Online Transaction Processing using Enhanced Sensitive Data Transfer Security Model

Sona Kaushik, Shalini Puri

***Abstract*-- As with any information processing system, authentication and reliability are considerations, online transaction system are generally more susceptible to direct attack and abuse than their offline counterparts. With the increasing popularity of the internet, the e-commerce market has grown rapidly in recent years. The Secure Electronic Transaction System to process securely electronic transaction is currently the main e-commerce application and due to increasing malicious activities, it requires fiddly approaches to be introduced. In this work, an algorithm is introduced which works to secure the critical information shared during the online transaction processing (OLTP).**

***Index Terms*-- OnLine Transaction Processing Security, Sensitive data transfer security, Barcode security.**

I. Introduction

ONLY retailing around the globe has grown at its fastest rate since recent years. In United States, the amount of money spent by consumers shopping online increased by 33.4% in year 2006 which has almost tripled over the last five years. Most of the customers prefer online shopping rather than in-store shopping. In addition, it is more convenient to do online transactions for money transfers or utility bill payments. These online transactions [1] – [8] require the sharing of critical and sensitive information like credit card number and card verification value.

During on - line transaction, sensitive information is exchanged and encrypted between the visiting website and Web Browser with the use of secure connection. Certificates are used to provide encryption through a document the website provides. When we send information to the website, it is first encrypted at our computer and then decrypted at the website. Under normal circumstances, the information cannot be read or tampered with while it is being sent, but it's possible that someone might find a way to crack the encryption.

Additionally, the secure connection between the computer and the website does not mean that the visiting website is reliable. In other words, it raises a big question mark about the web site authenticity and reliability. So, it does not ensure us that the *website is trustworthy* and privacy can be compromised by the way, the website uses or distributes critical information.

Therefore, such challenges and problems make us to re-think on the method used to protect the critical and delicate information during the on – line transactions. Our work aims to put such effort forward in this direction, which can protect the information being transferred in any way against the attacks and untrustworthiness.

Section II discusses the background related to the research work done on the existing and current systems. In section III, the proposed work is discussed in detail that how the OLTP can be made secured and safe. Finally, section IV concludes this research work.

II. Related Insights

With the technical encouragement and increased usage of transaction systems, the demand of assets and robust security of critical and sensitive data are significantly required to ensure about the related concerns. A lot of investigation work has been done on such systems to provide the high security to such type of data.

In recent decades, the research work on the security of On – Line Transactions has been a hot area to provide safe and protective environment around the globe. In this field and in the related application sectors, lots of researchers are doing significant work. Lot of studies put their efforts and provide the baseline for the online transactions, vendors [1], and management systems for E. Commerce.

To build Internet trading platform [4], human resource training and development, online stock broker and online trading system are developed. Some rating agencies [5] are also working for peer-to peer online transactions securely.

SET is the demanding transaction system, which provides a ways for secure transactions. Such systems are widely used in the different organizations and projects. In recent areas, many studies [6] and research work has been done on SET. In addition to this, the features of online shopping are frequently used and therefore, it requires online shopping related security measures [7] and transactions. Some models show that digitally sign transactions can be performed in an un-trusted environment using multi-agents [8] securely. It shows an agent-based scenario for e-Payment.

III. Proposed Framework

Work related to sensitive data transfer secure (SDTS) algorithms have been proposed by the author(s) in the study of

Sona Kaushik is currently pursuing M. Tech. degree program in computer science from Birla Institute of Technology, Mesra, India. E-mail: sonakaushik22@gmail.com

Shalini Puri is currently pursuing M. Tech. degree program in computer science from Birla Institute of Technology, Mesra, India. E-mail: eng.shalinipuri30@gmail.com

978-1-4673-0455-9/12/$31.00 ©2012 IEEE

barcodes, security and applications of the same [10]. The revised model of SDTS is proposed underneath providing the benefits of the following. Firstly, this makes the system more complex at byte level and thus, difficult to predict by the hackers. Secondly, provides tightly coupled security because of increased complexity of the system.

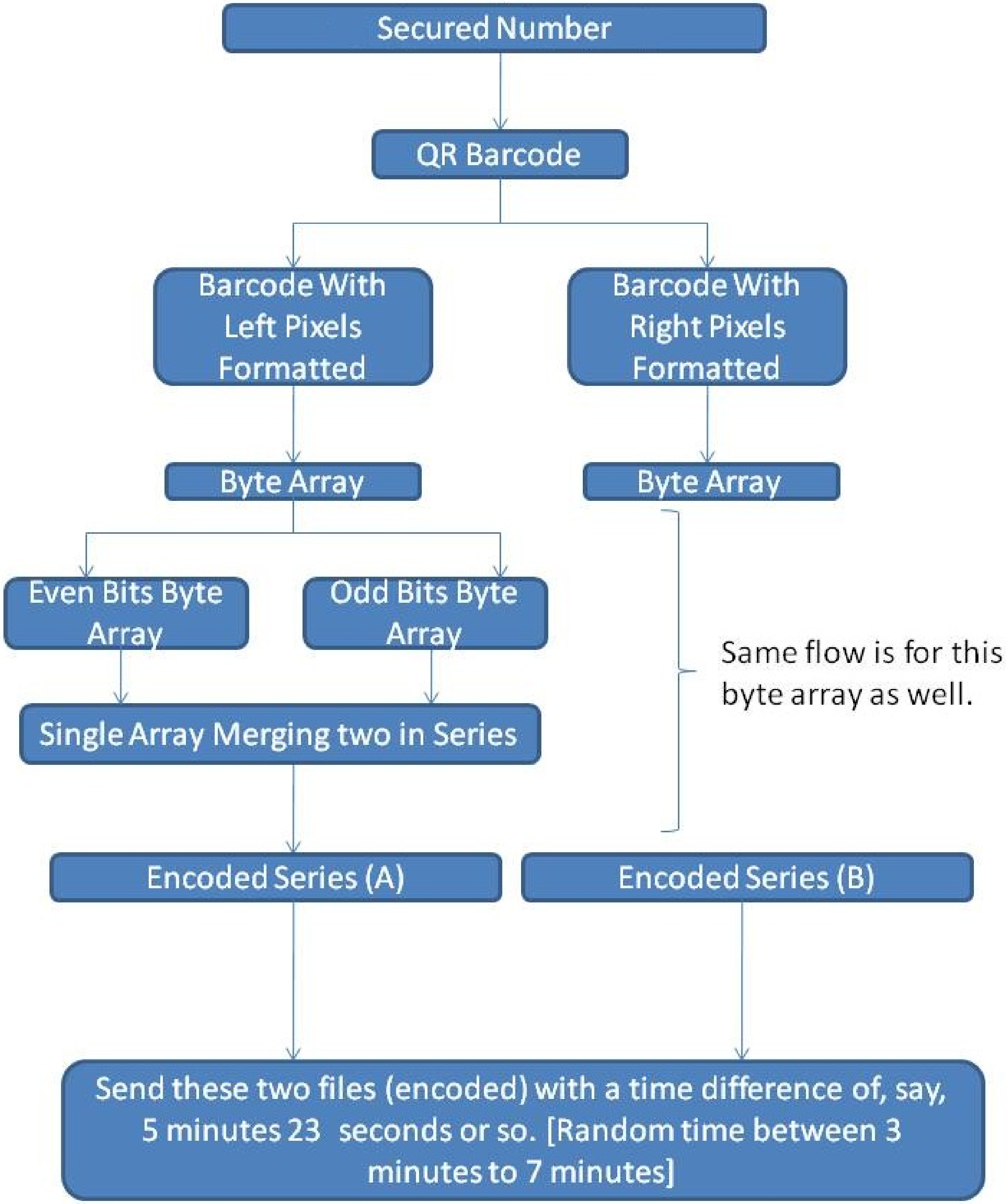
Secured Number
QR Barcode
Barcode With Left Pixels Formatted
Barcode With Right Pixels Formatted
Byte Array
Byte Array
Even Bits Byte Array
Odd Bits Byte Array
Single Array Merging two in Series
Same flow is for this byte array as well.
Encoded Series (A)
Encoded Series (B)
Send these two files (encoded) with a time difference of, say, 5 minutes 23 seconds or so. [Random time between 3 minutes to 7 minutes]

Fig. 1. Flow of Enhanced SDTS.

As is in the case of previous versions of SDTS model, it is converting the secure information into barcodes first, do some pixel manupulations and then convert the barcode image into byte arrays. Finally, it encrypts the bytes using standard RSA (Rivest, Shamir, and Adleman) algorithm.

The detail view of the enhanced model is shown in figure 1 is the revised model [9]. In reference to the online transaction processing applications [10], the information to be processed is not taken to be flowed over the network, but a corresponding security key is picked from database table to secure the real information from being exposed on the network.

Then *secure/secret key* before exposing to the network is processed under various layers changing the face of the information. A quick response barcode is created for the key and splitten into two identical barcode like images, using terminology explained in previous versions [9-10], called *False Images*. Each false image is converted to a byte array.

Unlike the previous SDTS versions, each byte array is further splitten to two; picking all the odds together and all evens together. Then these odds and evens are combined in sequence. The idea is to scramble the array in a predefined manner such that it gets tougher to identify the information within the arrays.

The transformed array is then encrypted using the RSA algorithm. The key management for the same is out of scope in this work. The two encrypted secure files are sent over the network with some random time difference of 3 to 7 minutes.

IV. Implementation

The top view of the enhanced structure is shown in figure 2. There are seven layers in the model and each has its own role and dependency. The secure secret key layer fetches the secret key from the database. The mapped key from the database is called *Secure Secret Key* which is fed as an input for Quick Response Barcode layer. In this layer, the secret key is converted to QR barcode using QR Barcode convertor. For the purpose ZXing library [11] can be used. This library is available open source. The following code snippet can be referred.

```
QRBarcode qr = new QRBarcode();
qr.encode(secureKey);
```

The identical looking false barcodes are created by manipulating the pixels of the image [11]. These barcodes seems to be the original barcodes, though are not the authentic barcode. These barcodes are then transformed to byte arrays. Unlike the previously proposed SDTS model, the bytes are played around in these byte arrays and each is slitten into two forming Even and Odd byte arrays. Then these arrays are joined together in the specified format discussed in earlier section and encrypted to form secure files. Then these secure files are sent over network for which a random time is set using following code snippet:

```
3 + (Math.random() *( (7 – 3)+1))
```

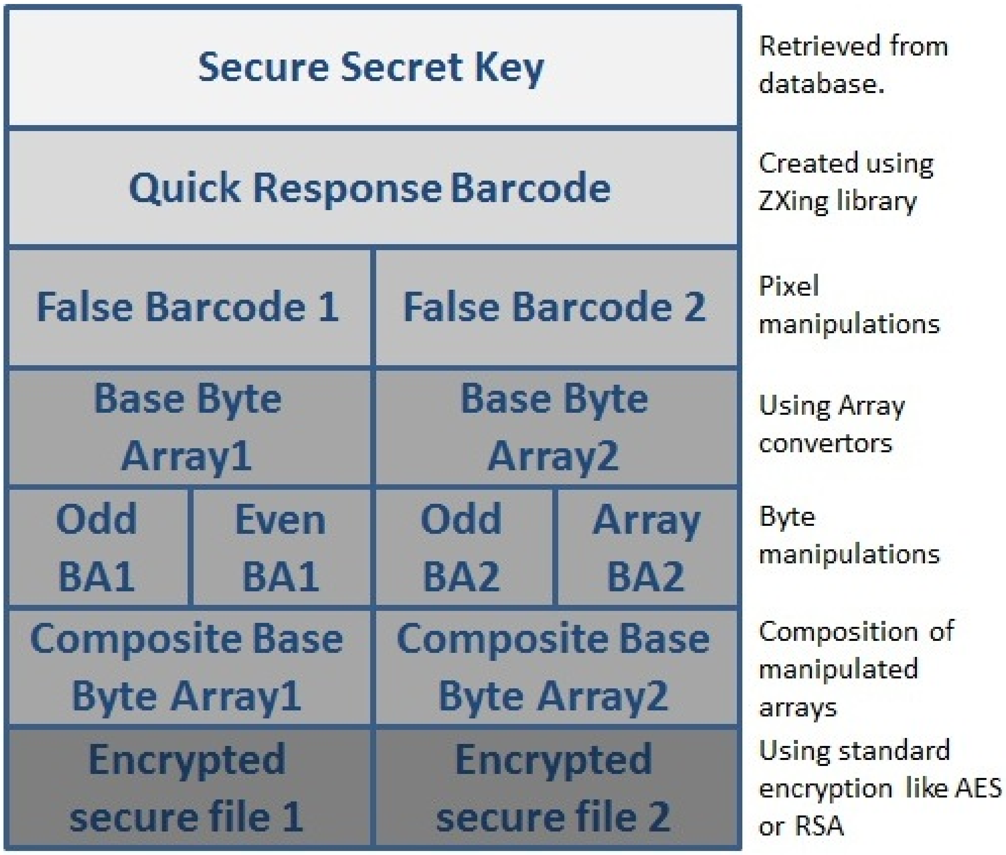

Fig. 2. Top View of Enhanced SDTS.

The implementation involves the number of APIs (Application Programming Interfaces) projected. Refer the detail view of the enhanced SDTS model [figure 3].

A request object from the application is created name here as ***request a***. *Request a* will do the connection set up using a connection listener. At the SDTS layer, a ***socket queue*** will listen the request and queues it. The request is read by the ***socket reader*** which is further handled by the ***Thread Request handlers***. The *thread request handler* will create anther request object named as ***request b*** to communicate with database, that is, a database connection is setup. Using connection listener, request b hits the ***Request Parser*** which identifies the *secure key* from database.

Database returns a response object, ***response b*** to the *request parser*. *Request parser* then returns this response object to the *thread request handlers*.

Further the secure key extracted from database is sent to the generator ***API for quick response barcodes***. This API creates a QR barcode for the secure key and passes them to *splitter API*. Using the *Logic APIs* pool, the splitter API creates false images of barcodes. Each of the false image is introduced to the ***Byte Array Formulator***. It uses the API from Logic pool and splits each byte array to their odds and evens byte arrays and recombines them in sequence. In this work, the recombination logic is static but can be further enhanced to dynamic logic pulling structure.

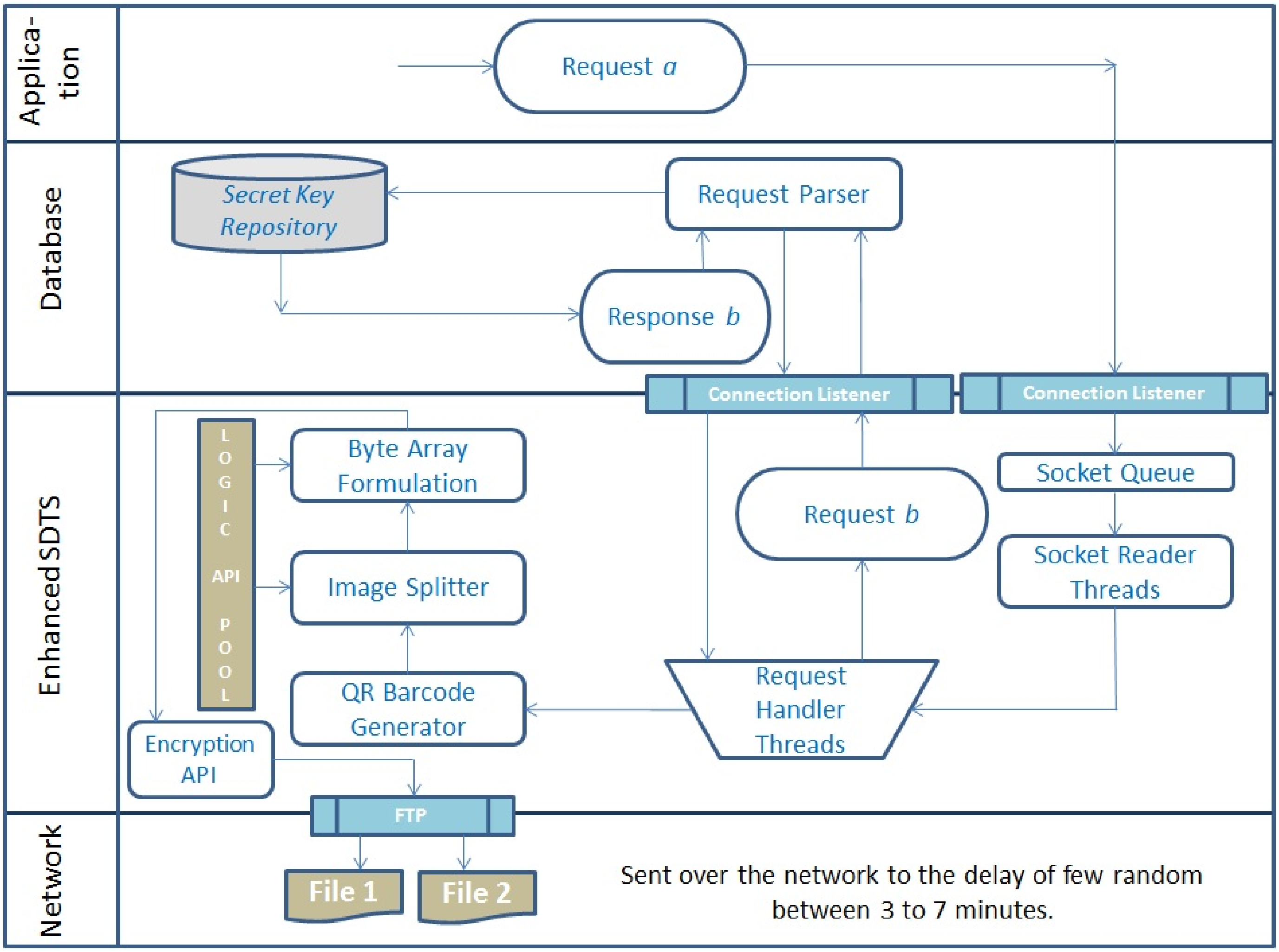

Fig. 3. Detail Structure of Enhanced SDTS.

Recombination logic states that for each array named as ***Base array1*** and ***Base array2***, two arrays are further assigned; one is named as ***Odd byte array1*** and another as ***Even byte array1***. All the odd bits are picked from the base array1and dumbed in Odd byte array1. Similarly, all even bits are picked from the base array and dumped in even byte array1. Further these Odd byte and even byte arrays are kept sequentially and base array content is replaced by this.

Thus, the final products from the array formulator; the two arrays are encrypted using RSA standard algorithm. The two encrypted files are then shared with user by exposing them on the network to the user destination network.

V. Conclusion and Future Activity

The current ongoing transaction system has the overhead for the user to carry the credit credentials along to perform transactions. Also such systems make more number of web service hits to share the sensitive credit credentials which is after SDTS model is even further minimized in the case of proposed enhanced structure.

The proposed work aims to further increase the complexity of the transaction process and make the transaction more tangled for the hackers to intrude. Therefore, concept used in the proposed model is increasing the complexity of transaction which makes it more robust against the attacks preserving the confidentiality and robustness.

ACKNOWLEDGMENT

We would like to acknowledge and thanks to Dr. Vikas Saxena, Dept. of Computer Science, Jay Pee Institute of Information Technology, Noida, Uttar Pradesh, India for his encouragement and guidance.

REFERENCES

[1] Alzomai, M.; Alfayyadh, B.; and Josang, A., “Display Security for Online Transactions: SMS-based Authentication Scheme,” International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, pp. 1 – 7, Dec. 2010.

[2] Na Wei; and Bo Zhang, “Construction of China's Securities Brokerage Business Online Transactions Innovation System,” 2nd International Symposium on Information Engineering and Electronic Commerce (IEEC), IEEE, pp. 1 – 3, July 2010.

[3] Lee Heng Wei; Osman, M.A.; Zakaria, N.; and Tan Bo, “Adoption of E-Commerce Online Shopping in Malaysia,” IEEE 7th International Conference on e--Business Engineering (ICEBE), pp. 140 – 143, Jan. 2011.

[4] Fengying Wang; Caihong Li; Zhenyou Wang; and Zhen Cheng, “Security Scheme Research of Digital Products Online Transactions,” IEEE International Conference on Automation and Logistics (ICAL), pp. 1521 – 1525, Sept. 2008.

[5] Ion, M.; Koshutanski, H.; Hoyer, V.; and Telesca, L., “Rating Agencies Interoperation for Peer-to-Peer Online Transactions,” Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), IEEE, pp. 173 – 178, Sept. 2008.

[6] Hong-Jun Guan, “The Research of SET-Based Electronic Payment System Model,” International Conference on E-Business and Information System Security (EBISS), IEEE, pp. 1 – 4, June 2009.

[7] Jihui Chen; Xiaoyao Xie; and Fengxuan Jing, “The Security of Shopping Online,” International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), IEEE, pp. 4693 – 4696, Sept. 2011.

[8] Kouta, M.M.; Rizka, M.M.A.; and Elmisery, A.M., “Secure e-Payment using Multi-agent Architecture,” 30th Annual International Computer Software and Applications Conference (COMPSAC), IEEE, pp. 315 – 320, Dec. 2006.

[9] Kaushik S., “Strength of Quick Response Barcodes and Design of Secure Data Sharing System” International Journal on Advanced Computing & Science (IJACSA), Dec 2011.

[10] Kaushik S.; Puri S., “Online Transaction Processing using Sensitive Data Transfer Security Model” 4th International Conference on Electronics Computer Technology (ICECT), IEEE, April. 2012.

[11] http://zxing.appspot.com/