Sensitive Data Transfer Security Model While Online Transaction Processing

Sona Kaushik

Student of Masters of Technology
Birla Institute of Technology, Mesra
Ranchi, India
sonakaushik22@gmail.com

Shalini Puri

Student of Masters of Technology
Birla Institute of Technology, Mesra
Ranchi, India
eng.shalinipuri30@gmail.com

***Abstract*—The E - Commerce market has grown rapidly in recent years with the increasing popularity of the Internet. As authentication and reliability play important and demanding roles in various Information Processing Systems, the key area On - Line Transaction Systems are generally considered to be attack prone and become more susceptible to direct attacks and abuse than their offline counterparts. In the current scenario, the Secure Electronic Transaction System (SETS) is used as one of the main E-Commerce applications to process the electronic transaction securely and safely via the Internet. Due to drastically increasing malicious activities, SETS requires fiddly approaches to be introduced. This insecurity of transaction puts a big challenge in terms of transaction protection. This paper aims to work on the aforementioned challenge, therefore, an approach is introduced which works to secure the critical information shared during the On - Line Transaction Processing (OLTP) over on the insecure channel.**

Keywords- Barcode Security, On - Line Transaction Processing Security, Sensitive Data Transfer Security, Secure Electronic Transaction, Information system.

I. INTRODUCTION

National agencies are heavily dependent upon their information and information systems to successfully conduct critical and precarious missions. With an increasing reliability on and growing complexity of information systems as well as a constantly changing risk environment, information security has become a mission-essential function. This task must be conducted in a manner that reduces the threats to the information entrusted to the agency. Information security is a business enabler when applied through proper and effective management of risks to information confidentiality, integrity, and availability.

Agencies may realize the value of integrating security into an established system development life cycle in many ways [1], including:

• Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;

• Awareness of potential engineering challenges caused by mandatory security controls;

• Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques;

• Facilitation of informed executive decision making through comprehensive risk management in a timely manner;

• Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases;

• Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment; and

• Improved systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

In this paper, initially overview on the information security has been highlighted discussing the relevance and role of security in any information system. In third section, background on the existing sensitive data transfer systems has been conversed. Further, in two sections, the proposed model along with its advantages and the proof of concept for the same is presented. The paper is concluded in the end with the references used throughout.

II. OVERVIEW OF INFORMATION SECURITY

Information system security processes and activities provide valuable input into managing information technology systems and their development, enabling critical identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle [1]. The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process as well as the supporting assets, and existing interdependencies and relationships. On identification of critical assets and operations, the organization can and should perform a business impact analysis. The purpose of the analysis is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities.

Executing a risk management-based approach for systems and projects means integrating security early and throughout the agency's established system and life cycles. Incorporation enables security to be planned, attained, built in, and deployed as an integral part of a project or system. It plays a substantial role in measuring and enforcing security requirements throughout the phases of the life cycle.

Risk management helps document security-relevant decisions and provides assurance to management that security was fully considered in all phases. System managers can use this information as a self-check reminder of why decisions were made so that the impact of changes in the environment can be more readily evaluated. Oversight and independent audit groups can use this information in their reviews to verify that system management has done an adequate job and to highlight areas where security may have been overlooked.

III. Background on Existing Systems

With the technological advancement and increased usage of on – line transaction systems, the necessity of protection and security of critical data and transaction process are importantly required to ensure about the related concerns. A lot of research work has been done on such systems to provide the high security to such type of data.

A. Existing Systems

In recent decades, the research work on the security of On – Line Transaction Processing Systems has been a hot area to provide safe and protective environment around the globe. Researchers are much more doing in this field and related application sectors. Many surveys and studies put their efforts and provide the foundation baseline for the online transactions, vendors [2], and management systems for E. Commerce. Some schemes combine the digital watermarking and fingerprinting with digital signatures to embed a relatively less amount of information in a digital product to reduce phenomena of descending quality, mutual interference, and improve efficiency [3] whereas some systems use SMS-based authentication scheme [4] for more robust system against the threat of compromised platforms. To build Internet trading platform [5], human resource training and development, online stock broker and online trading system are developed. Some rating agencies [6] are also working for peer-to peer online transactions securely.

One of the demanding and used transaction system is SET, which provides a way to do the transactions securely. Such system and its versions are widely used in the different enterprises and areas. In recent areas, many studies [7] 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 [8] and transactions. [9] Some models show that digitally sign transactions can be performed in an un-trusted environment using multi-agents securely. It shows an agent-based scenario for e-Payment.

B. Online Transaction Processing – Generic Entity Interaction

Most of the transaction systems available in the market use more or less the similar concept for transaction communication. The financial agency expects the customer to set the secure keyword for authentication. This is generally the one time or on request set up. For transaction, the entities interact in peers.

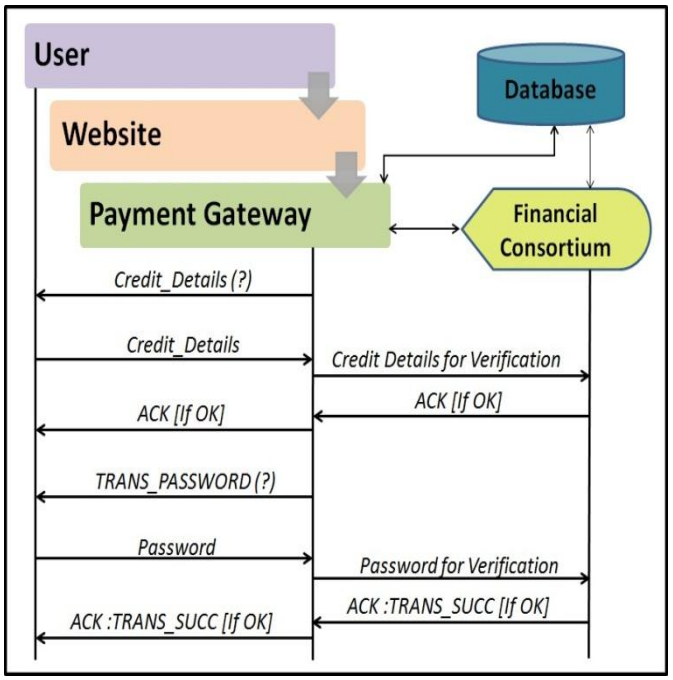

Fig. 1. Entity Interaction of Current Payment Systems.

The entity interaction is shown in figure 1. There exist three entities interacting during the transaction; User, Payment gateway and financial consortium or bank. User while trying to perform the payment is asked to enter the credit details like credit card number, expiration date, and/or card verification value (CVV) number. When user provides all the relevant information required, a web service is called to share the details with the financial consortium by the payment system. The financial consortium verifies the user comparing the details with database and acknowledges in accordance with the verification from database. Thus, if acknowledgement is positive from the consortium, the secure transaction password is expected to be provided by the user. User when enters the password, again a web service is called which shares the transaction sensitive credentials with the consortium. On verification from the consortium, the gateway system acknowledges the user for transaction completion.

IV. The Proposed Model

Maintaining the two important aspects of security; integrity and confidentiality, the proposed system flow is shown in figure 2. The user requests for the transaction on the website. On hit of the request over the server, a web service (file transfer) connection is setup which binds the interaction between web server and payment gateway. A web service flow the information of the user's sensitive file between web server and payment server.

A. Entity Interaction of Proposed System

In the proposed idea, the user is delivered a secure encrypted file as the transaction credential by the financial consortium. Unlike entity interaction diagram for current payment system, in the proposed system user is provided with the *encrypted secure file* which is provided by the bank or

financial agency whose credit details user is using. The payment gateway system ask the user for the *secure_file*, which user has either saved in his system or can download from his/her mailing servers on the fly. The user uploads the secure file and payment servers process it further.

The payment gateway manager asks to upload the secure file for transaction. The user uploads the file on the website. Payment manager now sets up a web service which sends the *secure_file* to the financial consortium or bank for verification.

On successful verification from the consortium, the transaction gets completed and payment gateways acknowledge the user for the same.

B. SDTS for Online Transaction

The concept of Sensitive Data Transfer System (SDTS) model [10], as shown in figure 3, is used here to provide the transaction security. The internet user is provided with the *secure_file* by the financial consortium. The secure file is created using SDTS model figure 3.

To resolve the problem statement identified in the previous section, the event flow of the current payment system is reassembled using the SDTS model.

The idea is that the credit card credentials are placed in the database table with its corresponding primary key as a random unique number called Secure Key.

This key is converted to quick response barcode and then its two identical false barcodes are created by formatting its pixels referring the standard SDTS model [10]. These false barcodes are then converted to byte arrays and then encrypted.

C. Decoder - SDTS for Online Transaction

The *secure file* shared by the user is sent to the concerned financial consortium for authentication. At the consortium, the secure file shared by the user is analyzed by using the decryption module of proposed model shown in figure 4. If authentication gets successful, then transaction is acknowledged as successful.

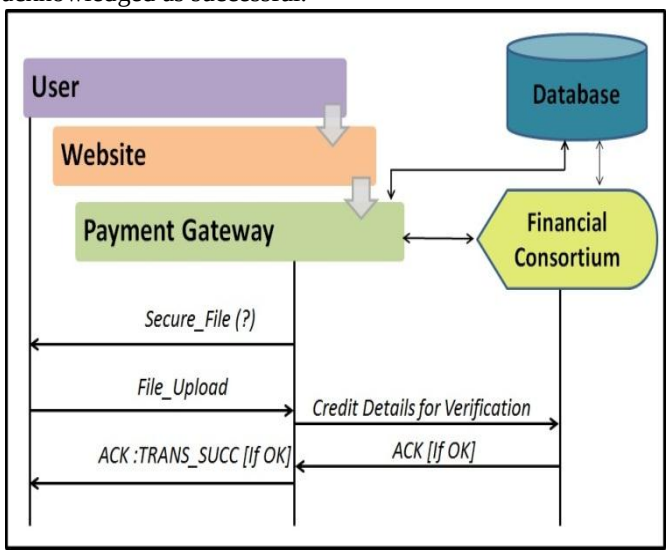

Fig. 2. Entity Interaction of Proposed Payment Systems.

The identical false image first is shared with user by financial consortium as one time activity. Another false image is kept in the database to rejoin it with the one with user at the time of transaction for verification.

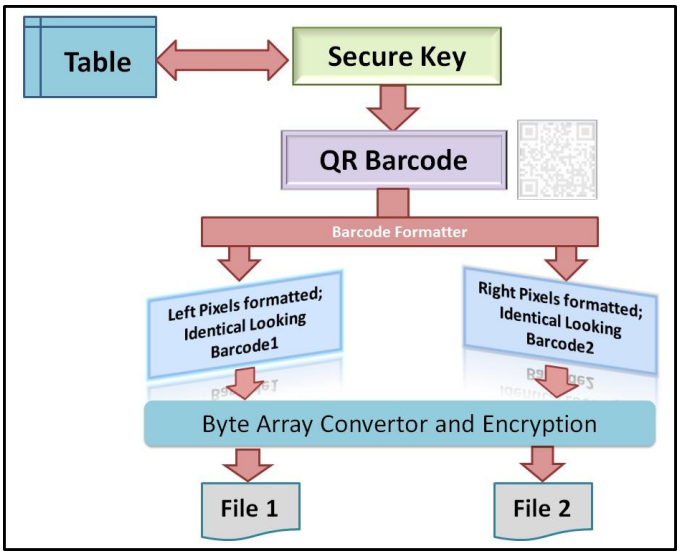

Fig. 3. Sensitive Data Transfer Security – Online Transfer Protocol System.

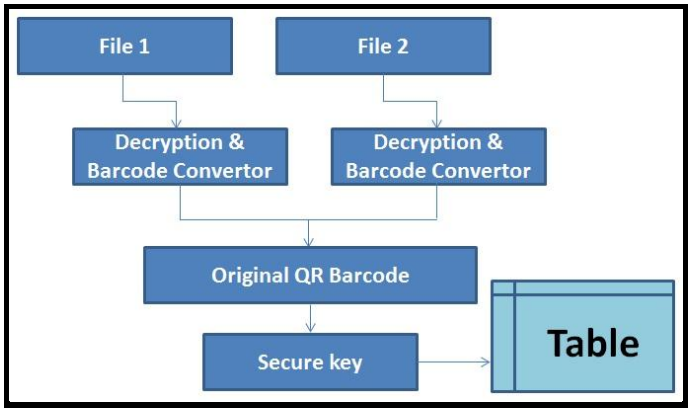

Fig. 4. Decoder of Sensitive Data Transfer Security – Online Transfer Protocol System.

The *secure_file* is when shared with financial consortium for verification and the file at database are first converted to barcodes mapped using a hidden key within the files and then barcode images are merged. This merged image is then read by barcode and retrieved product is the secure key. Corresponding to the secure key, authorities can get the credit details from the database and then perform the transaction.

In case of failure in any peer of the system, the transaction will be a fail.

D. Advantages of SDTS for Online Transaction

The ongoing system flow described in previous sections has certain unseen overheads. They require the user to remember the credit details or carry the credit or debit cards for transaction. With the proposed approach, the user has the convenience of just downloading the file from its favorite and attach at the time of transaction. This, thus, prevents the user's credentials from being played by the hackers.

Also the number of web service requests made is two for each transaction in case of ongoing systems. There is a possibility of improving the performance at this edge of the system. And thus, the web service calls here is reduced to just one.

V. PROOF OF PROPOSED CONCEPT

The methodology used to generate the false barcodes is defined in figure 5. From the original image, various pixels are picked from the original appropriately. While decrypting from the false images, the two false images are overlapped and regained.

The results generated by the system are shown below in figure 6. First image (a) is the original image to be secured by SDTS methodology. Next two consecutive images (b) and (c) are false images of the original image generated by the system, left false image and right false image, respectively. The last image (d) is the reconstructed barcode which contains the exactly same information as in (a) figure. The size of revealed image (d) is exactly same as that of original image (a).

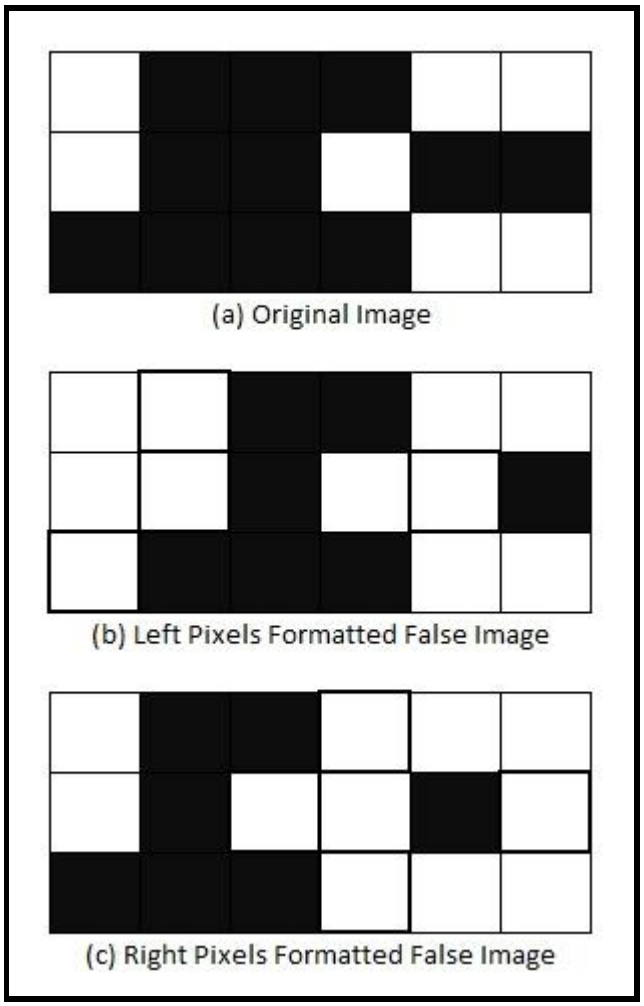

Fig. 5. False Image Formations

Following are the snapshots of the results of Sensitive Data Security model. The form shown in figure 6 (a) allows the user to enter the random secure key of 1024 length which in real application will be fetched directly from the database table. Also, user can provide a system generated random secure key using the *Generator button* provided. On click of the Create False Image button, the resultant is shown in figure 6 (b) and figure 6 (c).

To unmask the false images, separate client is provided. On providing the two false images as shown in figure 7 and on click of the *Unmask button*, unmasking gets successful and original image will be as shown, which is same as original barcode image. On reading this barcode image file, it returns the same secure key as original. Thus in real application, the original information can be fetched using the secure key encrypted.

Fig. 6. Proof of Concept - Encryption

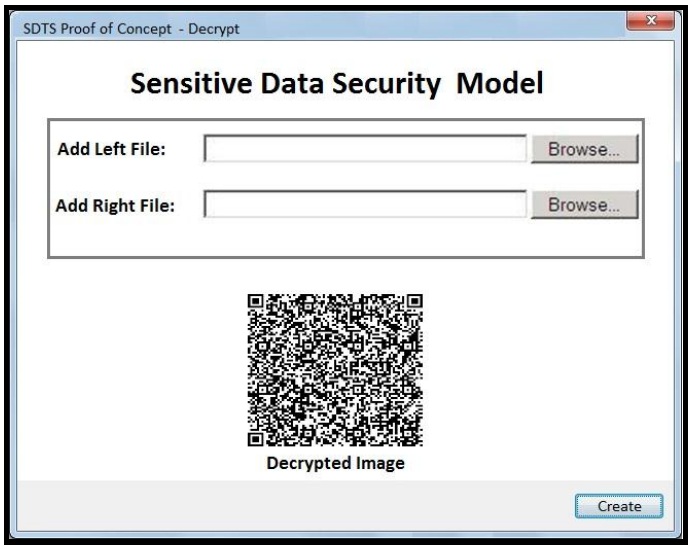

Fig. 7. Proof of Concept - Decryption

VI. CONCLUSION

While online transaction, a secure connection is when exchange of information between the website you are visiting and Internet Explorer is encrypted. However, user's privacy

can still be compromised by the way the website uses or distributes your information while transaction.

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 minimized in the case of proposed structure.

The proposed work aims to increase the complexity of the transaction process and make the transaction more convenient and strong for the user. Therefore, concept used in the proposed model is increasing the complexity of transaction which makes it more robust against the attack. However, this minimizing the overhead for the user and provides confidentiality.

REFERENCES

[1] Richard Kissel, Kevin Stine, Matthew Scholl, Hart Rossman, Jim Fahlsing, Jessica Gulick, "Security considerations in the system development life cycle," NIST special publication 800-64 Revision 2.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Sona Kaushik, "Strength of Quick Response Barcodes and Design of Secure Data Sharing System," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 2, issue 11, Nov. 2011.