SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I1P105

Volume 10 Issue 1, 53-62, January 2023

Original Article

Outsourced Analysis of Encrypted Graphs in the Cloud with Privacy Protection

D. Selvaraj[1], S. M. Udhaya Sankar[2], D. Dhinakaran[3], T. P. Anish[4]

[1]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India.*
[2,3]*Department of Information Technology, Velammal Institute of Technology, Chennai, India.*
[4]*Department of Computer Science and Engineering, R.M.K College of Engineering and Technology, Chennai, India.*

[1]*Corresponding Author : drdselva@gmail.com*

Received: 24 November 2022 Revised: 03 January 2023 Accepted: 13 January 2023 Published: 29 January 2023

Abstract *- Huge diagrams have unique properties for organizations and research, such as client linkages in informal organizations and customer evaluation lattices in social channels. They necessitate a lot of financial assets to maintain because they are large and frequently continue to expand. Owners of large diagrams may need to use cloud resources due to the extensive arrangement of open cloud resources to increase capacity and computation flexibility. However, the cloud's accountability and protection of schematics have become a significant issue. In this study, we consider calculations for security savings for essential graph examination practices: schematic extraterrestrial examination for outsourcing graphs in the cloud server. We create the security-protecting variants of the two proposed Eigen decay computations. They are using two cryptographic algorithms: additional substance homomorphic encryption (ASHE) strategies and some degree homomorphic encryption (SDHE) methods. Inadequate networks also feature a distinctively confidential info adaptation convention to allow the trade-off between secrecy and data sparseness. Both dense and sparse structures are investigated. According to test results, calculations with sparse encoding can drastically reduce information. SDHE-based strategies have reduced computing time, while ASHE-based methods have reduced stockpiling expenses.*

Keywords *- Cloud, Protection, Outsourcing data, Homomorphic encryption, Eigen deterioration.*

1. Introduction

The fast development of electronic gadgets and communications technology encourages the emergence of the cloud computing era, which has significant implications for and value for people from all walks of life. Data exporting services are accelerated by cloud computing, making them an essential and practical use [1]. The graph structure is common in many disciplines, including chemical structure, transportation, and sociological graphs. The cloud computing service often accepts extensive graph data, which is in charge of preserving, organizing, and analyzing such facts due to the cloud's tremendous processing capacity as well as the issue of cost savings [2]. However, because the CCP server is not entirely honest and reliable, it is important to consider and deal with the concerns about privacy related to the outsourced data. Before being outsourced to CCP, encryption of the exporting graph data is an efficient and often utilized technique [3]. However, encrypted outsourced graph data is difficult for data users to edit and use further. Implementing privacy-guarding optimum route discovery with assistance for query expansion on the secured graph in the cloud services context is thus critical work.

The privacy-preserving solutions of the majority of mining algorithms, particularly spectral information, can be built using two widely used general privacy-preserving techniques: homomorphic encryption and secure multi-party communication. However, their price makes them impractical [4]. Huge block cipher and intensive homomorphic multiplication are the consequences of the finest FHE scheme execution currently available. For recommender systems with scrambled networks, one cycle of factorization is a comparatively tiny 100 × 100 matrices using a confidentiality vector space algorithm in transmission.

Distributing graph data while protecting privacy is somewhat connected to our work. Its problem situation is quite different, in any case. To share graph data, publications must overcome privacy issues brought up by intrepid data miners [47]. With prior knowledge, however, the assaults can indeed be fully identified and comprehended. As a result, privacy for analyses has gained popularity recently. The publication of graph layouts is not our goal. Simple, sparse encoding, therefore, reveals excessive data because most graph matrices have unique structures. Our approach is

the same as adding fictitious edges to achieve differential privacy [6]. The new entries are encoded 0s; therefore, they have no impact on the calculation of the matrix, so the reliability is unaffected by this edge insertion.

2. Related work

Unfortunately, gathering and processing graph data via the cloud raises privacy issues. Individuals are reluctant to provide these datasets since they are typically sensitive because they need to have faith in the ability of the data proprietors to keep the data source safe in the cloud server. On the other hand, as data are now crucial to doing business or conducting a scientific study, data owners also have a tremendous stake in maintaining their ownership of these valuable data. Furthermore, according to recent research and events, sensitive data stored in the cloud is vulnerable to data loss, spying, and malicious insiders. They are finding ways to accommodate consumers' and data proprietors' worries in cloud-based data extraction.

To assure security, several matrix processing methodologies have indeed been presented. These secured outsourced alternatives are tailored for large-scale linear regression solutions and applications involving multiplication and additive noise filtering. Their methods could be more effective because they reveal sensitive data, rely on numerous servers that are not collaborating, or need significant overhead. Use client-cloud cooperation and matrix disruption to solve systems of equations iteratively.

R. Bost [7] builds three main categorization protocols—decision trees, hyperplane decisions, and Naive Bayes —that satisfy this privacy restriction. They also make it possible for these methods to work with AdaBoost. They show that such libraries can also be utilized to design other predictors, such as multiplexing and feature extraction. These constructions are based on new libraries of essential components for reliably generating classifiers. They applied filters and libraries into practice and evaluated them. When used with actual clinical data, the efficient methods accomplish a diagnosis in a few milliseconds to a few seconds.

By fusing a customer's query information with permission data credentials and indices, D. Leilei [52] presents a Dynamic Multi-client SSE (DMSSE) method with support for boolean queries. The system restricts a client's search capability to appropriate terms and enables a data owner to authorize numerous clients to run boolean inquiries over an encrypted format. The advantages of our DMSSE scheme over current MSSE solutions include the following: 1) Lack of interaction. After receiving search authorization, clients are free to do their searches without the assistance of the data owner. 2) Active. The data holder can effectively change the search authorization of a customer without impacting other customers. Using the DMSSE method in a large encoded file is beneficial, as shown by empirical assessments performed on actual data.

Li et al. [9] presented a dynamic additive homomorphic encryption scheme and discussed a couple of crucial dilemmas using attribute-based encryption and the k-nearest neighbor algorithms. However, none of the searchable encryption alternatives can be employed to accomplish optimized route discovery with assistance for information retrieval over cryptographic graph data. F. Berger [48] to discover an implied representation of a molecule's ring system. They offer effective cyclic graph referential integrity techniques that could speed up lookups by acting as molecular descriptors. The precise construction of a molecular graph's well-defined collection of rings is yet another task. They provide a brand-new approach for calculating a graph's relevant cycle set.

Catalano, D [11] demonstrate a method for converting linearly homomorphic encryption into a system that can assess degree-2 calculations on encrypted message. The translation is remarkably easy to implement and only necessitates one very minor requirement on the baseline continuously homomorphic scheme: the communication field should be a public ring that allows evenly distributed sampling of its members. With practically all current number-theoretic linearly elliptic curve schemes, including Goldwasser-Micali, Paillier, or ElGamal, they can instantiate the transformations as a result. When addressing a subset of degree-2 harmonics in which the amount of modifications of degree-2 terms is constrained by a fixed, our resultant techniques ensure circuit confidentiality and are small. Z. Cui [12] concentrates on a fundamental issue with geo-tagged data: identifying the top k frequently occurring phrases in a particular region of the cloud's spatial data. They first create a Region Tree Index (RTI) for geo-tagged data. Then, Sorted Terms and Weights (SSTW) are suggested to be stored in RTI using the array collection architecture. The top k often occurring phrases in a specific area are computed using an effective k Terms Search method. Finally, thorough tests confirm the viability of the suggested scheme.

In a cloud computing context, Xianyi [13] provides a method to carry out privacy-protecting optimum route discovery with assistance for semantic search on the encrypted graph (PORF). Based on the concept of searchable encryption and the stemming process, we developed a method by creating a safe query index to execute optimum path discovery with assistance from the keyword web. For our system, they provide a rigorous security analysis. Furthermore, through experiments, they also evaluate the plan's effectiveness. GOOSE, a safe architecture for Graph Contracting and SPARQL Analysis, is presented by R. Ciucanu [14].

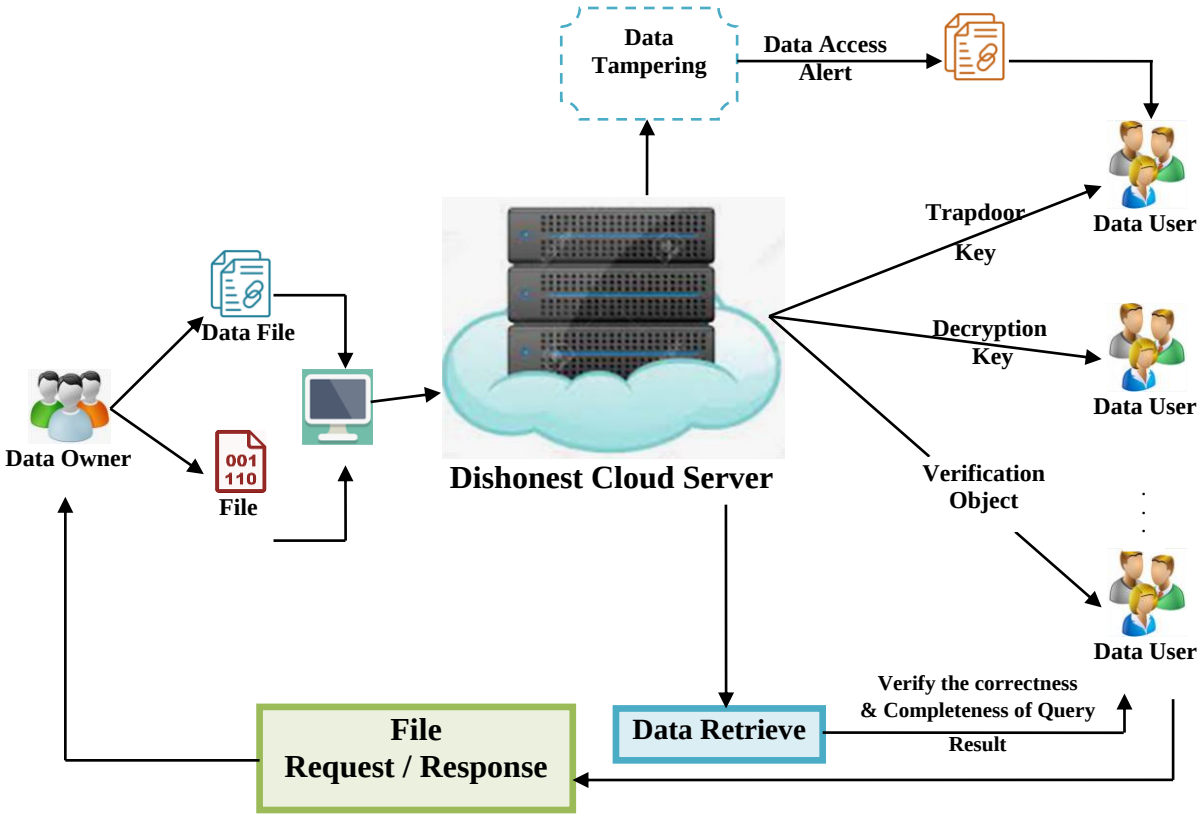

Fig. 1 Technical Architecture of Outsourced Analysis of Encrypted Data

To obtain the following attractive data security, GOOSE uses cryptosystem and secure multi-party computation: (i) no cloud node could indeed gain knowledge of the graph; (ii) no cloud node could indeed simultaneously learn the query and the query responses, and (iii) an outside network spectator could indeed gain knowledge of graph; the query; or the query answers. The core of the W3C's SPARQL 1.1 specification, Unions of Conjunctions of Regular Path Queries (UCRPQ), is supported by GOOSE as a query language and recursion queries. They demonstrate that the latency associated with cryptographic techniques scales linearly with input and output sizes.The FHE-based technique for mathematical systems will need to be demised at many levels. Re-encryption to preserve the usefulness of encrypted data [10,15]. Larger cipher messages and substantial processing expenses are needed for this. On the other side, the data owner wishes to control and analyze the growing customer data using public cloud services [50].

This study considers calculations for security savings for one essential chart examination: diagram extraterrestrial analysis for offshore charts in the cloud. The main task: Multiple information extraction procedures also depend on the Eigen decomposition of large frameworks. We consider a cloud-driven design with personal identification, content providers, and cloud suppliers as three synergistic groups. Charts are referred to as frameworks; their parts are stored and assembled by dispersed clients [17]. The information proprietor subsequently collaborates with cloud part initiatives to drive creepy investigation while safeguarding data security against the reputable but enquiring cloud service. While computations are made according to data contributors and proprietors.

3. Proposed Methodology

Using the SDHE and ASHE methodologies within the cloud-centric architecture presents several obstacles, which our research tackles. (1) Since SDHE permits homomorphic multiplication solely on a single level, implementing cloud-side operations is simple. However, the full extent of their costs has yet to be discovered. (2) ASHE techniques have smaller cipher text sizes, making storage and transmission effective. However, in the cloud, data providers must acquire, decode, and analyze information locally to ensure computational anonymity, as shown in Fig. 1.

We determine the privacy risk associated with sending sparse graph matrices and create a productive local differential—a secret technique for adding fictitious edges with identically encrypted values. Both may be rebuilt and adapted to a cloud infrastructure to accomplish practical-based division. The real effort of separating the consumer and cloud parts protects the confidentiality of data and analytic output, as shown in Fig. 2.

Protected search enables authorized data users to seek through the encoded data of the data owner and privately offers anonymized search terms [6,18,20,21]. It is a compelling adaptation of conventional cryptography for the cloud computing environment and is fueled by efficient content recovery from encrypted cloud data that has been subcontracted [16, 22-26]. A significant amount of study has been done on safe search terms and difficulties in cloud technology, with the goals of consistently enhancing search effectiveness, lowering computation and communication costs, and enhancing the range of search features with greater privacy and security protections [51]. All of these. strategies share the fundamental presumption that perhaps the cloud is an "honest-but-curious" phenomenon thatconsistently maintains resilient and reliable software and hardware environments.

As a consequence, whenever a search is finished, the cloud provider consistently returns accurate and comprehensive search queries without exception. For safe keyword search over secure cloud data, we officially present the provable secure searching model of the system and threat model and construct a perfectly all-right search outcomes classification method. We suggest a quick signature method based on public-key cryptography without certificates to validate objects' veracity.

3.1 Added Substance Homomorphic Encryption

The following characteristic of added ingredient homomorphic encryption exists. The additive homomorphic procedure is shown as follows for two integers.

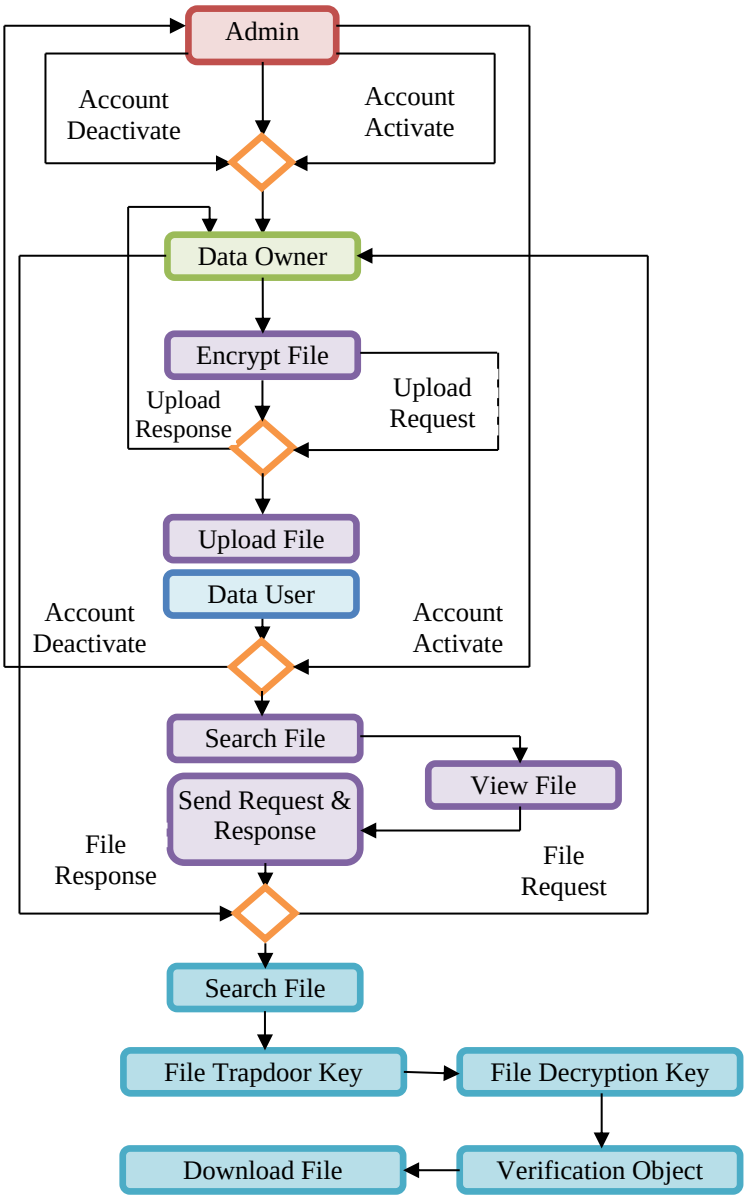

Fig. 2 Process Flow of Proposed Approach

$$E_n(x + y) = E_n(x) + E_n(y) \quad (1)$$

We will utilize Paillier cryptography as an example of one of the most effective ASHE strategies to illustrate our ASHE-based procedures. A series of pseudo-homomorphic processes that form the basis of our procedures are made possible by additive homomorphic encryption. Unencrypted for one parameter, or either, we obtain

$$E_n(\text{xy}) = \sum_{i=1}^{y} E_n(x) = \sum_{i=1}^{x} E_n(y) \quad (2)$$

$E_n(xy) = E_n(x)^y \bmod P_k^2$, where P_k is the public key, provides a more effective method to multiply for Paillier cryptography. Since an operand isn't encoded, we refer to it as pseudo-homomorphic multiplication. We can deduce the pseudo-homomorphic dot product, matrix-matrix multiplication (MMM), and matrix-vector multiplication (MVM), each employing one unencrypted parameter, from all these two essential aspects. Protecting the unencrypted operand is the main difficulty faced by ASHE-based solutions.

3.2 Some Degree Homomorphic Encryption

In recent years, systems for some degree of homomorphic encryption (SDHE) have indeed been created to accomplish a level or more of homomorphic multiplier concurrent with ASHE. For instance, it is possible to determine on encrypted numbers $E(n_i)$ while decoding them the sums $(n_1 + n_2)(n_3 + n_4) + (n_5 + n_6)(n_7 + n_8)$. Keep in mind that each value only requires one multiplication. In comparison, the multiplication in $n_1, n_2 n_3$ occurs twice. The degree-2 functions are frequently computed homomorphically using the SHE methods. Several well-known SHE prelisting: the BGN strategy, utilizing group pairings with elliptic curves, the RLWE method, relying on the ring learning-with-error issue; and the Catalano et al. [11] strategy, focused on an adaptation of the AHE strategy.

We will employ the RLWE method in the analysis instead of the other two because of cost concerns [28-33]. The decryption of the BGN technique relies on processing a discrete log, which has an $O(\sqrt{q})$ cost for unencrypted variables in the [0, q] range. We discover that it takes more than one second to decode 20-bit data by using the component dlog brute force technique, which may undoubtedly be reduced with some adjustment. The ciphertext extension of the Catalano et al. [11] algorithm led to its exclusion. When an N-dimensional space and an N*N-encoded matrix are multiplied, the result will contain $O(N^2)$ encoded components, which are too pricey to be sent to the customer. We omit the specifics among these techniques owing to space constraints.

Algorithm - Privacy-preserving - (PP) sparse submission (Hs, D_p, $An_{a,b}$).
Input:
Hs - histogram,
D_p - parameter (differential privacy),
$An_{a,b}$ - precise node degree.

Determine the bin containing $An_{a,b}$, where Up_a and Lo_a are its upper and lower bounds.

$x \leftarrow (\text{Up}_a - \text{Lo}_a)/D_p$;
$y \leftarrow x * 3.9$; // for y ≈ 3.9 for x = 1 the y scales linearly with x: y ≈ 3.9x;

Generate a variable $\phi_{a,b}$ based on dispersal Laplace (0, x); $K_{a,b} \leftarrow |y| + \phi_{a,b}$; add $An_{a,b}$ inadequate encryption and actual references to the listing; arbitrarily choose $K_{a,b}$ edges away from the others $N - An_{a,b}$ edges and as the encoded zero bits, encrypt it; Therefore, provide index (a, b) of the items for b ≥ a if the graph is directionless; if not, submit all $An_{a,b} + K_{a,b}$ items.

To create a brand-new Parlier Encryption-based verification object request method in which the Cloud provider has no idea whatever information the user is seeking or even which certification items will be presented to the user. To assess the precision and effectiveness of our suggested system, we offer comprehensive security specification and verification, as well as carry out thorough performance trials.

3.3 Query Process

The data user can validate the findings using the query result verification mechanism. In this article, we created a secure, straightforward to combine by providing a specific query result set. If the accumulation somehow fails to return either the number of or whichever qualifying files, the search client can do further checks and verify the accuracy of each data source in the accumulation [34-38]. This is known as a fine-grained query results validation mechanism.

The cloud computing idea enables speedy deployment and distribution of a shared pool of reconfigurable computational power, such as networking, processors, memory, programs, and applications, with minimum administrative labor or service provider participation.

Three separate keys will instantly be produced for the encrypted format when the data owner transmits to a remote server. To secure the anonymity of the validation objects while minimizing space and communication costs. Keys for trapdoors, verification objects, and decryption are generated automatically. The trapdoor key distinguishes between data owners and hackers [5,27,39-42,46]. The query results group and related validation objects are returned after a query is

complete and are provided to the querying user, who uses the validation item to check the accuracy and comprehensiveness of the query results. Our suggested query outcomes validation approach allows the information to execute completeness verification before decoding search queries rapidly and verifies each encrypted data file in the query results set by the query client.

When a cloud server or other unauthorized party accesses information or data that the user has stored. Anytime someone tries to access the information or data, the data user will receive a warning. We may stop unauthorized users from obtaining user data or information by validating the verification object [43-45,49]. When the data held within them cannot be retrieved typically, data recovery is the act of saving (retrieving) unavailable, stolen, distorted, corrupted, or reformatted information from secondary stores, portable media, or files. We can still retrieve the entire document even if a hacker has access to the data or tampers with it.

4. Experimental Evaluations

We have demonstrated that, given the framework's supposition, all strategies that have been constructed ensure privacy. The tests will assess different expenses related to these strategies to determine which algorithms are more effective. Our analysis has three main components: evaluating the Search complexity in carrying out the ASHE and SDHE-based privacy-preserving (ii) the Query time for the cloud and data providers with various cryptographic techniques.

4.1. Setup

After the data owners' logins have been verified and granted access, the datasets will be uploaded to the cloud so everyone can access them. After choosing the file from the system, we must enter the date for the cloud system upload. We have a search function that may show the encrypted search, the uploaded time, the owner of the data, and the action. So that we can find out who submitted the file, its owner, and when it was posted, since there is action here, we must request the individual who submitted the file. When you request files from a user, they will respond with whether you can retrieve those files or not. The specific individual cannot access the item from the repository if the owner does not grant access. If the user grants access to the file, the person can take any action they require. The four essential components are file name, user name, timestamp, state, and activity. The state will be given, and the activity will be a document action allowed just after the owner has provided the authorization.

4.2. Storage Complexity

When compared to existing methods like Dynamic Searchable Symmetric Encryption [9], Linearly-Homomorphic Encryption [11], and SPARQL [14], our schemes' storage complexity is $O(N^2)$ and $O(N + \lambda)$, correspondingly.

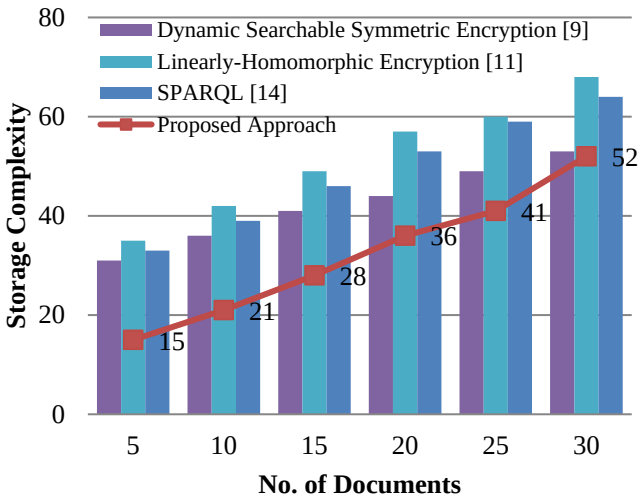

Fig. 3 Comparison of Storage complexity

In reality, the needed level of protection is supposed to be indeed achieved with a high enough security parameter λ level. Even though there are 230 documents, as shown in Fig. 3, the complexity of storage is reduced when we select $\lambda = 2^{64}$ and $\lambda = 2^{80}$ in the proposed strategies. The SPARQL schemes keep the data on the searching consumer and the cloud server, which could result in expensive storage costs for search users. While the majority of the data in Linearly-Homomorphic Encryption and Dynamic Searchable Symmetric Encryption is sent to a cloud server, which can be integrated into massive storage, the cost of the searching customer is little since only the numbers gathering D is kept there.

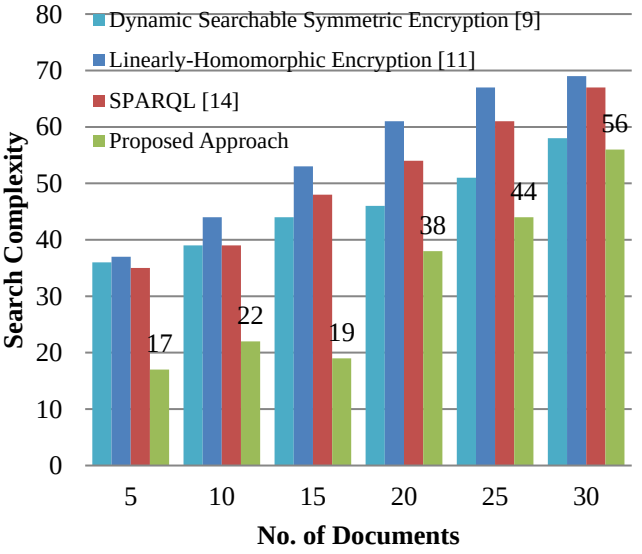

Fig. 4 Comparison of Search complexity

4.3. Search Complexity

Moreover, the search overhead of the proposed strategies, as well as the SPARQL strategies [14], is $O(N^2)$ and $O(\lambda \cdot \log^2 N)$, accordingly. Even if there are 2^{30} documents, as depicted in Fig. 4, our strategies are less search-complex than SPARQL strategies.

4.4. Query Time

The length of the dictionary and the number of documents significantly impact the calculation cost in the query phase, as illustrated in Fig. 5.

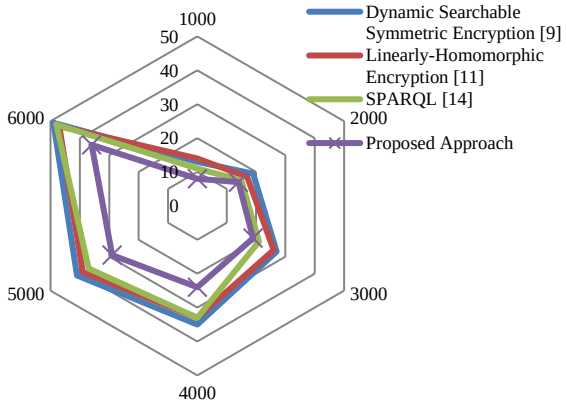

Fig. 5 Comparison of Query time

In contrast, the amount of query terms essentially has no effect. The strategies could be effective during the query stage as well. Our methods reduce storage complexity, modifying sophistication, and difficulty associated with creating indexing, a trapdoor, and a search. Exceptionally, compared to other systems, the upgrading complexity of our approaches may be nearly nonexistent.

5. Conclusion

We develop a platform for the spectrum analysis of huge matrices while maintaining privacy, which offers solid confidentiality assurance defense against sincere but inquisitive cloud providers. Secured graph data can be uploaded to the cloud by data contributors, and Using secure protocols, the analysis is conducted between the data owner and the cloud. The system successfully restricted in-house analyses to the resource-restricted data owner and storage capacity and safely outsourced the expensive analyses to the cloud. We create two privacy-preserving strategies for spectrum analyzers and investigate how they are built using additive substance homomorphic encryption (ASHE) and some degree of homomorphic encryption (SDHE).

The plaintext operands of the AHE methods must be protected from attackers, so we created masking approaches that fulfill the needed privacy guarantees while enabling the data owner to increase complexity. Large sparse matrices aid the privacy-preserving approach. We created the privacy-preserving dense data submission methodology for resource providers to find a balance between sparse data and anonymity. The approach to data sparsity dramatically lowers costs for the data owner. Using ciphertext packing in the RLWE-based approaches reduces computation overhead, while the Paillier-based methods significantly reduce online storage and data proprietors' transmission losses.

In the future, the cloud will need to seek across the complete database. It is highly wasteful and renders the technique of outsourced data-Search worthless. Future research in this field will focus on improvements for the effective verification of vast amounts of data that have already been outsourced. This technology currently only operates in partially authorized clouds, but it will eventually be expanded to include all cloud settings and can offer higher security. Additionally, we can expand our search approach in the future to employ external devices while protecting confidentiality.

References

[1] Xianrui Meng et al., “GRECS: Graph Encryption for Approximate Shortest Distance Queries,” *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 504–517, 2015. *Crossref*, https://doi.org/10.1145/2810103.2813672

[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, “Can Homomorphic Encryption Be Practical?,” *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, pp. 113–124, 2011.

[3] Cong Wang et al., “Harnessing the Cloud for Securely Solving Large-Scale Systems of Linear Equations,” *2011 31st International Conference on Distributed Computing Systems*, pp. 549–558, 2011. *Crossref*, https://doi.org/10.1109/ICDCS.2011.41

[4] D. Dhinakaran, and P. M. Joe Prathap, "Protection of Data Privacy From Vulnerability Using Two-Fish Technique with Apriori Algorithm in Data Mining," *The Journal of Supercomputing*, vol. 78, no. 16, pp. 17559–17593, 2022. *Crossref*, https://doi.org/10.1007/S11227-022-04517-0

[5] Lingaswami, and G. Avinash Reddy, “Offensive Decoy Technology for Cloud Data Attacks,” *International Journal of P2P Network Trends and Technology*, vol. 3, no. 6, pp. 23–27, 2013.

[6] D. Dhinakaran, and P. M. Joe Prathap, “Preserving Data Confidentiality in Association Rule Mining Using Data Share Allocator Algorithm,” *Intelligent Automation & Soft Computing*, vol. 33, no. 3, pp. 1877–1892, 2022. *Crossref*, https://doi.org/10.32604/Iasc.2022.024509

[7] Raphaël Bost et al., "Machine Learning Classification Over Encrypted Data," *Annual Network and Distributed System Security Symposium*, 2015.

[8] B. Murugeshwari et al., "Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network," *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 362-370, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I9P236

[9] Hongwei Li et al., "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 484–494, 2020. *Crossref,* https://doi.org/10.1109/TCC.2017.2769645

[10] Pawan Jaybhaye, and Dr. Bandu B. Meshram, "Malware Detection and Prevention on Cloud," *International Journal of Computer and Organization Trends*, vol. 9, no. 4, pp. 5-10, 2019. *Crossref,* https://doi.org/10.14445/22492593/IJCOT-V9I4P302

[11] D. Catalano, and D. Fiore, "Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data," *ACM SIGSAC Conference on Computer and Communications Security*, pp. 1518– 1529, 2015. *Crossref,* https://doi.org/10.1145/2810103.2813624

[12] Zongmin Cui et al., "A Novel Range Search Scheme Based on Frequent Computing for Edge-Cloud Collaborative Computing in CPSS," *IEEE Access*, vol. 8, pp. 80599–80609, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.2991068

[13] Bin Wu et al., "Privacy-Guarding Optimal Route Finding with Support for Semantic Search on Encrypted Graph in Cloud Computing Scenario," *Wireless Communications and Mobile Computing*, 2021. *Crossref,* https://doi.org/10.1155/2021/6617959

[14] R. Ciucanu, and P. Lafourcade, "GOOSE: A Secure Framework for Graph Outsourcing and SPARQL Evaluation," *Data and Applications Security and Privacy -34th Annual IFIP WG 11.3 Conference*, Regensburg, Germany, pp. 347-366, 2020.

[15] Dhinakaran D et al., "Mining Privacy-Preserving Association Rules Based on Parallel Processing in Cloud Computing," *International Journal of Engineering Trends and Technology*, vol. 70, no. 3, pp. 284-294, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I3P232.

[16] Sravan Kumar Nalla, and Konni Srinivasarao, "An Identity Based Authentication and Data Encryption in Cloud Computing," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 10, pp. 19-23, 2017. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V4I10P105

[17] Ming Li et al., "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," *Security and Privacy in Communication Network, Springer*, pp. 89–106, 2010. *Crossref,* https://doi.org/10.1007/978-3-642-16161-2_6

[18] S. M. Udhaya Sankar, Mary Subaja Christo, and P. S. Uma Priyadarsini, "Secure and Energy Concise Route Revamp Technique in Wireless Sensor Networks," *Intelligent Automation and Soft Computing*, vol. 35, no. 2, pp. 2337–2351, 2023. *Crossref,* https://doi.org/10.32604/iasc.2023.030278

[19] Dhruv Sharma, and C. Fancy, "Cloud Storage Security Using Firebase and Fernet Encryption," *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 371-375, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I9P237

[20] K. Sudharson et al., "Hybrid Deep Learning Neural System for Brain Tumor Detection," *2022 2nd International Conference on Intelligent Technologies*, pp. 1-6, 2022. *Crossref,* https://doi.org/10.1109/CONIT55038.2022.9847708.

[21] S.M Udhaya Sankar, V.Vijaya Chamundeeswari, and Jeevaa Katiravan, "Identity Based Attack Detection and Manifold Adversaries Localization in Wireless Networks," *Journal of Theoretical and Applied Information Technology*, vol. 67, no. 2, pp. 513-518, 2014.

[22] Ming Li et al., "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013. *Crossref,* https://doi.org/10.1109/TPDS.2012.97

[23] D. Dhinakaran, and P.M. Joe Prathap, "Ensuring Privacy of Data and Mined Results of Data Possessor in Collaborative ARM," *Pervasive Computing and Social Networking*, Springer, Singapore, vol. 317, pp. 431–444, 2022. *Crossref,* https://doi.org/10.1007/978-981-16-5640-8_34

[24] T. Sujithra et al., "Id Based Adaptive-Key Signcryption for Data Security in Cloud Environment," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 4, pp. 167-182, 2020.

[25] D.Ramya et al., "Performance Study on A Mono-Pass Solar Air Heating System (MPSAH) Under the Influence of A PCM," *Materials Today: Proceedings*, vol. 69, no. 3, pp. 934-938, 2022. *Crossref,* https://doi.org/10.1016/j.matpr.2022.07.375

[26] S. M. Udhaya Sankar et al., "Efficient Data Transmission Technique for Transmitting the Diagnosed Signals and Images in WBSN," *4th International Conference on Recent Trends in Computer Science and Technology*, pp. 251–256, 2022. *Crossref,* https://doi.org/10.1109/ICRTCST54752.2022.9781867

[27] Veena Gadad, and C. N. Sowmyarani, "Towards Privacy Preserving Data Publishing in Inter Cloud Infrastructure," *International Journal of Engineering Trends and Technology*, vol. 70, no. 10, pp. 27-34, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I10P204

[28] Hongbin Liang et al., "An SMDpbased Service Model for Interdomain Resource Allocation in Mobile Cloud Networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 5, pp. 2222–2232, 2012. *Crossref,* https://doi.org/10.1109/TVT.2012.2194748

[29] Qinghua Shen et al., "Exploiting Geodistributed Clouds for E-Health Monitoring System with Minimum Service Delay and Privacy Preservation," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 430–439, 2014. *Crossref,* https://doi.org/10.1109/JBHI.2013.2292829

[30] D.Ramya et al., "Performance Study on a Mono-Pass Solar Air Heating System (MPSAH) Under the Influence of A PCM," *Materials Today: Proceedings*, vol. 69, no. 3, pp. 934–938, 2022. *Crossref,* https://doi.org/10.1016/j.matpr.2022.07.375

[31] S.M. Udhaya Sankar et al., "Safe Routing Approach by Identifying and Subsequently Eliminating the Attacks in MANET," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 219-231, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I11P224.

[32] J. Aruna Jasmine et al., "A Traceability Set Up Using Digitalization of Data and Accessibility," *International Conference on Intelligent Sustainable Systems (ICISS)*, Tirunelveli, India, pp. 907-910, 2020. *Crossref,* https://doi.org/10.1109/ICISS49785.2020.9315938

[33] G. Gomathy et al., "Automatic Waste Management Based on Iot Using a Wireless Sensor Network," *2022 International Conference on Edge Computing and Applications*, pp. 629-634, 2022. *Crossref,* https://doi.org/10.1109/ICECAA55415.2022.9936351

[34] N. Dharini, Jeevaa Katiravan, and S. M. Udhaya Sankar, "Wireless Sensor Network-Based Detection of Poisonous Gases Using Principal Component Analysis," *Computer Systems Science and Engineering*, vol. 44, no. 1, pp. 249–264, 2022. *Crossref,* https://doi.org/10.32604/csse.2023.024419

[35] Wenhai Sun et al., "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 3025–3035, 2014. *Crossref,* https://doi.org/10.1109/TPDS.2013.282

[36] D. Dhinakaran et al., "Secure Android Location Tracking Application with Privacy Enhanced Technique," *2022 Fifth International Conference on Computational Intelligence and Communication Technologies*, pp. 223-229, 2022. *Crossref,* https://doi.org/10.1109/Ccict56684.2022.00050

[37] Jiadi Yu et al., "Towards Secure Multikeyword Top-K Retrieval Over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239–250, 2013. *Crossref,* https://doi.org/10.1109/TDSC.2013.9

[38] S.M Udhaya Sankar et al., "Mobile Application Based Speech and Voice Analysis for COVID-19 Detection Using Computational Audit Techniques," *International Journal of Pervasive Computing and Communications*, 2020. *Crossref,* https://doi.org/10.1108/IJPCC-09-2020-0150

[39] D. Dhinakaran et al., "Recommendation System for Research Studies Based on GCR," *International Mobile and Embedded Technology Conference (MECON)*, Noida, India, pp. 61-65, 2022. *Crossref,* https://doi.org/10.1109/MECON53876.2022.9751920

[40] Jena Catherine Bel D et al., "Trustworthy Cloud Storage Data Protection Based on Blockchain Technology," *2022 International Conference on Edge Computing and Applications*, pp. 538-543, 2022. *Crossref,* https://doi.org/10.1109/ICECAA55415.2022.9936299

[41] Ning Cao et al., "Privacy-Preserving Multikeyword Ranked Search Over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, 2014. *Crossref,* https://doi.org/10.1109/TPDS.2013.45

[42] S. M. Udhaya Sankar, S. Thanga Revathi, and R. Thiagarajan, "Hybrid Authentication Using Node Trustworthy to Detect Vulnerable Nodes," *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 625–640, 2023. *Crossref,* https://doi.org/10.32604/csse.2023.030444

[43] T S Arulananth et al., "Evaluation of Low Power Consumption Network on Chip Routing Architecture," *Microprocessors and Microsystems*, vol. 82, 2021. *Crossref,* https://doi.org/10.1016/J.Micpro.2020.103809

[44] T. Sujithra et al., "Survey on Data Security in Cloud Environment," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 4, pp. 155- 166, 2020.

[45] D. Dhinakaran et al., "Assistive System for the Blind with Voice Output Based on Optical Character Recognition," *International Conference on Innovative Computing and Communications, Lecture Notes in Networks and Systems,* Springer, Singapore, vol. 492, 2023. *Crossref,* https://doi.org/10.1007/978-981-19-3679-1_1

[46] R. Surendiran, and K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp. 2217-2224, 2013. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V4I5P174

[47] Yue Wang, Xintao Wu, and Leting Wu, "Differential Privacy Preserving Spectral Graph Analysis," *Advances in Knowledge Discovery and Data Mining*, Springer Berlin Heidelberg, pp. 329-340, 2013. *Crossref,* https://doi.org/10.1007/978-3-642-37456-2_28

[48] Franziska Berger, Peter Gritzmann, and Sven de Vries, "Computing Cyclic Invariants for Molecular Graphs," *Networks*, vol. 70, no. 2, pp. 116–131, 2017. *Crossref,* https://doi.org/10.1002/net.21757

[49] Richa Kunal Sharma, and Dr. Nalini Kant Joshi, "Security and Privacy Problems in Cloud Computing," *International Journal of Computer and Organization Trends*, vol. 9, no. 4, pp. 30-39, 2019. *Crossref,* https://doi.org/10.14445/22492593/IJCOT-V9I4P306

[50] Valeria Nikolaenko et al., "Privacy-Preserving Matrix Factorization," *ACM SIGSAC Conference on Computer and Communications Security*, pp. 801–812, 2013. *Crossref,* https://doi.org/10.1145/2508859.2516751

[51] P. Kirubanantham et al., "An Intelligent Web Service Group-Based Recommendation System for Long-Term Composition," *The Journal of Supercomputing*, vol. 78, pp. 1944–1960, 2022. *Crossref*, https://doi.org/10.1007/s11227-021-03930-1

[52] Leilei Du et al., "Dynamic Multiclient Searchable Symmetric Encryption with Support for Boolean Queries," *Information Sciences*, vol. 506, pp. 234–257, 2020. *Crossref*, https://doi.org/10.1016/j.ins.2019.08.014