JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

Website: http://www.jmrr.org **Vol.4, Iss.2 Pages:1-11**

PRIVACY PRESERVATION OF ONLINE TRANSACTION DATA USING THREE-TIER ARCHITECTURE

S MAHESWARI[1], K SHAHEEN[2]

[1,2] PG and Research Department of Computer Science

Holy Cross College (Autonomous), Tiruchirappalli, Tamilnadu, India

Article Received: August 2022 Published: September 2023

Abstract

The use of credit cards has increased dramatically due to rapid advances in electronic commerce technology. Credit cards are used to purchase goods and services with the help of virtual cards and physical cards while virtual cards are used for online transactions and physical cards are used for offline transaction. As credit cards have become the most popular means of payment for both online and regular purchases, it offers cashless purchases. This online shopping will be the most convenient way to make bill payments. In online payment systems, attackers will only need a very small amount of information to make fraudulent transactions (secure codes, card numbers, expiration dates, etc.). In this purchasing system, the most important is the transaction will be done through internet or telephone. To commit fraud in this type of purchase, the fraudster only needs to know the card details. Most of the time, the original cardholder is not aware that someone else has seen or stolen his card information. Therefore, the risks of fraudulent transactions using credit cards are also increasing. In the existing credit card fraud detection system, the fraud transaction will be detected after the transaction is done. Fraud is difficult to detect and issuance authorities will withhold about a loss. So in this paper it has implemented three tier server system to split the intermediate gateway with better security. Transaction details are segmented and stored as sensitive attributes across primary and secondary servers. And also implement a data suppression scheme to convert string and numeric characters into special symbols to overcome traditional cryptography schemes.

Keywords: Fraud detection Techniques, vertical partition approach, data suppression, authorized access, wireless network security

1. INTRODUCTION

Big Data Analytics is the process of analysing data sets to find hidden patterns, unknown contacts, market trends, customer preferences or other useful business information. The most effective marketing of analytical findings, new revenue opportunities, excellent customer service, better operational efficiency, a competitive advantage over rival organizations, and other business advantages.

The primary goal of Big Data Analytics is to help data scientists, predictive modellers, and other analytics professionals analysed large amounts of transactional data, plus other forms of data help companies make more informed business decisions, which may go unused by traditional business Intelligence (BI) program. It includes web server logs and web click stream data, social media content and social networking activity reports, text and poll answers from customer emails, and details of mobile phone call logs, and machine data captured by sensors connected to the Internet-of-Things. Semi-structured and unstructured data do not fit exactly in traditional databases based on relevant databases. In addition, data warehouses may not be able to handle the processing demands generated by large sets of data that need to be updated frequently or continuously.

2. FRAUD DETECTION TECHNIQUES

Credit card fraud is on the rise day by day due to the increasing use of credit cards. Instead of using various fraud detection techniques, fraudsters are so expert that they find new ways to conduct fraudulent transactions.

Table 1 Credit Card Fraud

METHODS	PERCENTAGE
Stolen/Lost Credit Card	48%
Site Cloning	15%
Skimming	14%
Credit Card Generator	12%
Phishing/ Internal Fraud	6%
Others	5%

2.1 Site Cloning

In site cloning, the fraudster clones the entire site or only the payment page of the site where the customer makes the payment. The customer feels that they are viewing the original site. The customer hands over the credit card details to the fraudster and then the fraudster sends the transaction receipt to the customer via email as the genuine site. Thus the fraudsters have all the details of the customer credit card so that they can commit the fraud without the knowledge of the customer.

2.2. Stolen / Lost Credit Card

When the customer's card is lost or stolen by the fraudster get all the information of the cardholders in a very easy way without investing any sophisticated technology. Credit card frauds is difficult to detect.

2.3. Skimming

Skimming is one of the popular forms of credit card frauds. It is a process where the actual data on one card is electronically copied to another. It is very difficult for the cardholder to detect this type of fraud.

2.4. Create Card Generator

In Credit Card Generator the computer program generates valid credit card number and expiry gate. This generator generates a valid credit card which is highly reliable in that it only shows up as a valid credit card number and is also available for free download from the internet.

2.5. Phishing

In phishing, the fraudster sends a lot of false emails to the card holder. The e-mails look like they came from a website where the customer trusts for example the customer's bank. The email asks the customer to provide personal information such as credit card number. With the help of these details fraudsters commit crimes.

2.6. Internal Fraud

Employees or owners access the details of customers. They steal customer personal information to commit a crime or pass on cardholder information to fraudsters for money. Large-scale data-mining techniques could improve to the state of the art in business practice. Scalable technology for analyzing the largest amount of transaction data generated powerful computations for fraud detectors in a timely manner is a significant problem, especially for e-commerce.

3. EXISTING SYSTEM

A credit network model enables trust between agents in a distributed environment, and arbitrary pairs to make payments between agents. With their flexible design and robustness against intrusion, Credit networks form the basis of many cibil-tolerant social networks, anti-spam

communication protocols and payment methods. Existing systems, however, expose the trust links of agents as well as the existence and volume of payment transactions, which are perceived as sensitive information in the social environment or financial world. This raises a challenging privacy concern, which has so far been largely overlooked by research on credit networks.

Privacy protection standards were recently developed because the most important information is now often stored on computers connected to the Internet. Also many tasks that were once done by hand are done by computers; Hence the need for Information Assurance (IA) and security. Maintaining confidentiality is a key to protecting against identity theft. Businesses also need security because they need to protect their trade secrets and confidentiality information.

Cyber-terrorism is one of the major terrorist threats facing our country today. As mentioned earlier, this threat is magnified by the large amount of information that is now available electronically and on the web. Homomorphic encryption is a form of encryption that allows a specific type of encryption to perform computations and obtains an encrypted result that matches the result of the process performed in encrypted plain text. For example, one person can add two encrypted numbers and then another person can encrypt the results so that they cannot find the values of the individual numbers.

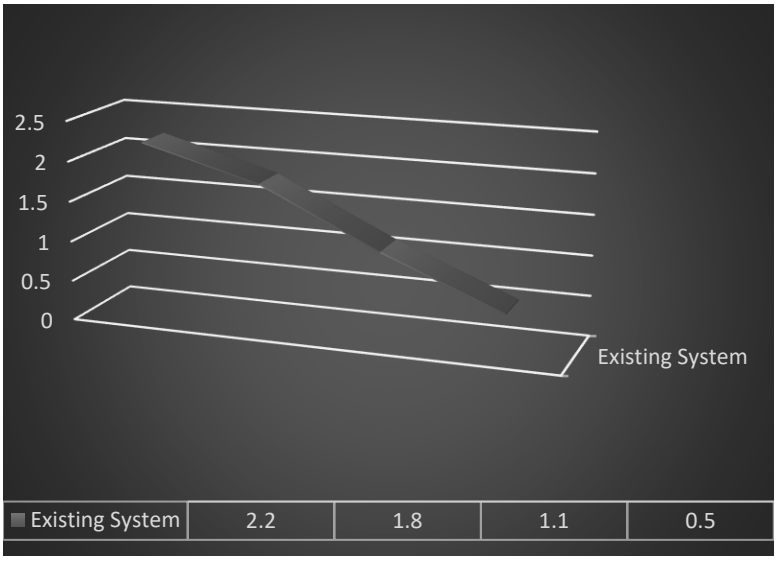

Fig 1 Existing System Graph Model

Table 2 Horizontal partition

Acc.No	Method	Amt	Date
@#$%&	Card_Credit Card	25000	14-03-21

Example for, Horizontal Partitioning table

The existing data management system presents several notable disadvantages. Its low security measures allow unauthorized individuals to easily access sensitive information, undermining data protection. Moreover, the practice of maintaining all details on a single server proves risky, as it creates a potential single point of failure and restricts data accessibility and redundancy. Due to the necessity of encrypting data to enhance security, a substantial amount of storage space becomes imperative, leading to considerable infrastructure costs. The system's vulnerability to hacking remains a pressing issue, casting doubt on the overall security and confidentiality of the stored data. These drawbacks collectively emphasize the urgent need for a more robust and secure data management solution.

4. PROPOSED SYSTEM

With the advent of communication technologies, e-commerce as well as online payment transactions are increasing day by day. Simultaneously, the financial fraud associated with these transactions is also increasing, resulting in loss of billions of dollars every year globally. Also various benefits like cash back, reward points, interest free credit, discounts offered on purchases made at select stores, and further motivate customers to use credit cards instead of cash for their purchases. The biggest problem for the e-commerce business today is the emergence of fraudulent transactions more and more like legitimate transactions and simple pattern matching techniques are not capable of detecting fraud. We can apply vertical clustering algorithm to cluster the dataset in more than one level. The subset (that is, the column) of the attributes make up the numerator. Rows of pieces that match each other should be connected by a double identifier. A vertical piece corresponds to the projection functions in the table. Data from the pieces can be reassembled to result in the original data set. For vertical fragmentation the join operator is used to join the columns in pieces on the tuple identifier; in horizontal fragmentations the union operator is used on rows coming from fragments. And also implement the K-anonymous algorithm which is a property of some unknown data.

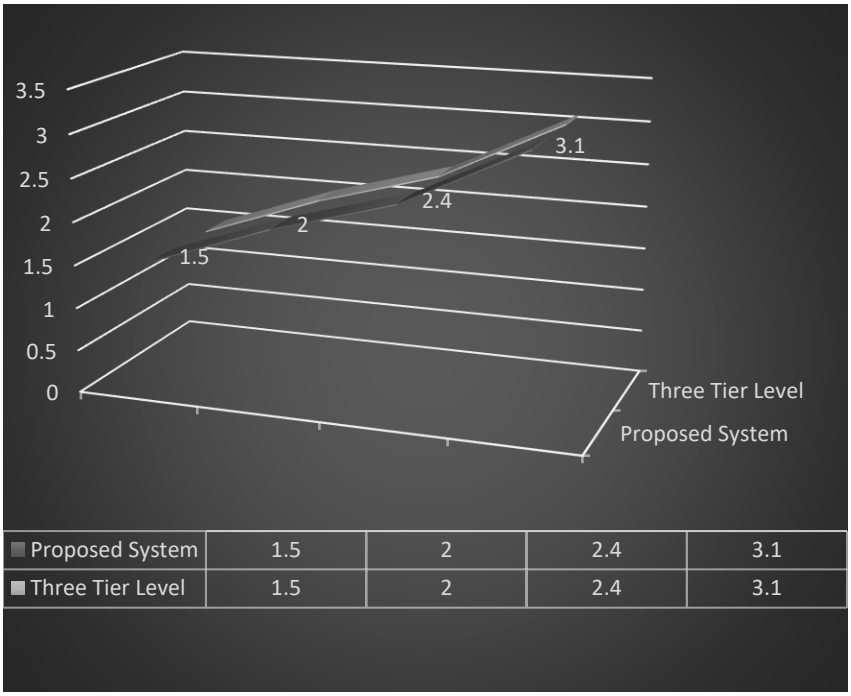

Fig 2 Proposed System with Three tier Level

Given individual-specific field-structured data, the scientist releases the data with the guarantee that the individuals who are the subjects of the data cannot be re-identified, while the data remains practically useful.

The output of the data's is said to be a k-anonymous property if the information of each person in the publication cannot be distinguished from at least k-1 persons. Various processes and programs are patented to generate anonymized data providing K-anonymous protection.

Table 3 Vertical partition

Acc.No	**Method**	**Amt**	**Date**
&%$#@*	Card_Credit Card	25000	14-03-21
Example for, Vertical Partitioning table			

The advantages of the proposed data management system are compelling. It significantly enhances security by making it exceedingly difficult for hackers to breach the server and access sensitive data, ensuring the confidentiality and integrity of the information. It reduces both time and computational complexity, streamlining processes and making data retrieval and

management more efficient. The system minimizes the need for manual manipulation, thereby decreasing the workload for administrators and improving overall efficiency. It proves resilient against a variety of cyber threats, including guessing attacks, man-in-the-middle attacks, and counter-attacks, making it a robust choice for safeguarding critical data. These advantages underscore the potential of this system to provide a secure and efficient data management solution.

5. ONLINE TRANSACTION DATA AND MODEL

5.1 Bank Interface Creation

Bank interface is an electronic information and payment system that enables one to communicate with the bank in automated and operative manners. The banking interface allows the company's accounting systems to integrate with banking services. Online Banking System is a web application that ensures a registered user to enjoy online banking. This online banking system is a web application where you can transfer money to other users and keep a close watch on all your transactions. Plus we've added additional security features to our online banking system. This module is used to create web based applications specially for banking sector. This application will be used by Bank Admin and User only. By using this application user can do online transaction.

5.2. Description Of Transaction

This module is used to collect all transaction data. A transaction statement is an electronic payment system that enables customers of a bank or other financial institution to conduct a variety of financial transactions through a financial institution's website. Online banking systems are usually integrated as part of a major banking system operated by the bank and, unlike a branch bank, are the traditional way for customers to access banking services. Any transaction like money deposit, withdrawal, money transfer is available using this web application. The amount gets automatically updated in the savings account. All transaction details are updated in a single gateway. Gateway is responsible for transferring the amount to the particular merchant without any leakage.

5.3. Vertical Partition Approach

Partitioning can provides tremendous benefit to a wide variety of applications by improving performances, management and availability. It is not uncommon for partitions to significantly improve the performance of certain queries and maintenance tasks. In addition, partitions facilitate public administration tasks. In addition, partitions can simplify general administration tasks. Partitioning enables database designers and administrators to solve some of the most difficult problems posed by state-of-the-art applications.

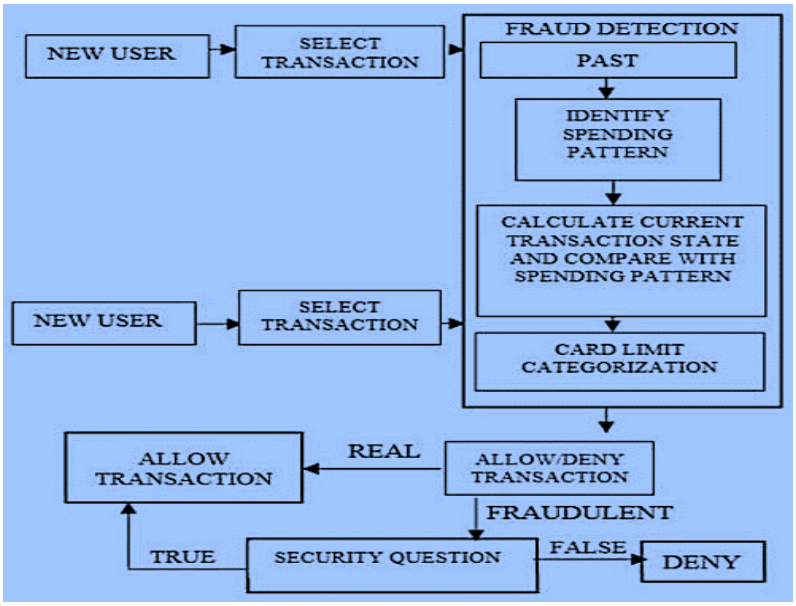

Fig 3 Transaction data

Partitioning is an important tool for creating a multi-terabyte system or systems. Partitioning the database improve performance and simplifies maintenance. Dividing a large table into smaller, separate tables can run faster because there is less data to scan queries that only access a portion of the data. Vertical partitioning divides a table into multiple tables that have fewer columns. This module can spread the features across different servers such as personal details, account details and transaction details.

5.4. Data Suppression

This module implements K-Anonymity to protect data privacy. K-anonymous is a property that contains anonymous data. There are two common ways to obtain k-oblivion for some value of k.

- Suppression: In this method, some values of the attributes are replaced with the asterisk '*'. All or some of the values in a column can be replaced with '*'.
- Generalization: In this method, the individual values of the attributes are changed to wide limits. It is one of the most recognizable scenarios, k-anonymous which makes continuous data sets hyper-anonymous, this hyper-anonymous is more pronounced with small sample fractions. Too much anonymity causes too much distortion in the data (i.e., too much information loss), making the data less usable for subsequent analysis.
- A hypothetical experimental approach provided better control over the risk of re-identification and minimal data loss compared to a basic k-anonymity. Obviously, this can guarantee k-anonymity by replacing each cell with *, but it renders the database useless. The cost of a k-anonymous solution for a database is the number of starts of *.

- A minimal cost k-anonymity solution suppresses the minimum number of cells required to guarantee k-anonymity.

5.5. Authorized Access

This module design creates authorized access for bank customers. Users can login to view transfer details with OTP security. OTP can be sent as SMS alter and can appear with special seconds. Users can view their details in a secure manner. A password that is only valid for login sessions and transaction on one of the computer system and other digital devices. OTP avoids many of the drawbacks associated with traditional (standard) Password-based authentication. The most important advantage of OTPs is that, unlike standard passwords, they are not subject to repeated attacks. An OTP that has already been used to sing in or make a transaction into a service can no longer be misused by an intruder because it is no longer valid. The second major advantage is that if a user uses the same(or identical) password for more than one computer and the password of one of them is compromised, they will not be compromised at all.

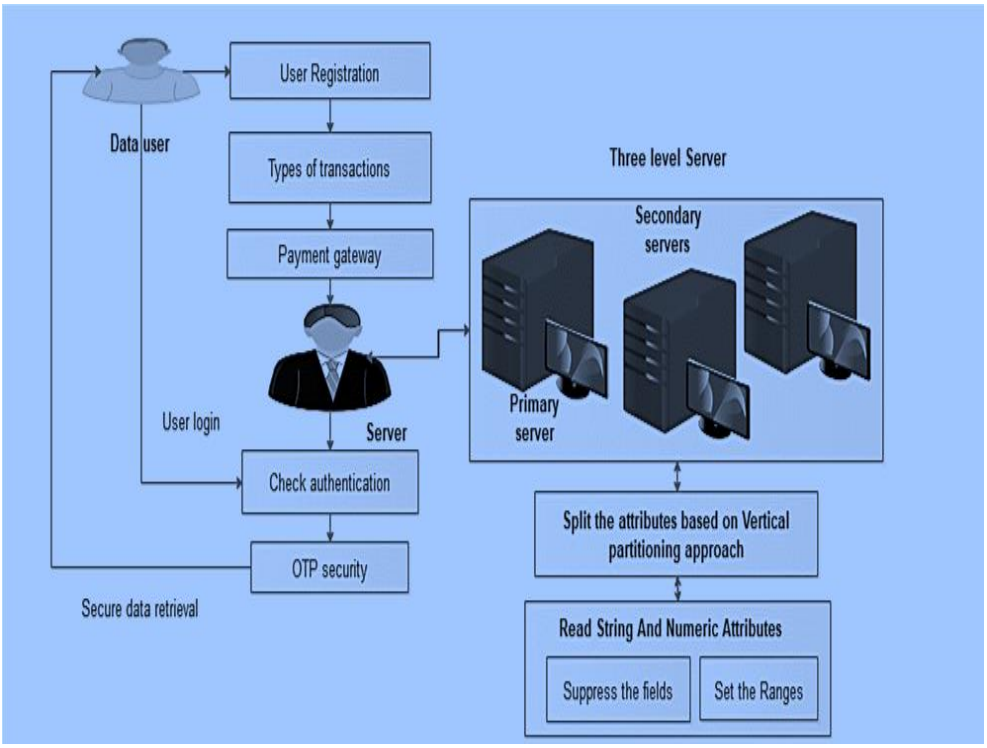

Fig 4 Three Tier Architecture Models

CONCLUSION

Personally identifiable information is protected. Generally, if directly or indirectly connected with a person, it is considered to be a sign of individual patterns. Therefore, the values of attributes associated with individuals that are subject to the mining of personal data must be kept private and protected from disclosure. Miners are then able to learn from the global model, rather than the characteristics of a particular individual. The article concludes that the proposed system provides better protection on cloud data. It can implement vertical division approach and k-anonymous approach. K-Anonymity is a privacy protection method to limit the disclosure of personal information in data mining. The process of anonymizing a database table usually involves the normalization of table entries and, consequently, the loss of relevant information. This simultaneously minimizes the loss of information and stimulates the search for anonymous algorithms that reach the required level of anonymity. The problem of k-anonymization is NP-hard with minimal loss of information. Different types of data conversion techniques such as randomization and K-anonymous based techniques have been studied and analysed based on their functions.

FUTURE ENHANCEMENT

In future work, this can extend framework to implement various algorithms to enhance the security with dynamic splitting. Many K-anonymities areimplemented for anonymous data with enhanced security.

REFERENCES

1. Wang, H., He, D., & Tang, S. (2016). Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. IEEE Transactions on Information Forensics and Security, 11(6), 1165–1176.
2. Liang, K., Huang, X., Guo, F., & Liu, J. K. (2016). Privacy-preserving and regular language search over encrypted cloud data. IEEE Transactions on Information Forensics and Security, 11(10), 2365–2376.
3. Wang, D., & Wang, P. (2018). Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Transactions on Dependable and Secure Computing,15, 1545-5971.
4. Gentry, C. (2009). Fully homomorphic encryption using ideal lattice. Proceedings of the ACM Symposium on Theory of Computing (STOC 2009), 169–178.

5. Gentry, C., Sahai, A., & Waters, B. (2013). Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically faster, attribute-based. Proceedings of the International Cryptology Conference (CRYPTO 2013), 75–92.
6. Yang, M., Zhu, T., Liang, K., Zhou, W., & Deng, R. H. (2019). A blockchain-based location privacy-preserving crowd sensing system. Future Generation Computer Systems, 94, 408-418.
7. Ning, J., Huang, X., Susilo, W., Liang, K., Liu, X., & Zhang, Y. (2022). Dual access control for cloud-based data storage and sharing. IEEE Transactions on Dependable and Secure Computing, 19(2), 1036-1048.
8. Singh, R., & Sharma, T. (2019). Security in Wireless Local Area Networks (WLANs). In J. Sen (Ed.), Computer and Network Security. Intechopen. DOI:10.5772/intechopen.89857.

Cite this article:

S Maheswari, K Shaheen, "Privacy Preservation of Online Transaction Data Using Three-Tier Architecture", Journal of Multidimensional Research and Review (JMRR), Vol.4, Iss.2, pp.1-11, 2023