International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Anti-Collusion and Revocation Based Approach in Dynamic Cloud Storage

Mr.N.KANNAN M.E., JALALIYA SIRAJ M, VASANTHA KUMAR S, VIKRAM M

Department of Computer Science and Engineering

EGS Pillay Engineering College , Nagapattinam

India

Abstract :-

Social networks have led to the emergence of numerous social applications for instant group communication and formation, and subgraph matching has become a popular research area in social networks. However, due to the high cost of managing and computing graph data, it may be necessary to outsource the computations to a cloud server. The main challenge is that the cloud server may leak the graph information during processing, and external attackers may modify the graph information during transmission on a public channel. Therefore, confidentiality and authentication are crucial attributes in the subgraph matching query service. In this article, we propose an efficient and privacy-preserving subgraph matching scheme that provides authentication in social networks. Our scheme allows the cloud to perform the subgraph matching query process without obtaining any sensitive information about the users. Furthermore, we achieve data integrity verification and user authentication, allowing each receiver to verify if the received messages come from the legitimate sender and have not been tampered with. Our security and efficiency analysis demonstrate that our scheme meets security requirements and achieves high efficiency in local users, making it suitable for practical applications.

Keywords:

Subgraph matching, homomorphic encryption,social network, privacy preserving, Query User,Data Owner,Cloud Server,cloud computing.

I.INTRODUCTION

Social networking sites like Twitter and Facebook have significantly transformed the way people communicate, interact, and share information online. Social network sites provide a platform for users to reconnect with old friends, build new relationships, and find like-minded individuals. Graphs are commonly used to represent social relationships in social networks due to their rich structure and semantic information. In such graphs, the vertices represent users, while the edges represent social relationships such as friendship and kinship between

users.Secure computation enables multiple parties to compute a function using their shared inputs without revealing more than necessary. The protocol can compute any polynomial time functionality with polynomial resources. This
is achieved through the use of a generic transformation process that converts an insecure computation of a function to a secure version, which is commonly known as the "garbled circuit" transformation. However, protocols generated from this transformation often have poor efficiency, especially in terms of communication complexity. The communication complexity of such protocols is proportional to the size of a circuit evaluating the functionality, which means that sub-linear communication protocols are not feasible. In there works, the subgraph matchingis a charming graph query description [6]–[9]. The subgraph matching query is defined as follows. Given a query graph H and a large original graph G, determine whether H is a subgraph of G. It is widely existed in social network applications such as social relationship retrieval and social network analysis.However, in some real-world applications over subgraph matching, the graph is extremely complex since the graph always contains a wealth of information expressing features of the graph [10]. Due to the high complexity of the graph, the graph data owner requires a large quantity of storage space to store the graph data. Thus, the limited storage space make it far more difficult for the data owner to handle the above tasks.Furthermore, even though the data owners have enough storage space to store the graph data, the data calculation and analysis may be other obstacles because of the lack of computation ability.

To address the challenges in privacy-preserving subgraph matching, the use of cloud servers has been introduced in previous schemes [7]-[10]. In this approach, the query user delegates the subgraph matching query operation to the cloud server, which then collects the necessary graph data from the data owner and performs the matching. However, this solution is not foolproof since the cloud server is an untrusted entity and may attempt to collect sensitive data from the query user and data owner. Additionally, external attackers may try to eavesdrop on the communication channels between the cloud server, the query user, and the data owner to corrupt the transmitted messages about the social network users. It is crucial, therefore, to ensure data privacy, data integrity, and user authentication in cloud-assisted subgraph matching for social networks. Sensitive data over the graph should not be exposed to the cloud server directly, and measures must be taken to prevent message tampering or identity forgery by external attackers.

In order to overcome the challenges of privacy in subgraph matching, various privacy-preserving techniques have been proposed by scholars, including anonymization and encryption. Anonymization-based subgraph query privacy-preserving schemes typically divide the original graph into at least k sub-graphs to generate multiple possible query results, making it difficult for adversaries to recognize the identity of a vertex. However, these techniques can result in heavy communication overhead, as they usually return a list of candidate results. Zhou et al. proposed a privacy-preserving method against neighborhood attacks based on k-neighborhood anonymity technology, while Liu et al. presented an identity anonymization technique based on degree sequences to prevent node degree information attacks. Chang et al. introduced a privacy-preserving subgraph matching scheme that utilizes k-automorphism technology to transform the original graph into a privacy-preserving graph, and Zou et al. presented a systematic k-automorphic network mode to avoid identity disclosure in released networks. However, these techniques have limitations and cannot address all privacy concerns, such as the information loss problem caused by changes in nodes and edges.

II.RELATED WORK

In the past research tradition on privacy-preserving algorithms in the secure multiparty computation (SMC) paradigm. The SMC paradigm defines security as computational indistinguishability from an ideal functionality in which a trusted third party handles the computation. The actual protocol is considered secure if an adversary's view of any execution can be simulated by an efficient simulator who only has access to the ideal functionality. Recent research has focused on finding more efficient privacy-preserving algorithms for specific problems, such as data mining and auctions, using techniques like Yao's protocol, oblivious transfer, and secure function evaluation. This paper aims to provide provable cryptographic guarantees of security for its constructions, following the SMC tradition. Other research has focused on statistical privacy in databases achieved by randomly perturbing individual data entries, while some work aims to bridge the gap between statistical and cryptographic privacy definitions in the SMC paradigm. Private information retrieval (PIR) is another line of cryptographic research on privacy, but its techniques and problems differ substantially from this paper's focus.

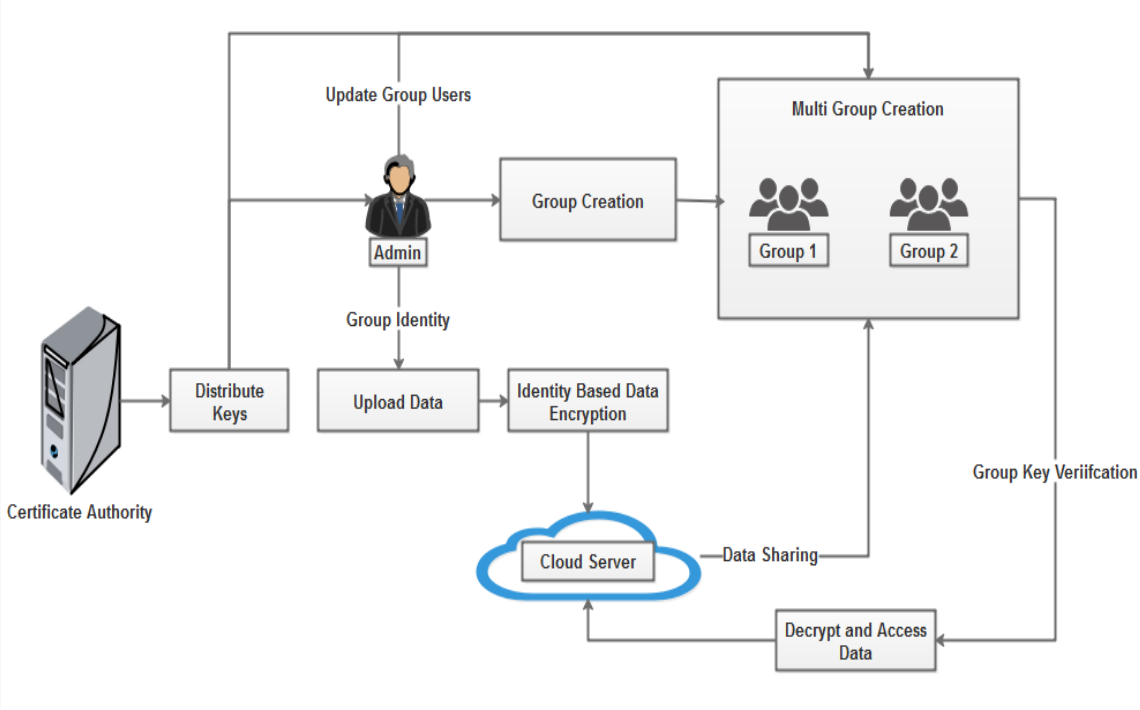
The recent approach introduced privacy-preserving protocols that enable two honest but curious parties to compute APSD and SSSD on their joint graph. However, there are still challenges in constructing privacy-preserving protocols for graph comparison, including graph isomorphism for which no known polynomial-time algorithms exist even without privacy concerns. Nonetheless, some graph comparison problems like maximum flow value comparison have reasonably efficient generic solutions. Future research can explore other interesting graph algorithms that can be computed in a privacy-preserving manner. Overall, this work opens up opportunities to apply privacy-preserving computation to graph algorithms and encourages further investigation into the field.

In recent years, privacy-preserving subgraph matching schemes have attracted considerable attention due to their applications in various domains such as social networks, web graph analysis, and bioinformatics.

Several existing studies have focused on developing privacy-preserving subgraph matching schemes. For instance, the authors in [1] proposed a privacy-preserving subgraph matching scheme based on a partially homomorphic encryption scheme. The scheme allows users to encrypt their graphs and query for subgraph matching in the encrypted domain. However, the scheme requires high computational overhead due to the use of a fully homomorphic encryption scheme.

Another related work is the scheme proposed in [2], which uses attribute-based encryption (ABE) to achieve privacy-preserving subgraph matching. The scheme allows data owners to encrypt their graphs using an ABE scheme and query users can perform subgraph matching without learning the actual graph data. However, the scheme has high communication overhead and requires a trusted authority to manage the ABE keys.Furthermore, the authors in [3] proposed a privacy-preserving subgraph matching scheme using a bloom filter-based approach. The scheme allows users to query for subgraph matching without revealing the actual graph data. However, the scheme has high computational overhead due to the use of a large bloom filter and a cryptographic hash function.Overall, while there have been several existing studies on privacy-preserving subgraph matching, the proposed scheme in this paper offers a low computation and communication overheads while satisfying security requirements.

III. ARCHITECURAL DESIGN



Working Of Secure Anti Collusion Attacks

In this work, we recommend a protected data sharing system, which can achieve protected key distribution and data sharing for dynamic group. The main contributions of our system include:

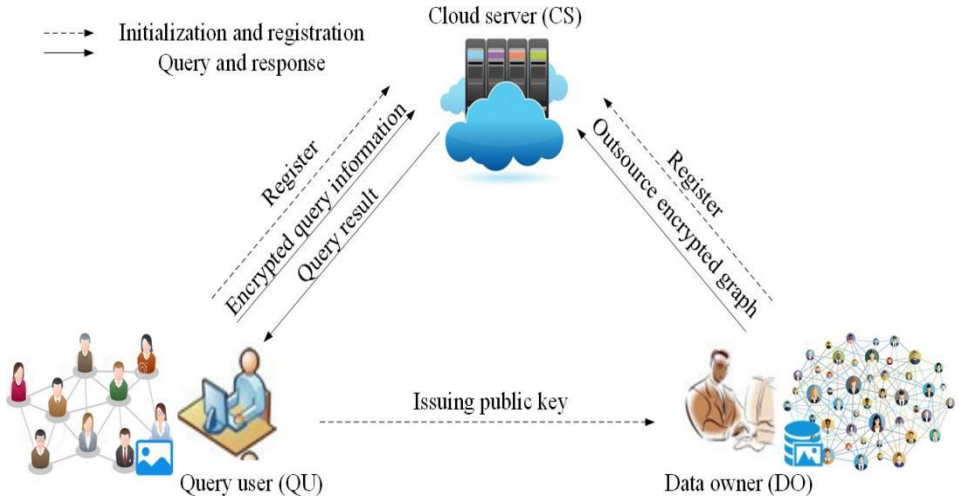
1. Our system is able to carry dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and altered.

2. We suggest a protected data sharing system which can be confined from collusion attack. The revoked users can not be capable to get the original data files once they are revoked even if they combine with the untrusted cloud. Our system can accomplish protected user revocation with the help of polynomial function.

3. We offer security examination to prove the security of our system. In addition,we also perform imitations to exhibit the competence of our system.

4. We provide a protected way for key distribution without any protected communication channels. The users can firmly obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

5. Our system can accomplish fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.



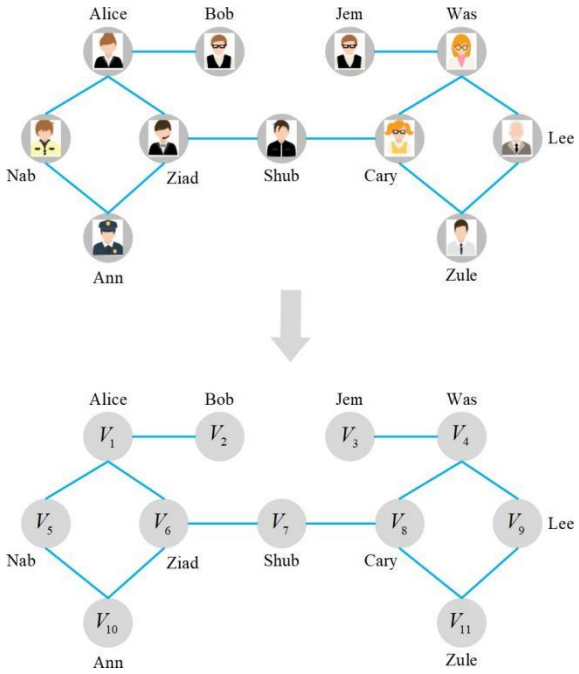
The architectural design for a secure anti collusion attack system.

Algorithm used for proposed work:

The construction of bilinear groups of a given order n is an essential component of the Boneh-Goh-Nissim algorithm. Boneh, Goh, and Nissim proposed a method for constructing such groups using elliptic curves and the modified Weil pairing. The method involves finding a prime p of the form l × n - 1, where l is the smallest positive integer such that p is prime and p is congruent to 2 modulo 3.Next, a subgroup of order n is constructed using the group of points on an elliptic curve defined over Zp. Specifically, the curve y^2 = x^3 + 1 is used when p is congruent to 2 modulo 3. Since this curve has p+1 points in Zp x Zp, there exists a subgroup of order n which is denoted by G.

Finally, the modified Weil pairing on the curve is used to construct a bilinear map e: G x G -> G0, where G0 is the subgroup of Z∗p^2 of order n. The modified Weil pairing serves as a bilinear map with the required properties for the Boneh-Goh-Nissim algorithm.Alternatively, there exist two different supersingular curves that can be used for constructing bilinear subgroups, as proposed by Galbraith, Harrison, and Soldera in 2008 [1]. The first curve is given by y^2 = x^3 + x over a prime field, while the second curve is given by y^2 + xy = x^3 + x^2 over a prime field. Both curves are supersingular and have a large automorphism group, which allows for efficient computations of the pairing.

In conclusion, constructing bilinear groups of a given order n is crucial for the implementation of the Boneh-Goh-Nissim algorithm. The method proposed by Boneh, Goh, and Nissim involves using elliptic curves and the modified Weil pairing to construct a bilinear map with the required properties. Additionally, there exist alternative methods such as using supersingular curves with large automorphism groups, as proposed by Galbraith, Harrison, and Soldera.



Graphical representation of social network data.

The Boneh-Goh-Nissim algorithm is a public-key cryptosystem that allows multiplication of text messages only once. It is based on the Subgroup Decision Problem, which is the problem of determining whether an element x of a cyclic group G belongs to a specific subgroup of G, without knowing the factorization of n = q1 × q2, where q1 and q2 are chosen to be distinct large primes. To perform a single multiplication of messages, the algorithm requires the use of a bilinear pairing, which is a map that satisfies bilinearity and strong non-degeneracy properties. There are different types of bilinear pairings used in cryptography, including the Weil pairing and the modified Weil pairing, which is equipped with a distortion map to ensure strong non-degeneracy. Efficient calculation algorithms for the modified Weil pairing are available in the literature.

System design :

1. Cloud sharing framework:

- In this module, can create cloud storage framework
- Includes group manager, certificate authority, cloud server and users
- Group manager can be provide the data to cloud

2. File Upload:

- Group manager can be upload the files into cloud in secure manner
- And implement encryption algorithm to encrypt the data
- Multiple group managers are available in the cloud server

3. Key distribution scheme:

- The communication entities can securely negotiate the public key and distribute the private key
- Group members are registered to pick group managers from drop down list
- Group manager obtain the correct message which is sent by the legal communication entity

4. Access control:

- From the group user list, which is generated by the group manager
- This operation is generally performed by the cloud.
- The cloud verifies the identity of the group manager by checking access mechanisms

5. Revocation scheme:

- Implement dynamic group management system to handle backward and forward security
- Removing user from the group user list in the local storage space and updating the group user list which is stored in the cloud.

6. Security:

- The System must ensure the security and privacy of user and prevent unauthorized access or misuse of the system. This may secure authentication methods, and regular software update to address potential security vulnerabilities.

1V. PERFORMANCE METRICS

In this section, the performance evaluation of a proposed system is presented with respect to three main aspects: computation cost, communication cost, and system features. The computation cost is calculated using the Pairing-Based Cryptography (PBC) library on a laptop with a 64-bit Windows 10 Multiple Editions operating system, an Intel Core i5-7500 CPU with a clock speed of 3.41 GHz, and 12 GB of memory. A large prime number q with a length of 512 bits is selected, and the elements in G and GT are 512 bits and 1024 bits, respectively. Additionally, the timestamp, identity, hash function, and message authentication code have lengths of 64 bits, 32 bits, 256 bits, and 256 bits, respectively.

For simulation purposes, a graph with 10-100 vertices is generated, and the simulation parameters are presented in Table II. The concrete runtime of cryptographic operations is listed in Table IV. These results demonstrate the efficiency of the proposed system in terms of computation and communication cost. It is important to note that the system's features, such as its security and usability, should also be considered when evaluating its performance. Overall, the presented evaluation provides a comprehensive analysis of the proposed system's performance in various aspects, allowing for a better understanding of its potential applications and limitations.

Accessibility:

Accessibility refers to the ease with which authorized users can access the subgraph matching scheme. The scheme should be user-friendly and easy to use. It should not require complex computations or additional hardware.

Moreover, the scheme should be easily integrated into existing social network platforms. High accessibility ensures that the scheme can be widely adopted and used to secure social networks.

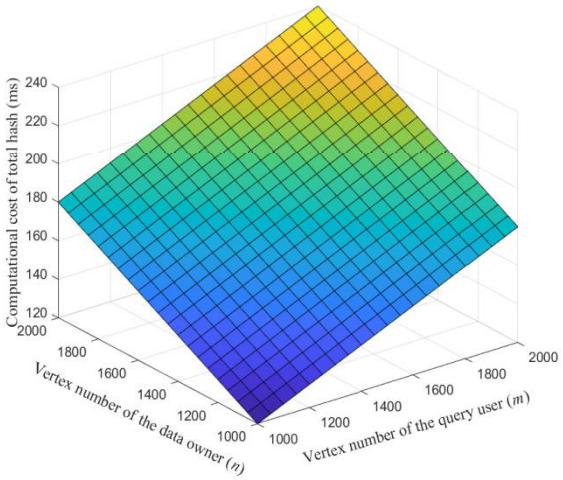
Security:

Security is the most critical performance metric in privacy-preserving subgraph matching schemes. The scheme should be able to protect the privacy of users and their data against unauthorized access and attacks. The scheme should prevent the leakage of sensitive information, such as user identities, social network structure, and subgraph matching results. Additionally, the scheme should resist attacks, such as replay attacks, man-in-the-middle attacks, and dictionary attacks. Robust security ensures that the scheme can provide reliable protection to social networks and their users.

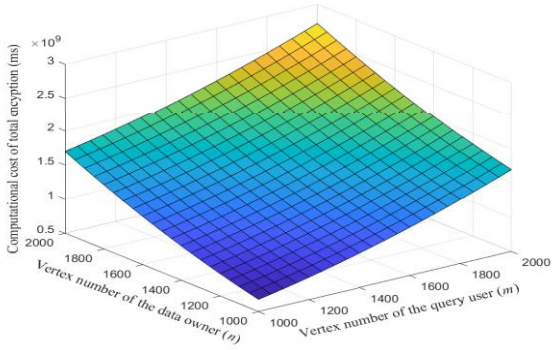
Efficiency And Productivity

Efficiency and productivity are important performance metrics for any privacy-preserving subgraph matching scheme in social networks. The efficiency of a scheme is determined by how fast it can perform the required computations and generate results. In the case of subgraph matching, the scheme's efficiency is determined by how fast it can search for a matching subgraph in a large network. The productivity of a scheme is determined by how accurately it can match subgraphs and authenticate users.

To ensure efficiency and productivity, the scheme should be designed with a low computation cost and a high accuracy rate. The computation cost can be minimized by selecting appropriate cryptographic primitives and



Computational cost of total hash operation on the proposed scheme



Computational cost of total encryption operation on the proposed scheme

optimizing the algorithm's implementation. The accuracy rate can be improved by using advanced graph matching techniques and authentication mechanisms.

Additionally, the scheme's scalability and flexibility are also important performance metrics. The scheme should be able to handle large-scale social networks and adapt to changes in the network structure. This can be achieved by designing the scheme with a distributed architecture and incorporating dynamic graph analysis techniques.

Overall, a privacy-preserving subgraph matching scheme with authentication in social networks should aim to achieve a balance between efficiency, productivity, scalability, and flexibility to provide reliable and secure subgraph matching services in social networks.

V. CONCLUSION

In conclusoion, we present a privacy-preserving subgraph matching scheme with authentication in social networks. The proposed scheme is efficient and based on Boneh-Goh-Nissim public key encryption technique, which allows users to access cloud service without compromising their graph information. The cloud server helps the query user to collect graph data from the data owner and performs subgraph matching operation while maintaining data confidentiality. The scheme also employs message authentication code to ensure data integrity verification and user

authentication. The security analysis shows that the scheme satisfies the security requirements.The proposed scheme is computationally efficient, and communication overhead is low, making it suitable for practical applications. The proposed scheme has the potential to improve productivity by allowing users to perform subgraph matching without disclosing sensitive data. It also enhances accessibility to cloud services while maintaining privacy. Overall, the proposed scheme is a significant contribution to the field of privacy-preserving subgraph matching with authentication, which has a wide range of applications in social networks, healthcare, finance, and other fields that require secure data processing.

VI. REFERENCE

[1]X. Ding, C. Wang, K.-K. R. Choo, and H. Jin, "A novel privacy preserving framework for large scale graph data publishing," IEEE Transactions on Knowledge and Data Engineering, 2019.

[2]M. U. Arshad, A. Kundu, E. Bertino, A. Ghafoor, and C. Kundu, "Efficient and scalable integrity verification of data and query results for graph databases," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 5, pp. 866–879, 2018.

[3]X.-Y. Li, C. Zhang, T. Jung, J. Qian, and L. Chen, "Graph-based privacypreserving data publication," in IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. IEEE, 2016, pp. 1–9.

[4]J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," IEEE communications surveys & tutorials, vol. 18, no. 3, pp. 1974–1997, 2016.

[5]H. Jin, C. Lin, H. Chen, and J. Liu, "Quickpoint: Efficiently identifying densest sub-graphs in online social networks for event stream dissemination," IEEE Transactions on Knowledge and Data Engineering, 2018.

[6]S. Sun and Q. Luo, "Scaling up subgraph query processing with efficient subgraph matching," in 2019 IEEE 35th International Conference on Data Engineering (ICDE). IEEE, 2019, pp. 220–231.

[7]Z. Fan, B. Choi, Q. Chen, J. Xu, H. Hu, and S. S. Bhowmick, "Structurepreserving subgraph query services," IEEE transactions on knowledge and data engineering, vol. 27, no. 8, pp. 2275–2290, 2015.

[8]L. Hong, L. Zou, X. Lian, and S. Y. Philip, "Subgraph matching with set similarity in a large graph database," IEEE transactions on knowledge and data engineering, vol. 27, no. 9, pp. 2507–2521, 2015.

[9]A. Dutta, J. Llados, H. Bunke, and U. Pal, "Product graph-based higher ´ order contextual similarities for inexact subgraph matching," Pattern Recognition, vol. 76, pp. 596–611, 2018.

[10] Y. Lou and C. Wang, "Osmac: Optimizing subgraph matching algorithms with community structure," in 2019 IEEE 35th International Conference on Data Engineering (ICDE). IEEE, 2019, pp. 1750–1753.