SECURE MINING AND SHARING OF FINANCIAL DATA:FUZZY LOGIC AND CRYPTOGRAPHY

MEENAKSHI BANSAL
Research Scholar, IK Gujral Punjab Technical University
Jalandhar, Punjab, India
Ermeenu10@gmail.com

DINESH GROVER
Professor, IK Gujral Punjab Technical University
Jalandhar, Punjab, India
dineshgrover@yahoo.com

DHIRAJ SHARMA
Asst. Professor, Punjabi University
Patiala, Punjab, India
Dhiraj.pbiuniv@gmail.com

Abstract Data mining, because of its broad spectrum of applications, is a popular research area. Due to the increasing amount of data in the database, there is a need to transform such data into useful information. Data mining techniques can transform data into knowledge, but mining process could leads to leakage of private information about individuals. Therefore, to address the privacy issues related to mining process, a new technique known as Privacy Preserving Data Mining (PPDM) is gaining acceptance. PPDM refers to the process of examining the data mining algorithms for the security of sensitive information. In the present study data-mining was performed on the financial dataset to make managerial decision making process better and secure. In this study an attempt was made to tackle principle security issues by proposing a secure model using fuzzy logic and cryptography.

Keywords: Cryptography; Financial database; Data mining; Fuzzy Logic; Privacy; Sensitive data.

1. Overview

Database in cyber banking sector, is growing at much faster rate, while banks need to administer and process this gradually growing database in an effective manner. These days banks are adapted to internet to perform many banking services. Internet facilitates customers to perform various banking operations anywhere anytime which lead to banking industry for its growth. But the privacy and security issues remain the major concerns with internet banking. Unauthorized signatories attack on banking data communicated over social network. Thus all-important is to establish a banking architecture that can secure the private data and integrity of transactions along with its usefulness.

Sensitive information taken from mined datasets by crooked users is frequently accepted as “database inference” problem. Registered users of this innovative technology are worried for security of the environment with which they transact. In most cases the bank’s databases is in readable form and also could be accessed by outside users. Therefore data needs to be protected by a stronger apparatus than the normally accepted cryptographic algorithms while making online transactions. The main objective of this research was to study the effectiveness of security of the database and the mechanism applied at client, server and the administrative levels. The areas of cryptography and fuzzy logic have emerged as pillars for the information security [Madanayake et al., (2012)]. In this study, we have used the hybridization of fuzzy logic and cryptography algorithms with secret sharing keys to prevent the leakage of sensitive information while data mining.

In this model financial database has been mined using one of the technique of data mining i.e frequent pattern growth (FP) and fuzzified for extracting sensitive information. Fuzzified sensitive rules were encrypted using strong cryptographic algorithm that gave access with legitimate key. The use of wrong key otherwise provide the encoded data for the assurance of private information.

2. Review of Related Studies

[Aburrous et al. (2009)] proposed an intelligent model for detecting e-baking phishing website using the combination of fuzzy logic and datamining. They have classified possible phishing website attacks and assessed

model's performance against those attacks. Traditional datamining techniques alone are not sufficient to deal with these problems. So new models were developed which aggregate data mining techniques with fuzzy logics [Ansari et al., (2007)].

[Bhanumathi and Sakthivel, (2013)] used binary integer programming model for multiparty collaborative data mining for addressing problems associated with discloser of sensitive data of an individual among other parties. The use of privacy preserving along with cryptography model using Elgamal encryption has ensured greater privacy of data without losing its accuracy in the distributed environment [Dung et al., (2010)].

[Ganesan et al., (2010)] hybridized hashing, symmetric and asymmetric algorithms and proved that the combination of HECC and AES is better than ECC and RSA. Privacy preservation on quantative data has been obtained using fuzzy rule hiding and fuzzy correlation analysis [Gupta et al., (2009)] [Hameed et al., (2012)].

[Helie et al.,(2005)] proposed the advanced security architecture for IPSec with the combination of quantum cryptography and quantum key distribution. [Wang and Yi, (2012)] assumed of replacing highest priority value of fuzzy item with zero to hide the sensitive rules. [Khelifi et al., (2013)] discussed that most of the banking architectures are using data encryption techniques to provide better security to their customers for performing online transactions.

[Kulkarni et al., (2012)] in their model merged the concept of fuzzy logic with cryptography to generate more strong ciphers. In earlier model the concept of substitution cipher was used which fails when number of repeated cipher were sent. It becomes easier for the attacker to guess the key. But by combining it with fuzzy logic this problem has been solved. [Mohapatra et al., (2013)] have proved in their study that the use of Fuzzy Logic along with Secret Sharing Concept provides the better approach for security and data integrity.

In the existing studies various loop holes has been analyzed in the security architecture used in financial organizations. Presently used models apply only cryptographic techniques, which lack in security due to the sharing of keys along the insecure communication channel. But in this research it is being proposed to make online financial transaction more reliable by designing new security model. First banking data is converted into the logical form using fuzzy concept and then that data is encrypted by applying asymmetric cryptographic technique. This model ensures the confidentiality of the financial data during online transactions. In the online financial transaction even if the data is hacked by the adversary it is of no use to them.

3. Problem Definition

Despite the use of security approaches studied in literature, several security accompanying challenges still exist. Now the problem definition is:

The design and implementation strategy of Privacy Preserving Data Mining (PPDM) model incorporating the concept of fuzzy logic along with cryptography during sensitive data sharing. Our main objective is to hide the sensitive information by applying association rule hiding, fuzzy sensitive rule hiding, fuzzy correlation analysis and cryptography. This model has 2 sub systems client and server which are implemented individually. These meta architecture are then combined to handle secure transactions of cyber systems.

4. Research Methodology

Along with strengthen of security of cyber systems this model minimizing the retrieval time of various queries of the database. Flow of the proposed approach is described in Figure 1. as follows:

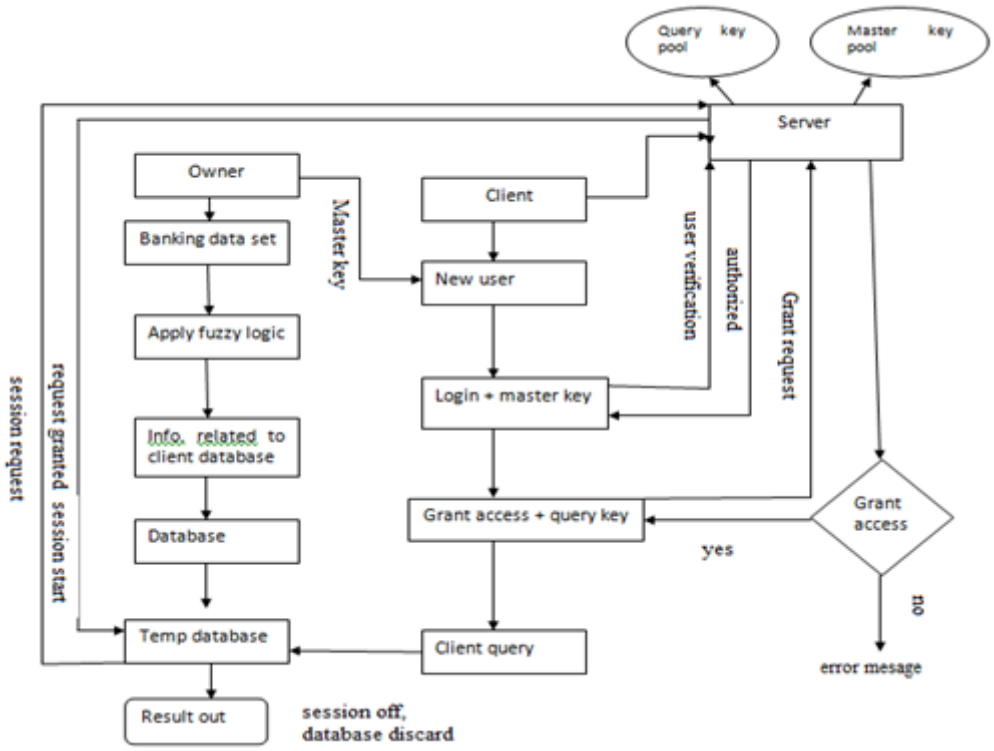

Fig. 1. Flow of Proposed Approach

4.1 Server Side Flow

On server side we can separate our flow in two modules.

(1) Module that will mine the data.
(2) Module to handle client request.

4.1.1. Module that will mine data:

(1) Owner will provide a data set on which data mining techniques will be applied to extract information or knowledge.
(2) First mine data using FP growth technique.
(3) Mine fuzzy item sets.
(4) Encrypt all the mined data and store that encrypted data in a database. This database will be queried for the user query.

Once we have database of the knowledge, we can accept user queries for the information. Therefore extracting data from the dataset is the first step in our project on the server end. Mining Module is described in Fig 2.

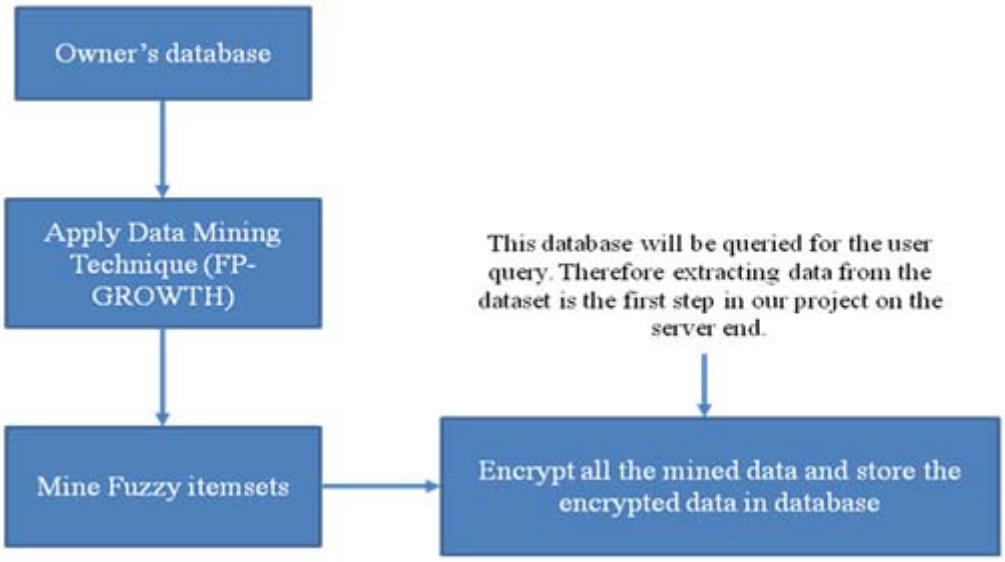

Fig. 2. Mining Module

4.1.2. Module to handle client request

This module is as described in Fig 3.

(1) For this we need to have a database with client information, database will contain information of the client on the basis of type of grant to the client i.e. whether (owner, admin, user). Whenever a new user will be added to the database a master key will be generated for the user.

(2) Whenever a client will login his details will be compared from the database and if details are right user will be given access on the basis of his/her grant. How user may query database depends on his/her type of grant.

(3) Further on the server we have a pool of keys, where each key is associated with a type of query. For example %^$6734RTY#$ this is a key which we have associated with select type queries. Now to execute select type query first user have to provide this key. If user will give right key he may execute the query else he will get an error message. We may associate different keys to a different type of queries. Concept of key will enforce the security and it will protect our database from unauthorised access. Keys will be distributed on the basis of type of grant so a user will be given only those keys that will allow him to read data from database, admin will be given only those keys that will allow him to read and update data from the database. Now it is clear that user can not make any change in the database as he/she doesn't has the relevant key.

(4) Now to enhance the security further, owner may update the query keys after a particular time period. The problem is how the clients will get the updated keys. Here client's master key can be used, if client try to query database and he/she is getting error that will indicate that owner has updated the keys, now client may request the server for updated keys, server will ask for client's master key and once client will provide valid master key, server will send updated keys to the client on the basis of client grant.

(5) This is a simple scenario of client-server interaction, but we need to enforce security here, to enforce security we will use encryption and hashing techniques.

(6) All the interaction between client and server will be in encrypted mode. That means client information and client queries both will be in encrypted form. When server will get client info, it will be in the form of encrypted hash. This information will be decrypted first, after decryption we will get hash, this hash will be compared with the information stored in the user details data base, if we will find a match in the database that means user is authenticated and his/her session will start.

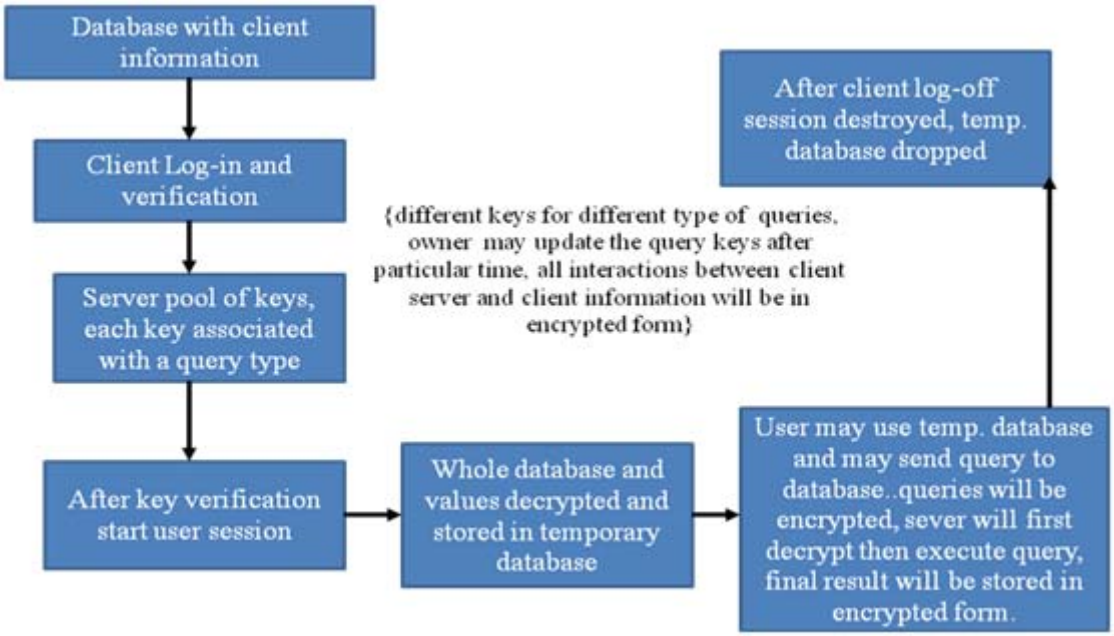

Fig. 3. Module to Handle Client Request

(7) Now we have already mentioned above that database will be in encrypted form, when a user session will start the whole database will be decrypted and values will be stored in a temporary database. Now user may query this temporary database, and only user for which this database is created may be able to use this database.

(8) Now user may send query to the server, queries will also be in encrypted form, to increase the security we will use two type of encryption on the query, so first query is encrypted using a symmetric encryption like AES and then we can further encrypt the encrypted query using an asymmetric encryption like elliptic curve. On server end first query will be decrypted using asymmetric encryption and then it will be decrypted using symmetric encryption. After decrypting the query we will first match the keys if the keys are matched then query will be executed.

(9) Results will again be encrypted using symmetric then asymmetric technique on the server, and will be sent to the client.

(10) When client will log off, his session will be destroyed and temp database will be dropped.

4.2 Client Side Flow

On client side a login interface will be provided that will allow client to login, after successful login client will enter his query key that is assigned to him based upon his role to access the attributes. Query key of the client will be mapped to the query key pool maintained in the database and corresponding rules will be displayed to the clients. When client will logout, or close the window server will be notified.

5. Conclusions

As now days of internet banking in banking sector, the main challenge is to protect the data from untrustworthy parties. So the credit card numbers, Debit card numbers and other banking information of individuals should not be disclosed to third party. We have proposed a secure client and server end mechanism for online banking transactions. The Research project being undertaken uses the various concepts such as association rule mining, fuzzy logic, association rule hiding, cryptography and secret sharing keys. The approaches proposed in literature proved that combination of fuzzy logic and data mining gives better results for privacy preserving data mining. We are applying concepts of cryptography and secret sharing keys for additional security. So our main goal is to develop a good and secured architecture for online banking transactions and we will achieve it through many approaches of privacy preserving data mining.

References

[1] Aburrous MR, Hossain A, Dahal K, Thabatah F. Modelling intelligent phishing detection system for e-banking using fuzzy data mining. In: CyberWorlds, 2009. CW'09. International Conference on 2009 Sep 7 (pp. 265-272). IEEE.

[2] Ansari AQ, Patki T, Patki AB, Kumar V. Integrating Fuzzy Logic and Data Mining: Impact on Cyber Security. In: Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on 2007 Aug 24 (Vol. 4, pp. 498-502). IEEE.

[3] Bhanumathi S, Sakthivel P. A new model for privacy preserving multiparty collaborative data mining. In: Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on 2013 Mar 20 (pp. 845-850). IEEE.

[4] Dung LT, Bao HT, Binh NT, Hoang TH. Privacy Preserving Classification in Two-*Dimension Distributed Data. In: Knowledge and Systems Engineering (KSE), 2010 Second International Conference on 2010 Oct 7 (pp. 96-103). IEEE.

[5] Ganesan R, Gobi M, Vivekanandan K. A Novel Digital Envelope Approach for a Secure E-Commerce Channel. International Journal of Network Security. 2010 Nov 1;11(3):121-7.

[6] Ghernaouti-Hélie S, Sfaxi MA. Guaranteerring Security of Financial Transaction by Using Quantum Cryptography in Banking Environment. In: International Conference on E-Business and Telecommunication Networks 2005 Oct 3 (pp. 139-149). Springer Berlin Heidelberg.

[7] Gupta M, Joshi RC. Privacy Preserving Fuzzy Association Rules Hiding in Quantitative Data. International Journal of Computer Theory and Engineering. 2009 Oct 1; 1(4):382.

[8] Hameed S, Shahzad F, and Asghar S. A Fuzzy Correlation Scheme for Privacy Preservation in Knowledge-Based Systems. Australian Journal of Basic and Applied Sciences. 2012, 6(9), pp. 562-571.

[9] Khelifi A, Aburrous M, Talib MA, Shastry PV. Enhancing Protection Techniques of E-Banking Security Services Using Open Source Cryptographic Algorithms. InSoftware Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS International Conference on 2013 Jul 1 (pp. 89-95). IEEE.

[10] Kulkarni SS, Rai HM, Singla S. Design of an Effective Substitution Cipher Algorithm for Information Security using Fuzzy Logic. International Journal of Innovations in Engineering and Technology, 1(2), 2012, pp. 50-57.

[11] Madanayake PR, Peiris MD, Ranaweera GH, Jayathilake KU, Senarathne A, Abeygunawardhana PK., "Advanced Encryption Algorithm Using Fuzzy Logic", International Conference on Information and Computer Networks, Vol. 27, 2012, pp. 32-36.

[12] Mohapatra AA, Saho M, and Mishra AK, "Message Security and Integrity Maintenance Using Fuzzy Logic and Secret Sharing", International Journal of Scientific & Engineering Research, 4(5), 2013, pp. 1055-1058.

[13] Wang H, Yi C. Privacy-preservation association rules mining based on fuzzy correlation. In: Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on 2012 May 29 (pp. 757-760). IEEE.