Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 4716-4725*

Research Article

Secured Multi-Party Data Release on Cloud for Big Data Privacy-Preserving Using Fusion Learning

Divya Dangi[a], Dr. G. Santhi[b]

[a] (Ph.D. Research Scholar), [b](Associate Professor)
[a,b] Department of Computer Science and Application, Sarvepalli Radhakrishnan University, NH 12, RKDF IST Campus, Hoshangabad Road, Misrod, Bhopal (M.P.)

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Previous computer protection analysis focuses on current data sets that do not have an update and need one-time releases. Serial data publishing on a complex data collection has only a little bit of literature, although it is not completely considered either. They cannot be used against various backgrounds or the usefulness of the publication of serial data is weak. A new generalization hypothesis is developed on the basis of a theoretical analysis, which effectively decreases the risk of re-publication of certain sensitive attributes. The results suggest that our higher anonymity and lower hiding rates were present in our algorithm. Design and Implementation of new proposed privacy preserving technique: In this phase proposed technique is implemented for demonstrating the entire scenario of data aggregation and their privacy preserving data mining. Comparative Production between the proposed technology and the traditional technology for the application of C.45: In this stage, the performance is evaluated and a comparative comparison with the standard algorithm for the proposed data mining security model is presented.

Keywords: Privacy-Preserving, Fusion Learning , Cloud Computing, Cryptography

1. Introduction

Among the privacy issues of cloud [1]We differentiate amongst the following: The deceptive conduct of the cloud provider: The cloud server may be malicious or interested and may inappropriately interpret, use or remove user data. Indeed, an inefficient supplier is in a place to take and analyze secure user data and constantly review it in an uncertain manner such that user data can be accessed. Frequency Analysis Attack[2], repeated User Problems Evaluation, and Surface Analysis Attacks can be seen as significant obstacles that could jeopardize the privacy of outsourced info cloud providers. Later in this survey, several implementations block the server from learning the results of the user.

Lack of consumer control: there is little connectivity, control and processing of cloud usage data and applications. There are longer networks for consumers. The underlying cloud infrastructure is often not controlled or governed, but rather selective oversight and control of the use of management interfaces by the service provider. In comparison, the expertise of customer care depends on a service model.[3]

Malicious outsiders: Cloud's various resource retention and pooling features can jeopardize the privacy of cloud customers. In fact, the share of virtualized and pooled platforms offered free trial opportunities and unregulated usage of the network and resources in multi-site public cloud environments at a cheaper price would allow risky cloud subscribers to exploit information from lawful users who have access to the same tools, not just violating the security, but also distributing it to other victims.[4]

Attain conformity with regulations: difficulties of preserving compliance across many locations across the globe that may contribute to legal trouble by choosing to move from one cloud to another.[5]

Data proliferation: Many cloud providers ensure the duplication of data and copies in separate data centers[8]. In comparison, data transactions through the cloud and potentially to data owners are unchanged. Therefore, a third party server could be in violation of the records.[6]

Information disclosure**:** Cloud data protection and homomorphic encryption faces several obstacles. In fact, there are still many limitations of encryption technology, including operational complexities, unreliable implementations, poor encryption keys, and the need to perform certain operations on decrypted data on cloud servers. It would damage the protection of the user's data if the confidential data is disclosed.

Dynamic provision: Responsible group is responsible for ensuring confidentiality related to cloud nuances. In addition, certain services could be malicious by the dynamic delivery of cloud subcontractors engaged in data collection by customers. As a result, the consumer is not expected to process his data properly and no longer trusts the sub-providers. [7] Report to the Council of Ministers.

Secondary unauthorized use: there is a risk that data stored or handled in the cloud could not be utilized. For instance, the cloud provider can sell private data to its rivals in order to obtain revenue.

In this stage, the performance is evaluated and a comparative comparison with the standard algorithm for the proposed data mining security model is presented.

2. Related Work

J. C. Lin, et al[1] This paper proposes a new Privacy and Safety Mining Framework focused on Data Mining and Privacy Protection. PPSF is an open source data mining library that offers a range of algorithms: (1) data safety, (2) data mining data security, and (3) mining protection capabilities (PPUM). PPSF has a user-friendly gui that lets algorithms operate and display findings and is a continuing project with new algorithms that are continuously being written, refined and documented.'Z. Ma, et al[2] Kalman Filter Ensemble Relies on the Likelihood Transfer Position Matrix Users shall be used for predictive calculation to ensure data availability. In order to provide better protections for high user intensity regions, we are also developing a data delivery structure that is based on the weight of regional private life. RPTR not only maintains the security of trajectory information in real-time, but also guarantees the availability of data by its analysis and testing.

P. R. Nivetha et al[3] The primary goal in protecting privacy is to extract details and to provide a series of data without the publication of private data. Sequential data appears to predict the next event, which may threaten the protection of sensitive data. We looked briefly at sequential patterns, k-anonymity, data destruction and safe quantity computing techniques for data sharing conservation issues.

H. Cao et al[4] In this article, we present an explicitly private system for protecting the privacy of energy on the Internet. Our goal is to release aggregate data from the data owner after additional noise in scattered data. Theory shows and checks that our approach can meet the objective of data protection and usability.

D. Yang, et al[5] Analytical review of both virtual and real-world data sets demonstrates that our design can efficiently and consistently protect privately identifiable users while maintaining the accessibility of obscured data for personalized rating advice. PrivRank maintains both a higher degree of privacy protection across all the ranking-based guidelines we tested and a higher level of utility than the state-of-the-art approaches.

S. Sharma et al[6] This paper introduces a modern data model that safely integrates distributed data vertically partitioned by adding encryption to suitable characteristics that lead to privacy leakage and also allows data owners to reclaim their data after incorporation. In addition, we use CART algorithms on integrated data sets and contrast the impact with C.45 algorithms to compare various parameters.

3. Proposed Methodology

Data outsourcing is becoming a popular concept that enables customers and businesses to leverage external resources. Selective methods of access must be implemented where compilation and distribution do not include open-ended objects. In this respect, the service provider, who is effective in carrying out the distribution but is not allowed to access the information, often allows the data owner to supply their data. Row-Based Encryption: proposed a novel explanation for querying distantly stored data, while preserve their privacy. The author presuppose that a little security constraint are definite on outsourced data identify which sets of attributes cannot be unrestricted together and which attributes cannot illustrate in plaintext. To guarantee constraint approval, the authors propose to vertically section the general relation, decomposing the database into two fragments that are after that stored on two dissimilar servers. The technique is based on the assumption that the two servers do not trade information and that everyone the constraints can be fulfilled by encrypting immediately a little attributes in every fragment.

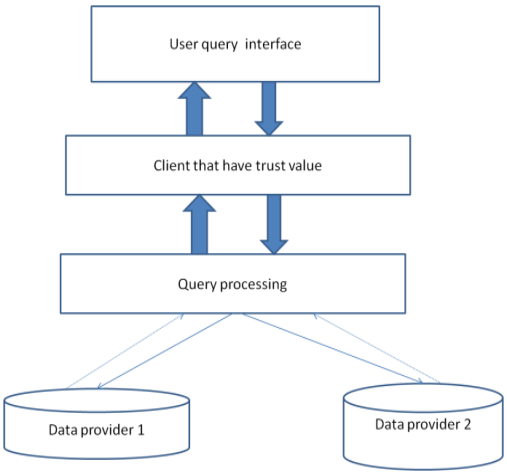

Figure 1: user query interface

The key is that the consumer will delete his data from two, judiciously free systems with databases that cannot communicate to each other. The dissemination of information is carried out in a manner that means that there is no violation of the safety of the perception of the substance of a certain database. The customer carries out queries by submitting relevant sub-questions into each database and eventually assembling the customer-side results. In this case, a unique name and the number of the cargo card could constitute a serious violation of security. It may not, however, be a major ordeal to uncover the name alone or unassisted Mastercard number. In these cases, when putting your Visa figure away, we may put your names in the single database, but refrain from scratching any quality.

4. Classification Method

The outsourced database imitation is an example of the perceived client server standard. External database providers are responsible for hosting outsourced databases and providing their clients with a strategy for supplying, storing, revising and questioning their databases. We need to explain the importance of the articulate customer before the production is booked. In this context, for example, the customer is not essentially a solitary substance. For example, a responsible consumer may be referred to as an association or an agreement with authorized clients as an alternative to a managerial substance. The consumer is known in the outsourced database to assume that the server stores knowledge on an ongoing basis. In particular, the replication, reinforcement and opening of outsourced databases that are stored depends on the server. Therefore, the transparent content of the database and/or the uprightness of this substance are not certain of the consistency of the server. This be insufficient in

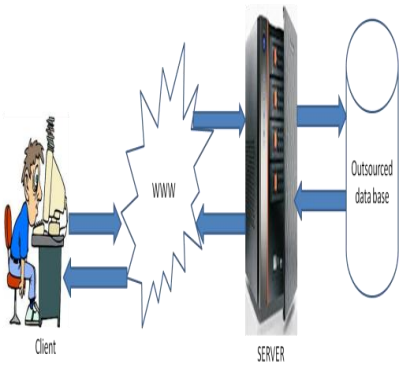

Figure 2: user selects the dataset

of trust is discriminating, as it open up novel security issue and serves as the boss boost for our work. We separate amongst the three kind of the outsourced database reproduction: The almost everybody essential setting is the place each outsourced database is utilized by a specific element, the customer who makes, controls, and inquiries the information. We allude to it as the incorporated customer copy . In the further progressed multiquerier imitation we separate amongst two sorts of customers: proprietors and questions. The past is the distinct information proprietor who includes, erases, and upgrades database tuples. In contrast, a querier is simply admissible read-access (i.e., question benefits) to the database or parcel thereof. This distinction is both vital and characteristic, as it mirror a considerable measure of certifiable database situation.

In apply, a questions may be a computationally feeble and stockpiling tested gadget, for example, a mobile phone or a remote PDA. moreover, the transmission capacity realistic to a querier may be entirely constrained because of correspondence middle distinction the battery force enlivened by getting gigantic measures of information.

In third, basically basic, outsourced database copy a solitary database can have a few proprietors (for a known customer database). This is alluded to as the multiowner copy. The contrast between the multiquerier and multiowner copy can develop controlled. In the past, a solitary security key make and control database tuples, while in the last, different tuples can be made by dissimilar security principal. However, in together replica there can be numerous queriers. The incentive for the multiowner replica is straightforward: believe the instance of an outsourced user database. every tuple in this database is created and maintain by the user dependable for a scrupulous user. A user then own the tuples that he or she generate.

Number of Secret Keys and Scalability

One of the significant issues in uphold passageway control by means of segregating encryption is the figure of mystery keys that each client must keep safely. In our methodology, each client necessities essentially to protect one mystery key to become acquainted with every last bit of her approved assets, which is very much leverage. This point of interest is a consequence of utilizing a mutual quality for every asset's mystery esteem which is put away alongside each asset there by the permitted client can ascertain the asset's mystery esteem smoothly.

Fitness of operation especially strategy redesign operation is one more renowned component. developing the quantity of clients does not inspire any extra endeavor to the framework. also, the time intricacy for stipend and withdraw is stay polynomial as Garner's calculation infer, which help the versatility of the determination. Hypothesis determination, as per an ingenious calculation in. besides, the aggregate many-sided quality of yielding or deny protected rights is valuable by the many-sided quality of the mystery esteem encryption which is perform for each approved client. In this way, utilizing a direct encryption system, a gift or withdraw operation has a period unpredictability contrast and the methodology in our procedure the client does not need to get a great deal of keys to contact her passable assets. Along these lines, get to the assets is extra skilled here and does not oblige various cooperations with the server to drive the suitable keys. In our methodology, protection of security arrangements is safeguarded close to both the server and clients as reached out as the clients are unknown. The server, normal clients, approved clients, and some subject get to the server can't repossess or finish up any proprietor embrace access control arrangement. This is the result of the with shared qualities in its place of key starting strategy in our methodology assignment of access control authorization to the server is likely by means of key inference by the client. Our proposed methodology, apply to share a mystery esteem among approved clients, and clients only unscramble the common qualities to get the fitting mystery values. No data is uncovered even after unscrambling. each client or some other inside or outside gathering, just on account of the approved clients' keys proprietorship will have the capacity to perceive admissible clients from. Then again, in our methodology the clients' mystery keys are unspecified to be private and hence the past data spillage is incomprehensible.

Save Privacy of User Integrated clarification

In our strategy the client taking after figuring assets' mystery qualities, sends them to the server amid a mystery channel. In the event that they are precise, the server gives back the equal approved assets to it. Here, to actualize access control, the server doesn't oblige knowing the client singularity, so it could smoothly be helpful in a mixed bag of outsourcing situation where various client protection concern require clients to be unknown. we address the trouble of how to put into impact access control arrangements in a circumstance where information is put away and realistic to clients by an outside server. We proposed a capable clarification with a specific end goal to complete access control requirement on outsourced information taking into account hypothesis. Our clarification shields protection of access control strategies from unapproved clients and in addition the un trusted server. In examination with the related work, in our procedure customer side computational intricacy and in addition the quantity of associations among the customer and the server has been consolidated subsequent to of shared worth solicitation rather than key starting strategies. Such a strategy is adaptable close by access control arrangement element changes and keeps the quantity of fundamental keys restricted. It likewise monitor the protection of approval strategies with no assistant endeavors.

In this part, we introduce a model for securing access to outsourced databases. Encryption is the customary path in which an outsider can be kept from getting to data it would have generally access to [5]. Our proposition is taking into account the use of column based encryption as an intends to uphold verification and classifiedness. The proposed model additionally gives an answer for effective administration of arrangement overhauls, constraining the appropriation of lavish re-encryption procedures.

Model And Assumptions

The model, is made out of a Database Owner, Service Provider and clients related to the Database Owner [2] [12] [15]. In the proposed model, neither the Database Owner, nor the client must be dependably on-line, yet Service supplier is dependably on-line as in [2] [12]. At first, client registers itself with the Database Owner, who thusly gives encryption key and token to the client.

The proposed plan accept that the calculation utilized for era of encryption keys is secure with the Database Owner. Each new client needs to enlist itself with the Database Owner. Database Owner conveys this database to the Service supplier in the wake of encoding every one of the columns (containing secret data which can uncover character of the client) utilizing the relating encryption keys.

Presently valid client's solicitation is coordinated to the Service Provider, who thusly handle client questions in a secret way. This plan accept that no outcast can break Service Provider's security. Correspondence between Service Provider and clients is made secure utilizing an altered Diffie-Hellman Key Exchange [16] and Public Key Encryption. D-H Key trade is picked, as it produces mystery session keys every time the session lapses. With the session's assistance key, proposed plan accomplishes secure information trade as an one of a kind key is traded every time for each new session.

Proposed Algorithm

The proposed methodology comprises of a changed column based encryption procedure which helps us to accomplish secure and productive information access control. The proposed approach likewise utilizes specific encryption and stored line sets (rather than result sets) to build execution of the framework. In this segment pseudo code of the calculations and the documentations utilized as a part of it are additionally given. An illustration of the proposed plan that shows likeness of it with the genuine situations is additionally portrayed in Figure 2

The conventional database outsourcing model is indicated in Figure 1, where entire database

is scrambled utilizing a solitary key, and that key is appropriated to the clients. The suspicion

is just restricted to shielding information from the Service Provider, while the clients have full access to the database [12]. Then again, in a certifiable situation complete access to the entire database is not worthy. In this situation for the most part over-encryption or token based verification is utilized to handle denial. Rather than these security primitives, there is a probability of conspiracy assault in which a malevolent client passes the way to the Service supplier to achieve full access to the database. To stay away from this Database Owner needs to reencrypt the entire database with another key which is unrealistic in a genuine situation. Along these lines, there is a need to actualize an instrument which can permit a controlled and secure access to the outsourced databases.The client points of interest which are sent to the Database Owner and the inquiries' aftereffects which are acquired from Service supplier must be secured in travel, to counter any security dangers from the noxious untouchables. The proposed plan discloses how to accomplish the obliged security measures and productive access control.

Illustrative Example

The proposed plan is outlined by the sample indicated in Figure 5. Here, the proprietor can be a bank who transfers his record holder's subtle elements on to the Service Provider's server and the client is a client (account holder) having a record in the bank who access his record points of interest from the Service Provider's server. At whatever point another client opens a record in the bank, a passage is made for the client containing his own and record subtle elements. Private points of interest (which can uncover the account's personality holder) are scrambled utilizing a remarkable key, and the rest are kept as it may be. At that point the came about passage is conveyed to the Service Provider. Bank stores Primary key and Encryption key comparing to the client in the table kept up with the bank. Finally, Bank conveys a bundle containing UID, record number, encryption key and a token to the client.

This data is utilized by the client later on to recover it's record points of interest from the Service Provider's server. The proposed methodology utilizes MD5 calculation [16] for message honesty, and session keys (created with the assistance of D-H key trade calculation) for privacy.

Data Transfer From Database Owner To Service Provider

The procedure that the Service Provider uses after receiving data tables and revocation

list from the Database Owner is illustrated in algorithm 1. Service Provider decrypts the

Algorithm 1 : Steps followed by Service Provider, after receiving data table and revocation list from Database Owner.

Step 1: Storing encrypted database tables and revocation list

ResultSet0 Receive(EKPUSP (EKPRDO(RevoList));

ResultSeti Receive(EKPUSP (EKPRDO(ETi));

Step 2: Updating the Database

Ti DKPRSP (DKPUDO(ResultSeti));

Step 3: Updating Revocation List

RevoList DKPRSP (DKPUDO(ResultSet0));

Message using the Database Owner's own private key and public key, and stores encrypted data tables and a revocation list in their storage. Since data tables are protected using a line-based encryption method, and the service provider does not know the encrypted row keys, actual data cannot be known to the service provider. The Service Provider Revocation List contains the UID of revoked users. Therefore, when the user request is met, the revocation list matches its UID. If the user UID is in the list, the user application will be rejected.

Key Acquisition Phase

The procedure for protecting the keys as seen in calculation 2. The customer shall contact the owner of the database for the keys that he or she may use to further connect to the owner and service provider of the database. The Database Owner then sends an open/private key and a symmetry key to access the line of user points of interest. This is done by the user of the archive.

Calculation 2 : Key procurement stage.

Step 1: User asks for the DO for the keys.

Send(EKPUDO(EKKS (N1jjreq)jjKS));

Step 2: DO reacts with open/private keys and a symmetric key.

Receive(EKKS (EKPRDO(N1jjreqjjKjjPRUSRjjPUUSR)));.

User Registration Phase

The method obliged when another client is to be included is portrayed in calculation 3. New client needs to send an enrollment solicitation to the Database Owner. Database Owner makes a section for the client containing his subtle elements and afterward creates a key utilizing a calculation. Database Owner encodes the section with that key. At that point Database Owner stores Primary key and Encryption key relating to the client in the table kept up at its end and conveys that encoded passage to the Service Provider (section is initially scrambled with its private key and afterward by open key of the Service Provider with the end goal of confirmation and secrecy between Service Provider and Database Owner). Finally, Database Owner conveys a parcel containing UID, encryption key and a token to the client. This data is utilized by the client later on to recover his points of interest from the Service Provider's server. The nonce and timestamps in the solicitation and answer message fill the need of replay and man-in-the-center assault evasion.

Calculation 3: Algorithm for enlistment of another client

Step 1: User sends a scrambled enlistment solicitation to Database Owner.

Send(EKPUDO(EKPRUSR(UserDetails)));

Step 2: Database Owner upgrades Key Constraints table at its end

KeyTable add(UID;EKUi);

Step 3: Database Owner encodes the column and sends it to the Service Provider.

Send(EKPUSP (EKPRDO(EKUi(rowUi))));

Step 4: Service Provider Updates its duplicate of the database

DBSP insert(DKPUSP (DKPRDO(EKUi(rowUi))));

Step 5: Now the client can straightforwardly contact Service Provider for recovering his subtle elements.

Communication between Service Provider and User

After the keys and token are conveyed to the client, client can demand Service Provider for the points of interest. On the off chance that UID of the client is not present in the disavowal rundown, D-H is started by Service Provider. This satisfies the configuration target of not keeping the Database Owner constantly on the web. Calculation 4 portrays the utilization of Modified D-H key trade calculation to get a common session key KS with the end goal of secure correspondence between Service Provider and client. The proposed plan utilizes Modified D-H key trade [16] to avert man-in-the-center assault by scrambling the Diffie-Hellman parameters and utilizing nonce as a part of every bearing.

Administration Provider scrambles the question result (ri) and it's process (Di) utilizing the common session key KS which is created from the Modified D-H key trade [16]. This sort of encryption guarantees secrecy of the message between Service Provider and client as nobody has the capacity perused the message with the exception of the client. Session key stays legitimate for a predefined span of time which guarantees secure correspondence over a duration of time. The client decodes the message after getting an encoded reaction. After decoding client at long last have entry to data identified with him in a safe and proficient way

Calculation 4 : Algorithm for secure correspondence between Service Provider and client

Step 1: User sends demand for information access to Service Provider.

Send(UID; Token; q;N1);

Step 2: Service Provider checks denial rundown if the client is not in the rundown then just inquiry is handled

StorageArray Receive(UID; Token; q);

in the event that (StorageArray[1] == RevoList(UID)) then

Goto step 7

else

Goto step 3

end if

Step 3: Service Provider and client trades a session key Ks created with the assistance of changed D-H Key Exchange Algorithm.

Step 4: Service Provider scrambles the information utilizing shared session key

EOi EKs(EKUi(rowUi));

Step 5: Service Provider sends the scrambled information to the User

Send(EOi;N1 + 1);

Step 6: Exit;

Step 7: Service Provider sends a dismissal message to the User

Send(request can't be allowed);

Read and Write Operations

The execution procedure of read and compose operations is demonstrated in Figure 6. In the proposed methodology, stored line sets are utilized rather than result sets, as reserved column sets doesn't oblige a database association. When client presents his login points of interest, an encoded RowSet is made, which dwells with the server's occurrence process with which the client is conveying.

At whatever point read operation is performed by the client, subtle elements are perused from stored column set just, and whatever progressions he has made are overhauled to the database living with the Service Provider. RowSet is revived after a general interim of time. This methodology helps in enhancing simultaneousness, and keeping up consistency at the database. In this section, various cryptographic primitives are analyzed in terms of their scalability and strength.

Data Confidentiality

Information confidentiality may be an important concern with the outsourcing of information since information can be sensitive and repair services are not inside the protected realm of the information owner. The details cannot then be kept at the service provider in an unencrypted way. The assigned theme uses row encoding

per row with a distinctive key is encrypted. As the row size is too little, after the encoding has been finished the ciphertext is also small. This kind of encoding is also pretty much like a single pad. In cryptanalysis it has only been attempted to once pad (OTP) coding once. Thus, utilizing this method of coding unbreaks this paradigm, which means the knowledge remains confidential.

Authentication

Line-dependent encryption itself means that the consumer validates when the customer's key is scrambled via a column containing the customer's points of interest. The column will now be open to a single person. The current system utilizes tokens given to the user during the registration season to guarantee that the rejection is carried out.

Integrity

The draft proposal used the calculation of MD5 hash and revised the key Diffie-Hellman trade[16] to maintain confidentiality of data. Altered D-H industrial key calculations are used for various keys to differentiate sessions. To secure interactions between the provider and the client, encrypt the data using the session keys.

Performance Analysis

To the implementation, the proposed solution avoids a large portion of the processing costs by comparing various security approaches, e.g. over-encryption. Unlike the whole database, the new proposal would scramble lines from the database. So planning SQL queries is anything but complicated, and complete database re-encoding is not required if consumer rights are waived. The strategy is categorized into importance, expenses for estimates, competitiveness etc. and the perceptions are outlined below.

Applicability

Bennani [2] Plan employs numerous RSA encryption, which forces customer gadgets to do a lot of computational work. This technique is not relevant to cell phones, as the bandwidth of mobile phones is small. Once again, the new plan provides for the usage of fewer computational AES encryption and is related once. It's again. Using AES cryptography, the appropriateness of the proposed technique is finally expanded.

Cost Efficiency

The cost depends on the number of the inquiries and projections for the outsourcing of the platform. The decoding and encoding of the Service Provider portion of Bennani[2] is done several times. This improves the cost of the forecasts. Clearly, the new proposal helps the Service Provider to resolve a problem concerning the reduction of costs.

Concurrency

The proposed strategy is profoundly attuned to the server side protocol at any point the client signs in. The user can now carry out all manner of activities, such as reading and writing on this foot. While the article on the line set does not have a relation between a database and a job that is separate from the result set entity, the structure increases. This approach also protects progress, when the user has evolved online as the updates are continuously updated to the database.

5. Conclusion And Future Work

Data mining can extract substantial knowledge in a broad variety of datasets-often split into different classes. The main objective of data mining protection is to locate global mining results while maintaining private data/information on individual sites. In the case of multiple partitioning methods, such privacy conservation fusion algorithms are proposed following privacy restrictions. Different author methods, such as randomization, disturbance, heuristic and cryptography techniques, are presented in horizontally and vertically partitioned datasets to locate privacy-preserving link rule. This thesis analyzes and compares the results of a variety of fusion algorithm methods. Crypothecary technology algorithm, homomorphic encryption, robust scalar product to satisfy privacy criteria in vertically partitioned databases. Algorithm incorporating cryptosystal RSA Public Key as well as Homorphic Encryption Schemes as well as Lateral Partitioned Database algorithms. This paper discusses the broad procedures used in the mining association rules for the dissemination of results, while protecting confidentiality.

References

J. C. Lin, P. Fournier-Viger, L. Wu, W. Gan, Y. Djenouri and J. Zhang, "PPSF: An Open-Source Privacy-Preserving and Security Mining Framework," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 1459-1463, doi: 10.1109/ICDMW.2018.00208.

Z. Ma, T. Zhang, X. Liu, X. Li and K. Ren, "Real-Time Privacy-Preserving Data Release Over Vehicle Trajectory," in IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 8091-8102, Aug. 2019, doi: 10.1109/TVT.2019.2924679.

P. R. Nivetha and K. T. Selvi, "Techniques for privacy preserving data sharing: A survey," 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Coimbatore, India, 2014, pp. 1-1, doi: 10.1109/ICGCCEE.2014.6921415.

H. Cao, S. Liu, R. Zhao, H. Gu, J. Bao and L. Zhu, "A Privacy Preserving Model for Energy Internet Base on Differential Privacy," 2017 IEEE International Conference on Energy Internet (ICEI), Beijing, 2017, pp. 204-209, doi: 10.1109/ICEI.2017.43.

D. Yang, B. Qu and P. Cudré-Mauroux, "Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation," in IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 3, pp. 507-520, 1 March 2019, doi: 10.1109/TKDE.2018.2840974.

S. Sharma and A. S. Rajawat, "A secure privacy preservation model for vertically partitioned distributed data," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-6, doi: 10.1109/ICTBIG.2016.7892653.

H. Cai, F. Ye, Y. Yang, Y. Zhu and J. Li, "Towards Privacy-Preserving Data Trading for Web Browsing History," 2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS), Phoenix, AZ, USA, 2019, pp. 1-10, doi: 10.1145/3326285.3329060.

M. Shateri, F. Messina, P. Piantanida and F. Labeau, "Real-Time Privacy-Preserving Data Release for Smart Meters," in IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5174-5183, Nov. 2020, doi: 10.1109/TSG.2020.3005634.

A. S. Rajawat, U. Dwivedi, D. C. Jain and A. R. Upadhyay, "Integration of data source using query processing for distribute heterogeneous environment," 2011 Nirma University International Conference on Engineering, Ahmedabad, India, 2011, pp. 1-7, doi: 10.1109/NUiConE.2011.6153226.

C. Yeh, P. Wang, Y. Pan, M. Kao and S. Huang, "A Scalable Privacy Preserving System for Open Data," 2016 International Computer Symposium (ICS), Chiayi, 2016, pp. 312-317, doi: 10.1109/ICS.2016.0069.

M. Shateri, F. Messina, P. Piantanida and F. Labeau, "Deep Directed Information-Based Learning for Privacy-Preserving Smart Meter Data Release," 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 2019, pp. 1-7, doi: 10.1109/SmartGridComm.2019.8909813.

S. Sharma and A. S. Rajawat, "A review of privacy preserving models for multiparty data release framework", Proc. ACM Symp. Women Res., pp. 165-168, 2016.

R. B. Messaoud, N. Sghaier, M. A. Moussa and Y. Ghamri-Doudane, "Privacy Preserving Utility-Aware Mechanism for Data Uploading Phase in Participatory Sensing," in IEEE Transactions on Mobile Computing, vol. 18, no. 9, pp. 2160-2173, 1 Sept. 2019, doi: 10.1109/TMC.2018.2869865.

Xiaonan Wang and Zhengping Jin, "A differential privacy multidimensional data release model," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 171-174, doi: 10.1109/CompComm.2016.7924687.

Z. Zhou, H. Zhang, Q. Zhang, Y. Xu and P. Li, "Privacy-preserving granular data retrieval indexes for outsourced cloud data," 2014 IEEE Global Communications Conference, Austin, TX, USA, 2014, pp. 601-606, doi: 10.1109/GLOCOM.2014.7036873.

M. S. Mohd Pozi, A. A. Bakar, R. Ismail, S. Yussof, F. Abdul Rahim and R. Ramli, "Shifting Dataset to Preserve Data Privacy," 2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), Langkawi Island, Malaysia, 2018, pp. 134-139, doi: 10.1109/IC3e.2018.8632641.

Y. Shen and H. Jin, "Privacy-Preserving Personalized Recommendation: An Instance-Based Approach via Differential Privacy," 2014 IEEE International Conference on Data Mining, Shenzhen, China, 2014, pp. 540-549, doi: 10.1109/ICDM.2014.140.

A. Shaikh and S. Patil, "A Survey on Privacy Enhanced Role Based Data Aggregation via Differential Privacy," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, India, 2018, pp. 285-290, doi: 10.1109/ICACCT.2018.8529634.

S. S. Wu, S. Chen, A. Bhattacharjee and Y. He, "Collusion Resistant Multi-Matrix Masking for Privacy-Preserving Data Collection," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 1-7, doi: 10.1109/BigDataSecurity.2017.10.

Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49

J. Wang and W. Lin, "Privacy Preserving Anonymity for Periodical SRS Data Publishing," 2017 IEEE 33rd International Conference on Data Engineering (ICDE), San Diego, CA, 2017, pp. 1344-1355, doi: 10.1109/ICDE.2017.176.

S. K. Thakur, B. Bhagat and S. Bhattacharjee, "Privacy-Preserving Outsourced Mining of D-Eclat Association Rules on Vertically Partitioned Databases," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697353.

Y. O. Basciftci, Y. Wang and P. Ishwar, "On privacy-utility tradeoffs for constrained data release mechanisms," 2016 Information Theory and Applications Workshop (ITA), La Jolla, CA, USA, 2016, pp. 1-6, doi: 10.1109/ITA.2016.7888175.