persuaded to provide accurate information by guaranteeing that the mining process cannot, with any reasonable degree of certainty, violate their privacy while also making sure the mining process is as accurate as possible in terms of its results [9]. Therefore, by using approximate solutions that offer practically acceptable levels for these measures, we compromise on the ideal—and possibly unachievable—goal of having both perfect privacy and complete accuracy. Furthermore, keep in mind that 100 percent accuracy in the mining outcomes is probably not even a necessary quality, as the main goal of data mining is to find statistical trends.

The investigation suggests a cloud-assisted privacy-preserving frequent itemset mining method for databases that are vertically partitioned. This method is subsequently applied to the development of a privacy-preserving association rule mining method. Applications with strong privacy requirements for data owners are the focus of both solutions. Data owners who want to outsource data storage can also use the solutions [10]; in this case, they can safely and privately assign their encrypted data and mining tasks to a semi trusted (i.e., inquisitive but

trustworthy) cloud. This is the first work that we are aware of that deals with frequent itemset mining and outsourced association rule mining for datasets that are vertically partitioned. The two main underlying strategies in our solutions are a safe outsourced comparison scheme and an effective homomorphic encryption approach.

METHODS AND MATERIALS

3.1 Privacy preserving data mining techniques

This section concentrates on the various PPDM approaches that have been developed, such as data perturbation, blocking-based, cryptography, etc.

A. Data Perturbation

The technique of data perturbation uses random processes to change data. This method seems to alter critical data values by adding, subtracting, or using any other mathematical formula, so distorting them. Different data kinds, including character, Boolean, classification, and numeric types, can be handled by this method. Preprocessing the initial data set is necessary when dealing with discrete data [11]. Attribute coding and acquiring coded data sets are two categories for data preprocessing. The method merely reconstructs the distribution; it does not recreate the original data values.

Data perturbation is also known as data noise or data distortion. Sensitive data security is crucial, and data perturbation is a key factor in protecting sensitive data. A variety of techniques, including adding noise, a data transposition matrix, adding unknown values, etc., are used to achieve distortion. It can be somewhat challenging to maintain the original data with certain perturbation techniques. Several of these methods rely on dispersion. This issue was resolved by developing a new algorithm that could recreate the distributions. This means that a new distribution-based data mining technique must be created for each unique classification, clustering, or association rule mining task.

Subsequently was predicated on the sparsified singular value distribution (SSVD) and singular value decomposition (SVD) techniques, with the ability to pick features to narrow the feature space. The original dataset and the deformed dataset are compared or their differences are measured using various matrices introduced in this procedure. SSVD is a more effective way for maintaining data utility than other common data distortion techniques that disturb the data by adding noise. The perturbation method has a disadvantage. Every dimension of the data has its own unique reconstruction of its distribution. This implies that every data mining technique based on distributions operates under the implicit premise that each dimension is treated independently. A lot of pertinent data for data mining techniques, including classification, is frequently concealed in inter-attribute correlations.

B. Blocking based technique

The creators of the blocking-based strategy claim that a sensitive classification rule is employed to conceal sensitive information from prying eyes. The anonymity of this technology is maintained through two procedures. First, sensitive rule transactions must be identified. Next, known values must be changed to unknown ones. The original database is scanned in this method to find the transactions that support the sensitive rule. Subsequently, the algorithm substitutes unknown values for the sensitive data for every transaction. This method can be used in applications where it is possible to save uncertain values for certain attributes. The writers hide the true values in a given transaction by using "1" for "0," "0" for "1," or any other unknown (?) value [12]. The way these values are altered is not governed by any rules. The main objective of this strategy is to protect sensitive data from unauthorized access. Depending on the requirements, there might be several sensitive regulations. An original database scan is performed for each sensitive rule. Transactions can support any rule as long as the right side of the rule matches the transaction's attribute class and the left side of the rule is a subset of the transaction's attribute values pair. The program substitutes unknown values for the characteristic in each transaction that complies with those sensitive criteria. Until all sensitive properties are obscured by the unknown values, these processes will be repeated.

C. Cryptographic Technique

One method for encrypting private information is cryptography. It is an effective method for data preservation. The authors presented a cryptographic algorithm that is widely used since it protects sensitive information. Different cryptographic algorithms are available. But there are a lot of drawbacks to this approach. It is unable to safeguard

the results of calculations. The computation's privacy is protected. Using this technique to discuss more parties does not yield useful results. The application of this approach to large databases is quite challenging. The final data mining output can compromise personal information.

D. Condensation Approach

Condensation is another method that is employed. It creates restricted clusters within the data collection and then generates pseudo-data. Condensing the data into several groups of a predetermined size is the method's fundamental idea. There are specific statistics kept for every group. Stream issues and other dynamic data updates are addressed by this method. Every group has a minimum size of "k [13]," which is the level of that secure strategy. The level of privacy increases as the level rises. They create the associated pseudo-data using the data collected from each group. Although this is a straightforward method of protecting privacy, it is ineffective since the data is lost.

E. Hybrid technique

The field of privacy preservation is vast. Numerous algorithms have been put forth to safeguard the data. A novel approach that combines two or more methods to preserve data is called a hybrid methodology. A hybrid approach that combined generalization and randomization. The changed or randomized data is first generalized using this method, which involves first randomizing the data. This method provides data without losing information and can reconstitute original data, protecting private information more accurately. Numerous more techniques, including data perturbation, blocking-based methods, cryptographic techniques, condensation approaches, etc., can also be coupled to create hybrid strategies.

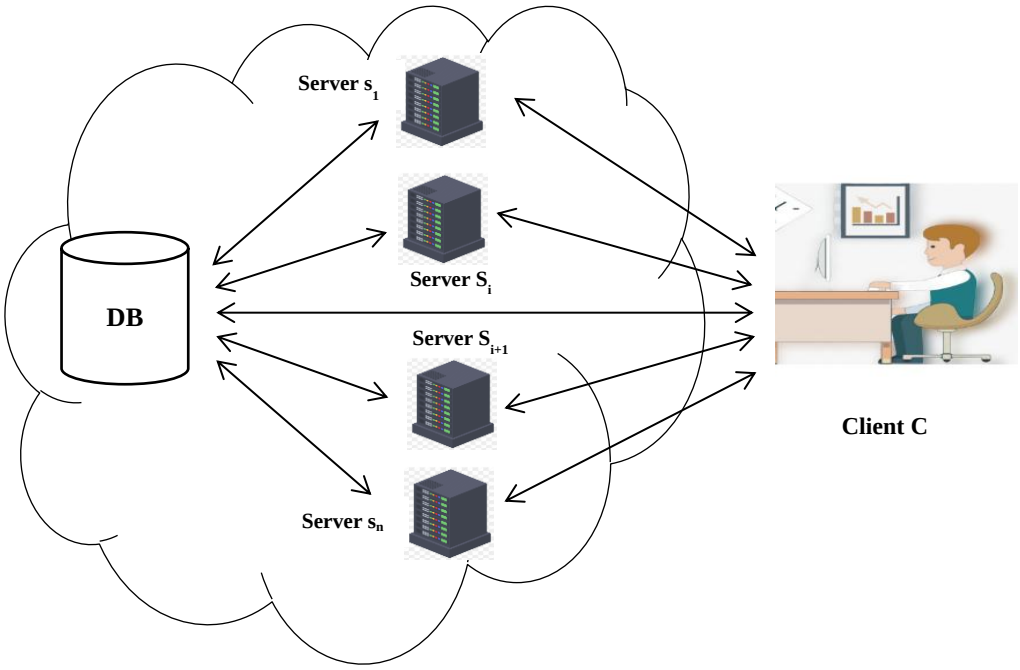

Figure 3.1: Our Framework for Cloud-Based Privacy-Preserving Data Mining

3.2 MODEL

A cloud computing infrastructure with clients and servers is taken into account by our model. It is considered that the clients lack computing power, data storage, and experience, but the servers can offer the customers a range of services, such as data mining and storage. Figure 3.1 shows our paradigm, which consists of one client, one database (DB) server, and n data mining (DM) servers [14]. The client uses a cloud-based database server to store itsdata. ElGamal is the cryptosystem employed to safeguard its data privacy. Around The client first creates its pair of ElGamal public and private keys. Prior to transferring the data to the database server, it encrypts it using its

ElGamal public key. The client chooses n DM server in the cloud, where $n \geq 2$, divides its secret key into n pieces, and distributes them to the n DM servers, accordingly, in order to mine rules for association from the encrypted data. The DM servers can also be regarded as decryption servers since they can work together to decrypt data that is encrypted on the client's behalf. The customer can employ servers from various cloud providers to lessen the likelihood that all servers would be compromised.

All servers, whether DB or DM servers, are thought to be "semi-honest," meaning they strictly adhere to protocols or algorithms but might be concerned about the client's data privacy. Furthermore, it is presumed that at least one DM server out of n is trustworthy and won't conspire with other DM servers. Therefore, only when needed by data mining techniques can the n servers work together to decode the encrypted data.

The goal of our concept is to safeguard the client's data privacy when they contract with the DM and DB servers to handle their data mining needs.

Considering association rule mining is the main topic of this research, we exclusively look at databases made out of transactions. Every transaction has a collection of objects as well as transaction identification (ID). Every transactional item is encrypted and kept on the database server. Since the database server lacks the client's private key, it is unable to decrypt any transactions.

IMPLEMENTATION AND EXPERIMENTAL RESULTS

Text mining and topic modeling approaches are never used to examine the adoption trends of cloud computing in relation to big data [15]. The introduction of this type of information extraction methodology in this field will be beneficial to the research community.

A. Category 1 articles (word cloud & term frequency analysis)

A useful visualization tool for showing the frequency of words in a text corpus is the word cloud. Plotting this diagram allows you to see the main idea of the concepts, associated keywords, and most common words. The term "big data" is evidently the most prevalent one in the category 1 collecting. The other classification terms in the list are cloud, computing, approach, application, and service, in that order. Given how frequently the terms "big data" and "cloud computing" appear in all of the articles gathered under this heading, we can conclude that the cloud computing model is covered in relation to its use in big data processing. The database-wise distribution of word cloud phrases is provided in Tables 1, and 2.

Table 1: Cluster centroid words for (group 1 items)

Clusters	Cluster Centroid Terms
0	Software, reliability, cloud, big data OpenStack, computing, faults, rate, federation
1	Big Data Cloud computing, Security, Storage, Analytics, Service, information, applications
2	Big data, Cloud Computing, Mobile, Service, user Application, Platforms, Information, devices
3	Big data, Cloud computing, healthcare, Hadoop, Cluster, telehealth, mapreduce
4	Histogram, Event, Big data, Time, Processing, Energy, Server, Allocation, Intermediate, Performance

Table 2: Centroids for clusters in (items class 2)

Clusters	Clusters Centroids Terms
0	Adoption, Cloud Computing, clouds, organization, Capabilities, assessment, enterprise
1	Cloud, Security, phase, assessment, checklist, gaps, methodology, computing, compliance
2	Cloud, SMES, Computing, Adoption, factor, information, data, technology
3	Cloud, computing, adoption, technology, data, Services, Security, Management
4	Data, cloud, migration, tenant, application, analytics, computing, components, node, service

E. Similarity Analysis

The comparable analysis method described in was used on both categories' articles. Similarities between the articles are displayed in the heat map. As illustrated in Figures 4.1 and 4.2 [16], the pieces in both groups fall under the specific areas mentioned in the preceding section. Although the similarity algorithm is unable to pinpoint the precise link between the articles, all of them are related to one another and share a similar meaning. In terms of category, similarity analysis reveals that these pieces are not precisely alike, but rather have meanings that are connected within their respective fields. The first category's articles are more comparable to those in the second category.

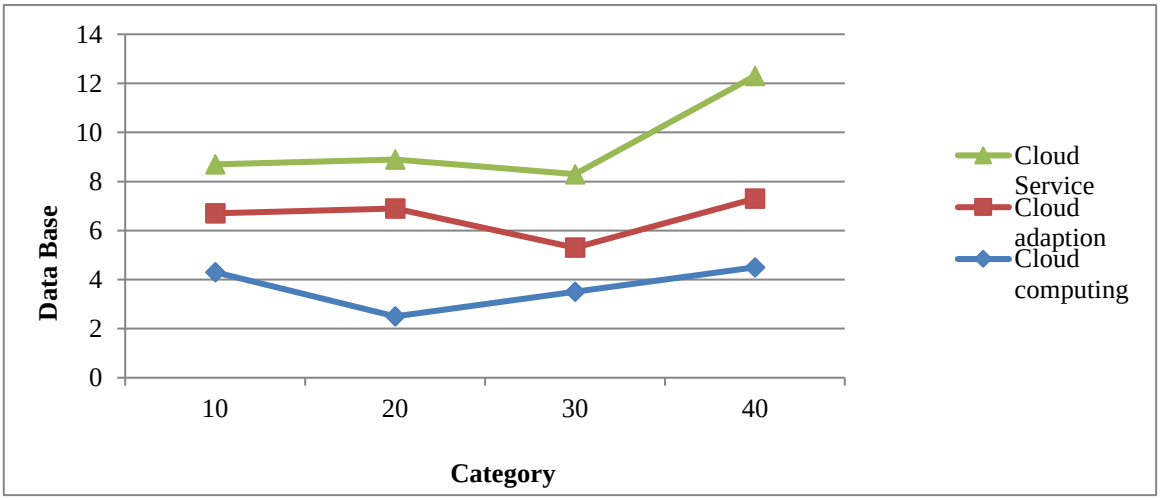

Figure 4.1: Word cloud for every database

F. Cluster Analysis

The methods described here were used to perform cluster analysis on articles in the first category. Clusters are designed using the K-Means clustering technique. We experimented with K values ranging from 1 to 7, but ultimately decided on k=5 because it produces the best outcomes. Five clusters are depicted in Figure 4.1 [17]; whereas clusters 0 and 3 each have one article. Cluster 1 has three articles, whereas Cluster 4 has five. The most articles that can be gathered in cluster 2 (K=108). This indicates that the primary subject of these articles—the use of cloud computing for big data—is being covered. We attempted to discover that the articles grouped in different clusters (K=11) discuss big data, however marginally and from a different angle.

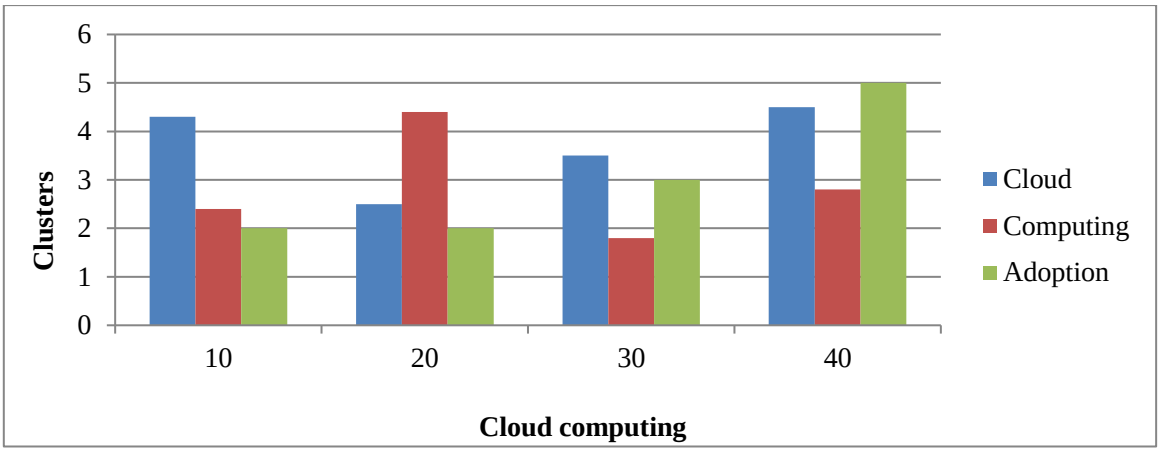

Figure 4.2: Distribution of word frequencies in all databases

The terms that appeared in the cluster centroid are displayed in Table 2. According to a study, the terms in the cluster center indicate the topic covered in a cluster's articles. As a result, the papers gathered in this cluster are centered on tools related to big data and cloud computing. Similarly, cluster 1's unique centroid terms are

"security," "storage," and "analytics," among others. This indicates that the articles gathered in this cluster are centered on large data preservation, analytics, and cloud computing service applications.

The unique center definitions for cluster 2 include "mobile," "devices," "user," and so forth. This indicates that the articles gathered in this cluster are centered on big data, which is produced by user devices and applications using mobile cloud platform services. The largest number of articles in the collected collection is concentrated in this subcategory, as indicated by the biggest number of entries accumulated in this cluster. Cluster 3's unique terms are "map-reduce," "health care," and "telehealth," indicating that the articles in this group are centered on the use of cloud-based computing in healthcare Processing large amounts of data.

CONCLUSION

In this research, we have suggested three ways to mine association rules in the cloud computing environment while maintaining privacy. Accordingly, they maintain the privacy of the items, transactions, and databases. Our experiment and implementation have proven the usefulness of our solutions. Additionally, we observe that parallel computing can greatly enhance performance. Specifically, we may make our protocol more efficient in terms of time by splitting the encrypted operations into disjoint subsets, each of which would be handled by a different set of n DM servers. Nevertheless, further adjustments to our procedures are required to produce the right outcomes. Our future work will take this into account, and we'll look at how well it performs when we implement our ideas in the cloud environment that the cloud service providers offer.

The investigation focuses on the use of text mining algorithms for big data processing and information extraction in the cloud computing space. It identifies important elements for successful adoption, adoption barriers, and other related information from many angles.

REFERENCES

[1] Rajasekar, M., Nahar, G., Jagatheeswaran, S., Chinthamani, S. A. M., Mohammed, S. H., & Al-Hilali, A. (2024, May). The Roadmap to Classify Malware Using ML Algo Through IOT Based SN. In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 127-130). IEEE.

[2] Rajasekar, M., Arunachalam, P., Priyadharsini, P., Devi, N. L., Abbas, H. H., & Al-Qaisy, S. A. (2024, May). An Optimized Framework Development of ABC Algorithm Along with SVMP Algorithm for Lung Cancer Detection. In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 184-187). IEEE.

[3] Reddy, N. K., & Rajasekar, M. (2024, November). Increasing F1 score with VGG16 during plant disease classification over VGG19. In AIP Conference Proceedings (Vol. 3193, No. 1). AIP Publishing.

[4] Parra-Royon, M., Atemezing, G., & Benitez, J. M. (2020). Semantics of data mining services in cloud computing. IEEE Transactions on Services Computing, 15(2), 945-955.

[5] Zorrilla, M., & García-Saiz, D. (2013). A service oriented architecture to provide data mining services for non-expert data miners. Decision Support Systems, 55(1), 399-411.

[6] Parra-Royon, M., Atemezing, G., & Benítez, J. M. (2018). Data mining definition services in cloud computing with linked data. arXiv preprint arXiv:1806.06826.

[7] Haq, M. I. U., Li, Q., & Hassan, S. (2019). Text mining techniques to capture facts for cloud computing adoption and big data processing. IEEE Access, 7, 162254-162267.

[8] Gupta, G., & Pathak, D. (2016). Cloud Computing:“Secured Service Provider for data mining”. International Journal Of Engineering And Computer Science.

[9] Heidari, A., & Jafari Navimipour, N. (2022). Service discovery mechanisms in cloud computing: a comprehensive and systematic literature review. Kybernetes, 51(3), 952-981.

[10] Manimegalai, T., Ravishankar, T. N., Kannagi, L., Kannan, K., & Anitha, G. (2022, April). A Novel approach for Data mining Classification using J48DT Classifier for Intrusion Detection System. In 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 601-607). IEEE.

[11] Anitha, G., Sethukarasi, T., & Sugumaran, S. (2023, December). A Robust Data Communication Model to Transmit Data through Human Body using Intelligent Wearable Sensors. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-7). IEEE.

[12] Sharma, A., Sangeetha, R. G., & Anitha, G. (2022, July). Analysis of Broadcast Reliability for Data Center Inter connects. In 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-6). IEEE.

[13] Sugadev, M., Rayen, S. J., Harirajkumar, J., Rathi, R., Anitha, G., Ramesh, S., & Ramaswamy, K. (2022). Implementation of combined machine learning with the big data model in IoMT systems for the prediction of network resource consumption and improving the data delivery. Computational Intelligence and Neuroscience, 2022(1), 6510934.

[14] Bommu, S., Babburu, K., N, S., Thalluri, L. N., Gopalan, A., Mallapati, P. K., ... & Mohammad, H. R. (2023). Smart city IoT system network level routing analysis and blockchain security based implementation. Journal of Electrical Engineering & Technology, 18(2), 1351-1368.

[15] Rajasekar, M., Celine Kavida, A. & Anto Bennet, M. A pattern analysis based underwater video segmentation system for target object detection. Multidim Syst Sign Process 31, 1579–1602 (2020). https://doi.org/10.1007/s11045-020-00721-4

[16] Kumar, G. T., & Rajasekar, M. (2024, November). Accurate segmentation of blood cell section in thresholded image with Chan-Vese compared to level set. In AIP Conference Proceedings (Vol. 3193, No. 1). AIP Publishing.

[17] Naganuma, K., Yoshino, M., Sato, H., & Sato, Y. (2014). Privacy-preserving analysis technique for secure, cloud-based big data analytics. Hitachi Rev, 63(9), 577-583.