Secured Smart Card System using PostGreSQL Database

N.V. Jaswanth Raj#1, R. Anitha*2

[1]*Scholar, Master of Computer Applications, S.A. Engineering College, Chennai*
jaswanthraj3007@gmail.com
[2]*Assistant Professor, M.C.A. Department, S.A. Engineering College, Chennai*

Abstract — This paper is concentrated on smart card security in increased transmission rate of information. The retrieval of data from the database for the application of smart cards is normally made up with embedded system technologies and various methods which is convenient for their own purpose. Technologies like Passive Infrared Receiver (PIR) sensors, Denial of Service (DoS) attacks, Radio Frequency Identification (RFID) modules and machine to machine communications are used for developing a secured end to end communication. Smart cards are used for single person identification and so this system should be much secured. The process of it is completed with various algorithms for making it a working model in real time. PostGreSQL database is used for storing the data and which also reduces cost. PostGreSQL databases are reliable and used in many forums for their various characteristics like unlimited storages, solving security issues, and fast data transmissions.

Keywords — *PostGreSQL; PIR Sensor; DoS Attacks, RFID Modules; Smart Cards.*

1. Introduction

This paper is mainly based on providing the reliable Relational Database Management System which is used for transferring data in the smart cards, that consists of our personal details. This smart card technology can be done using embedded system. Whereas in real time, embedded systems are most popularly used for the automation system with secured data storage and transformation of those confidential data between one another. Smart cards consist of storage space which is used for storing and retrieving of data, so we need a Database to manage those data which should be reliable and secure[1][2]. Various encryption algorithms were used like PIR sensors, DoS attacks controls and RFID modules are used as the additional security for smart cards. So device may able to handle or protect from the entry of any intruders or unauthorized accesses. Device like smart cards will provide all in one information about a particular person includes aadhar card details, Banking details and all necessary details which represents their identity[3]. So reliability of the database systems is very essential. PostGreSQL is an open source Database, so the cost may also be reduced. It is also useful in the online transaction which has a healthy transformation of data from one end to other end.

2. Existing System

Developing highly secured software has more challenges while it has to be implemented in real time. As for most of the secured devices, preferably used embedded system but the complexity of developing a quality embedded system is costly. As hardware and software is used, the hardware used will be of high range for maintaining its quality of work. We also need a database to store all the details about a particular person and the transactions made by them. The database must be highly secured, that is data should be protected by using various strong encryption algorithms. The existing system uses SQLAccessGroup (SAG) database. Although it works well, they have some issues with their performance. So, to overcome those backdrops, we introduce PostGreSQL database to be replaced with the SQLAccessGroup (SAG) database [3][5].

2.1 Disadvantages of Existing System

- SQLAccessGroup databases are slower compared to PostGreSQL database.
- Less concurrency in data retrieval.
- Storage space of the data is less.
- Cannot use high level encryption algorithms.

3. Proposed System

PostGreSQL are known for its high reliability and secured transaction of data over the network. As smart card consists of personal details about a person, the security of data is more important. PostGreSQL is an up growing database in recent times, as they are replacing many of the older databases because of its user friendly nature and reliable characteristics. Unlike many proprietary databases, it is extremely common for companies to report the details by using simple queries in the database. It is also used to analyse the historical data and as it will be very useful for the companies for developing their business by knowing their statistical analysis of data. It has unlimited storage space, so the cost of managing the database will also be reduced and moreover it is an open source database.

Concurrency of accessing the data will be more when compared with other databases [2][3].

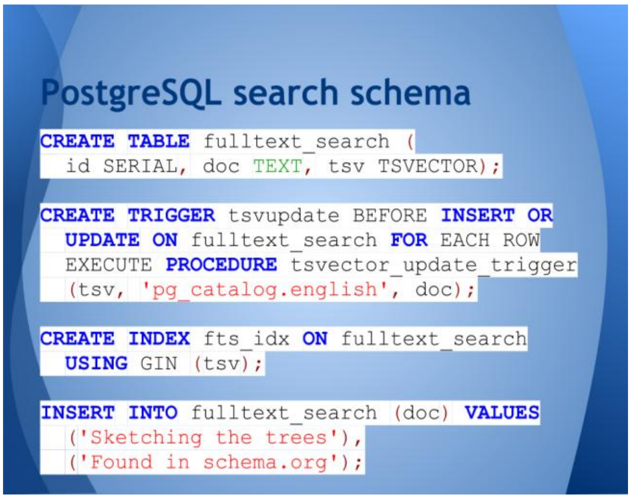
3.1 Advantages

- It uses multiple row data storage strategy called Multi-Version Concurrency Control (MVCC)
- It also has unlimited data storage capacity.
- It also ensures the Atomicity, Consistency, Isolation, and Durability (ACID) compliance.
- Cost of buying is less when compared with other preparatory databases.

4. Methodology

While replacing the SQLAccessGroup (SAG) database with PostGreSQL Version 9.6.2 database, PostGreSQL gives number of server-side pagination techniques that differ in speed, integrity and support. There are three kinds of functions in PostGreSQL as fundamental constraints. The fast path interface available in PostGreSQL offers a powerful, convenient and reliable functionality over the data in the store.

- Maximum database size is unlimited.
- Maximum table size is 32 Terabyte (TB).
- Maximum row size is 1.6 TB.
- Maximum field size is 1 Gigabyte (GB).
- Maximum rows per table is unlimited.
- Maximum columns per table is 250 - 1600 depending on column types.
- Maximum indexes per table is unlimited.



PostgreSQL search schema

```
CREATE TABLE fulltext_search (
  id SERIAL, doc TEXT, tsv TSVECTOR);

CREATE TRIGGER tsvupdate BEFORE INSERT OR
  UPDATE ON fulltext_search FOR EACH ROW
  EXECUTE PROCEDURE tsvector_update_trigger
  (tsv, 'pg_catalog.english', doc);

CREATE INDEX fts_idx ON fulltext_search
  USING GIN (tsv);

INSERT INTO fulltext_search (doc) VALUES
  ('Sketching the trees'),
  ('Found in schema.org');
```

Fig. 1: Queries for implantation

The process of the smart card will be quite easy while viewing in the front end but the mechanisms used in the backend will be more complicated, that is it has to maintain the security, control network traffic, collisions, mismatching of data and etc. As seen in figure 2.

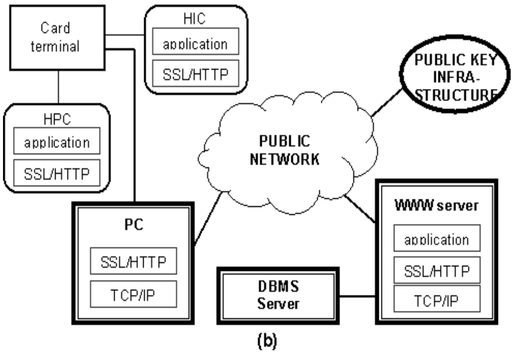


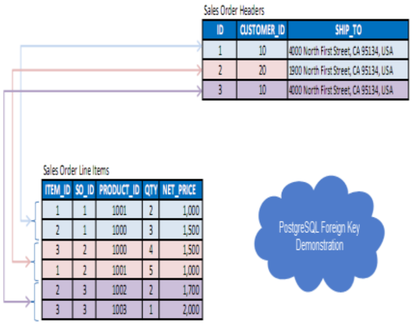
Fig. 2: System Architecture

5. Working Model

First, we have to insert the smart card in the card reader terminal, within a second it will recognize our overall details by matching the details in the database by using Secure Socket Layer (SSL) or Hyper Text Transfer Protocol (HTTP) network and it takes the Internet protocol (IP) address from the public server and processes it to display in the monitor. With the help of the chip presented inside the silver coated part in the smart cards, it does all these operations. It will display the username or ID and ask for the authentication like passwords or pins. Those passwords will also be checked with the database for the specific user. If the data provided is correct, it will proceed for the further steps or it will be terminated when the password is wrong. Once the password we entered is correct, then it asks for what type of transactions we needed. Then it will be done and the system will be terminated or the connection will be closed once the process is completed.[4]

6. Implementation:

After adding data in the database, the primary key and the foreign key will be set and the tables will be linked according to the keys. Then the data are filtered under some relationship based on the priorities. There are certain relational models for PostGreSQL that are used in the tables for developing the overall relational schema of the application system (figure 3). That would be useful for moving on to the further steps of the designing process [4].



Sales Order Headers

ID	CUSTOMER_ID	SHIP_TO
1	10	4000 North First Street, CA 95134, USA
2	20	1900 North First Street, CA 95134, USA
3	10	4000 North First Street, CA 95134, USA

Sales Order Line Items

ITEM_ID	SO_ID	PRODUCT_ID	QTY	NET_PRICE
1	1	1001	2	1,000
2	1	1000	3	1,500
3	2	1000	4	1,500
1	2	1001	5	1,000
2	3	1002	2	1,700
3	3	1003	1	2,000

Fig. 3: Database table connectivity

Encryption is made using various algorithms for making data secured in the database. The data will be retrieved with the Primary Key (figure 4).

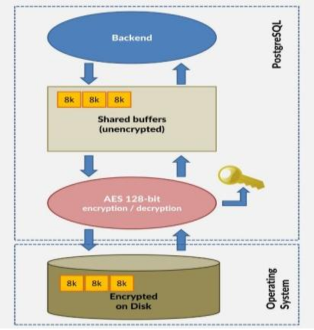

Backend
8k
8k
8k
Shared buffers (unencrypted)
AES 128-bit encryption / decryption
PostgreSQL
8k
8k
8k
Encrypted on Disk
Operating System

Fig. 4: Connecting operating system with PostGreSQL

When the user enter the ID of their personal smart card, it asks for some kind of authentications like passwords, pin numbers, patterns and various Biometrics, etc. to make sure that the data card is used by a valid user [5].

Because of using the PostGreSQL database, the data retrieval will be faster than other databases. Whereas the matching data speed of rows and columns in a database will be around 3000 to 4000 data per second. When the data are found, the user details will be displayed on the screen and then the user can go for further processes of what they need to do. After the process is completed, the session time of that particular ID of smart card will be terminated. Then it will wait for another user to access the application or system.

6.1 Real Time Applications of Smart Cards

There are many real time examples available for smart cards which are useful in every fields, it has been an essential thing in our day to day life and which is easy to carry and use.

- *Payphones:* The first card technology was used in 1983 in payphones in France. The advanced features are like phone banking and on-line services.
- *Banking and Retail:* Smart banking cards can be used as credit and for direct debit cards. The microchip placed on the card and the card readers are using mutual authentication process.
- *Electronic Purse:* Card readers retrieve the amount currently stored and subtract the amount for the goods or services are being purchased.
- *Health Care:* Smartcards allows the information for a patient's history to be stored safely.

7. Result

The data will be retrieved faster as compared to other databases for storing the data. As the performance of the smart card increases and the usage of smart cards will also be increased around the people. Large data can be managed easily without investing large amount. As the reliability of system is more, then the security level will also be more than that of other systems. We can also reduce the corruption and bribery in the country by making all the transactions over smart cards. So, we can have every single track of transactions made by every individuals.

8. Conclusion

In the current generation, the use of technologies by people has been increased. A new device or an automated system is being invented day by day. The smart cards are used in this fashion, as an automation tool for many automation devices. It can be improved by introducing some new encryption algorithms to keep the data even more secured than before. As PostGreSQL database contains large storage space, more details can be added for the anti-theft of the smart cards from unauthorized persons. It will also be useful in reducing the corruption issues by making the transaction of money over smart cards, it leads to safe banking and it is most important to store data in a reliable database. We can also track and easily retrieve the data.

9. Future Enhancement

To reduce the unauthorized access of the smart cards, various effective biometrics techniques can be used. We can also store more details and at the time of loss of card that can be retrieve easily. we can use Challenge Response System (CHS) method to make sure that one who currently using the card is a valid user. CHS is that asking different questions to the user about their personal details and checking whether the data provided are matching and then confirming that they are the valid user and they can proceed for further steps. To implement these technologies, it needs more time and cost, but it will be more effective for solving the security issues. PostGreSQL databases are also in developing stage, it can also be improved with some other extra features in future.

References

[1] Embedded Surveillance System Using PIR Sensor. Padmashree S. Dhake1Sumedha S. Borde2,Volume No.02, Issue No. 03, March 2014 .

[2] Smart Security System Using Embedded System Technology. K.S.Tamilselvan. T.Balakumaran, Volume 1, Issue 6, December 2012.

[3] Security needs in embedded systems. Anoop MS, Tata Elxsi Ltd. India.

[4] Embedded Controller Based Smart Card Access. Vivek Kumar Sehgal, Nitin ,Durg Singh Chauhan, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[5] Usage of Embedded Systems for DoS Attack Protection. I. Dodig, D. Cafuta, V. Sruk., Politechnic of Zagreb HR-10000 ZAGREB, I. Lucica 5, CROATIA, Faculty of Electrical Engineering and Computing HR-10000 ZAGREB, Unska 3, CROATIA.