Need of Tokenization and Dynamic Data Masking for Financial Sector of Sri Lanka

S.J. De Silva, D.C. Amarasinghe, D.C. Jayasuriya, Ranatunga R.M.H.N., K.D.D.P. Premarathne, Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- This paper presents a detailed study about how tokenization and dynamic data masking assist for security of banks. Financial sector is one of the most important sectors in any developing country. In financial sector banks are playing a vital role. All over the world, there are lot of transactions happening in banks per day. Most of the people have choose banks as a safe place to keep their money and valuables safely. To secure those money and valuables are difficult for banks because of frauds and vulnerabilities. As a developing country, Sri Lankan financial sector should have proper security mechanisms to secure information, different encryption methods can be used. When it comes to Tokenization and dynamic data masking together it's a new face of encryption methods. It does both encryption and Tokenization which provide more security. Technology is developing day by day. To face the future, new technology should be applied. Therefore the need of implementing research of tokenization and dynamic data masking for Sri Lankan banking sector is the purpose of this study. How tokenization and dynamic data masking assist for security of banks in Sri Lanka has been discussed as in results.

Index Terms- Banks, Tokenization, Dynamic data masking, Encryption, Sri Lanka, Security

I. INTRODUCTION

In the digital world, Security of the financial sector has become an essential factor. Financial sector includes banks which has an important role in it. Banking information is the most precious, therefore banks are increasingly discovering tokenization as a way to keep away cybercriminals. Tokenization can be used to keep the sensitive customer data within the bank's control at all times as external systems have no access to the real data.
Credit cards have become a popular payment instrument in the 21st century. Increasing popularity of business through Internet has make it essential for every business to maintain credit card information of its clients in some form. Credit card data theft is considered to be the most serious threat to any business. Not only amounts to a serious financial loss to the business but also a critical damage to the image of the company. Credit card data are a very sensitive information, and theft of sensitive data is a serious threat to any company. Any organization that stores credit card data such as cardholders name, credit card number, expiry date, card verification value, etc. needs to achieve Payment Card Industry (PCI) compliance. Which is a process where the organization needs to demonstrate that the data it stores are safe. PCI sets a standard called PCI Data Security Standards (PCIDSS) which provides a framework for developing a robust payment card data security process.

However, it is quite expensive for each merchant to maintain a PCI DSS compliance server. There is also a risk if the server has security faults. Therefore there has been a shift in treatment of the problem of storage of payment card information. In this new concept instead of the real credit card data a token is stored, this process is called "Tokenization". The token signifies a look alike of the credit/debit card number, but ideally has no relation with the credit card number that it represents. Solution features the Token Server, which is a virtual appliance for managing access to tokens and tokenizing records and clear-text data.

Tokenization makes it more challenging for hackers to gain access to sensitive data, as compared with older systems in which credit card numbers were stored in databases and exchanged freely over networks. Tokenization technology can, be used with sensitive data of all kinds including bank transactions, criminal records, medical records, loan applications, vehicle driver information, stock trading etc. Solution as Tokenization does not eliminate the need to maintain and validate PCI DSS compliance, but it may simplify a merchant's authentication efforts by reducing the number of system components for which PCI DSS requirements apply.

Reducing the risk of tokenization can be achieved by representing it more difficult for attackers to gain access to sensitive data external to the tokenization system or service. Execution of tokenization may simplify the requirements of the PCI DSS, as systems that no longer collect or process sensitive data. It may have a reduction of applicable controls required through the PCI DSS guidelines.

In addition, Dynamic data masking can be substitute to applications to protect the actual data while having a functional supplement for occasions when the real data is not required. The format of data remains alike and only the values are changed. The figures may be altered in a number of ways, including character shuffling, encryption, and character or word substitution. In any kind of method is chosen, the values are changed in some way makes detection or reverse engineering impossible. Policies regarding security can be created using data masking by creating privileged logins, masking rules, and masking functions. Those logins which are privileged logins get unmasked data. Dynamic data masking certifies that nonprivileged users see only the data they are permitted to see while other data is masked.

Through this paper authors has concentrated on how important is to use tokenization and dynamic data masking in financial sector Sri Lanka as in banks must give priority to the security of confidential information. Similarly banks are supposed to provide all measures necessary to make customers believe that information is transmitted safely and securely. Authors explain about the security vulnerabilities and limitations of banks and how to overcome them. Therefore, the authors suggests tokenization and dynamic data masking to implement in financial sector of Sri Lanka.

II. AIM

The aim of this research paper is to introduce a secure system to encrypt sensitive data in banking sectors. Along with tokenization and dynamic data masking, the system would assist to protect confidential information between the client and the bank when credit transaction process happened. It would create a secure location to store those data with no access to the general database.

Research Questions

A. *Main Research Question*

How tokenization and data masking can be used to secure the confidential information of a banking sector in Sri Lanka?

B. *Sub Research Questions*

a) What are the security issues and attacks related to the Sri Lankan banking sector?

b) What is the procedure of tokenization and data masking?

c) What are the advantages for Sri Lankan banking sector with the proposed solution?

Deliverables

The output of this project will be a report in how tokenization can be used to improve banking and credit card security in case of an intrusion. The main purpose of this report is to cover the scope of the project aim as shown below.

- Identify the main issues and attacks that could be commonly seen in a banks.
- Investigate available security systems to avoid those issues.
- Build a more reliable system to eliminate those security issues and attacks through tokenization and data masking.

III. LITERATURE REVIEW

Usage of data tokenization and other technologies in existing researches:

RSA technology has developed by Xin zhou and Xiaofei Tang, In this encryption method works using two keys called private key and public key. Private Key keeps the server and public key can be given away for any party. These keys are generated with two prime numbers and put it into a particular algorithm as a result it produce private and public keys. This technology lacks secured encryption management, secure application integration and dynamic data masking. Research team will try to develop them in the upcoming project [1].

End to end encryption technology is an encryption method which uses to transfer data, from source to the destination securely. This method uses public and private pre-shared keys to encrypt and decrypt processes. End to end encryption also uses known algorithms in order to generate private key and public key. In the proposed project secured encryption key management and secure application integration will be improved as they are not included in this research [2].

Payment Card Industry Security Standard Council (PCI SSC) has also formulated its guidelines regarding Tokenization. Since this research lacks on demand scalability, secure application integration and dynamic data masking, it will be developed in the proposed project [3].

Euro pay, MasterCard, and Visa (EMV) Tokenization Specification is concerned with a new kind of tokenization that prevents cross-channel fraud by replacing card data (PAN and PAN expiration date) with token data (token and token expiration date). In the proposed project secured data encryption, secured application integration and scalability will be developed as those functionalities are not included in this project [4].

JIET Group of Institutions found a data encryption algorithm that can be used to encrypt data by using ASCII values. It is an algorithm for data encryption and decryption. The secret key used will be modifying to another string and that modified string is used to encrypt or decrypt the data. This algorithm operates only when the length of input and length of key are same. Since this research lacks in dynamic masking and scalability, Research team will try to improve them [5].

SMS security algorithm is used for the interchange of confidential data. The encryption algorithm is characterized by a secret key. The application is develop using programming language Java and the J2ME environment. Sort-time password method is in software-based security systems, the coding and decoding of information is done using specialized security software [6].

Encrypting in the data center applications, servers, databases, and storage, which help us to determine to pick the best encryption option for the projects. It is covers different high-level options and technologies. Proposed project will improve on demand scalability which is lacking from this research [7].

Point to point encryption to validate a secure element in a mobile device when scanned by a terminal. This project lacks on demand scalability and it will be included in the proposed project [8].

Secured application integration technique is before a device starts accessing sensitive data, the device request for a token from the server. After the device receives the token it can access the data that is associated with the token information. The functionalities that are missing such as dynamic data masking and on demand scalability will be included in the proposed project [9].

Dynamic data masking by replacing sensitive data by fake information in technical terms of hiding the sensitive data in the result set of a query over designated database fields. Non-disruptive implementation and on demand scalability will be improved in the proposed project as they are lack from this research [10].

IV. PROBLEMS IN SECURITY SYSTEM OF CURRENT SL BANKING SECTOR

Security of Sri Lankan banking sector is not in safe aside. Day by day financial frauds happening in Sri Lanka. As a developing country these problems will affect in the future in critical ways. And also these problems will lead to reliability issues in customers. In sub section A and B will be discussed some of the security issues and attacks as well as potential problems and limitations in Sri Lankan banking security.

A. Security issues and attacks

In worldwide people are used to do transactions through credit cards and debit cards. Electronic card payment transaction security has become an important issue in Sri Lanka rather than the other foreign countries.

Millions of credit card numbers are stored and sent in to insecure networks. Malicious ones might break into a merchant's server and obtain thousands of credit card numbers as well as consistent information.

There are a various types of credit card fraud but two which are the most common types experienced are such as 'skimming' and application fraud. Skimming is the theft of credit card information in legitimate transaction. This is often done by placing a small device on an ATM which will read and store card details. Which allows the thief to capture a customer's debit or credit card information, including their PIN with each swipe. Basically in foreign countries Systems are implemented using the latest technologies such as tokenization and data masking [11].

Recently Sri Lanka has been ranked amongst the top 10 countries in the world for credit card fraud. Therefore, a number of high profile cases have been recorded recently.

- Four suspects involved with credit card fraud worth Rs. 32.8 million were arrested by the Criminal Investigations Department (CID). The money was all withdrawn on a single day last May out of a well-known bank's ATM network. ATMs in Colombo, Kilinochchi and Jaffna were all targeted [12].
- Involved in the Rs. 263 million frauds by withdrawing money from foreign credit card holders through an e-commerce application service provided by a State bank in Sri Lanka.
- Information on frauds committed using mobile phones [11].

Recently group of two Turkish nationals and one Ukrainian national after surveillance have arrested a by the Police on a tip received. Investigations have revealed that the group has made a number of withdrawals using 33 such fraudulent cards from ATMs (Automated Teller Machines) around Colombo and had visited Sri Lanka three times in the recent past [12].

B. Limitations and potential problems

As defined in section A, there is genuine need to protect confidential information. Limitations of banking due to unavailability of confidential information security. As in security is not perceived as an obstacle or a major concern in mobile banking transactions. It can be understood that people are ready to settle with less secure environment in courtesy of ease of use and convenience. Trust between the bank and the customers will affect due to such circumstances.

Potential problems such as hackers accessing Bank databases and removed withdrawal limits on prepaid debit cards and created access codes. Awareness of potential loss due to fraud or a hacker compromising the security. Therefore, a lot of security vulnerabilities may occur due to lack of security in banks.

V. SOLUTION AND IMPLEMENTATION

According to sub section A and B in section IV, current status of the Sri Lankan banking security and related issues and attacks cannot be satisfied as a developing country. As a solution to eliminate these issues banking security systems must be upgraded. Tokenization is an easy way to maintain sensitive data in banking databases, with data masking can be assign policies and privileges for different users. Figure 01 in Appendix shows how tokenization procedure work and how systems are integrated.

As shows in Appendix Figure 01, Customer credit details will directly go to the Application server in the banking system. Then App server forward customer credit details to token server for tokenization through REST API (REpresentational State Transfer Application Program Interface) which helps to integrate systems securely and to create faster management process. Once the token is created token key related to token will be send to Data security manager to store it securely. Then the original data will be stored in token vault and tokenized data will be send back to app server through REST API. Then app server will store tokenized data in database.

When it needs to DE tokenize stored data it will go back to the reverse order. App server will get related tokenized data from the database and send it to the token server for DE tokenize then data security manager will arrange the token key related to received token value. Once it DE tokenize using token key, token server will get the original information from token vault and set it back to the app server then it will distribute the data for the relevant parties.

As shown Appendix Figure 02, illustrates the task of the dynamic data masking feature. It assigns policies and privileges to control data flow among different users. Which means as an example, User needs to take customer support from bank then customer support person needs to verify the customer first. In this stage customer support person can ask the last four digits of the card because data masking make sure customer support person will only see last four digits of the card number, nothing more shared of credit details. Rest of the details can be verified in other ways such as birthday, address and etc. If customer needs to go for advance change of his or her account then customer service supervisor needs to assist because data masking service can arrange privilege to access his or her credit details. In this case customer support person got half privilege and customer service supervisor got full privilege.

So tokenization and data masking together will give a successful solution for above mentioned problems in sub sections A and B in section IV.

VI. CONCLUSION

Based on the findings done through related research papers and other available online materials, it has become clearer that security for organizations and banking sector is becoming a priority day by day. In order to avoid intrusion to online database systems and other confidential information in banks, the project team has implemented a security system based on data tokenization and dynamic data masking.

APPENDIX

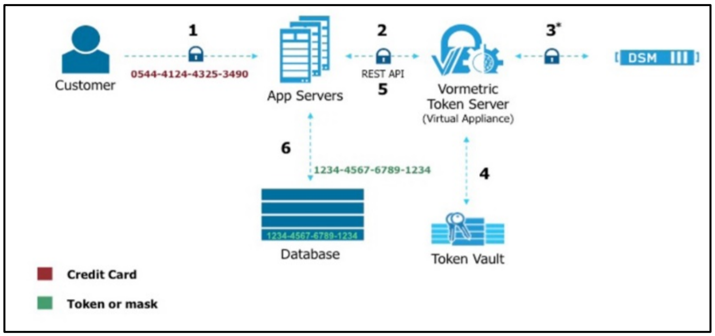

Figure 01: Tokenization procedure
(Source: http://enterprise-encryption.vormetric.com/Tokenization-With-Dynamic-Data-Masking.html)

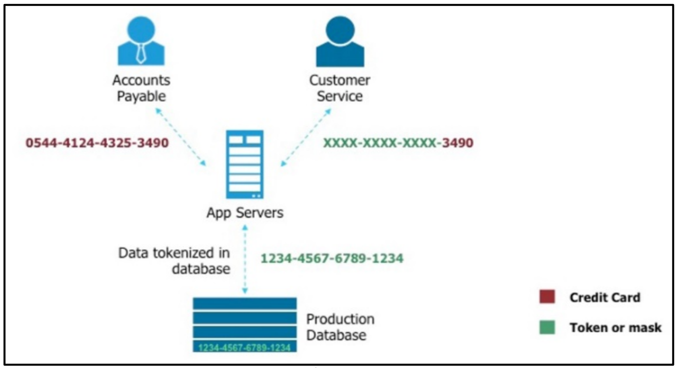

Figure 02: Task of data masking
(Source: http://enterprise-encryption.vormetric.com/Tokenization-With-Dynamic-Data-Masking.html)

ACKNOWLEDGMENT

The research team sincerely thank the lecturer and supervisor in-charge of Computer Networks Designing and Implementation, Mr. Dhishan Dhammearatchi, for carefully guiding the team to improve the research, with kind advice and assistance.

At the same time, the team would like to thank lecturers and staff members of Sri Lanka Institute of Information Technology Computing (Pvt) Ltd and the authors of the referred research papers. Without their contribution to the field, the research would have not been possible to success.

REFERENCES

[1] Zhou X., Tang X., “Research and implementation of RSA algorithm for encryption and decryption”, (2011), <Available URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.4834&rep=rep1&type=pdf>, vol 41, no 14 [Accessed 26.01.2016]

[2] Zeidler H.M., “End-to-end encryption system and method of operation”, (1986), <Available URL:https://www.google.com/patents/US4578530> pg1-3 [Accessed 26.01.2016]

[3] Diaz-Santiago S., Rodríguez-Henriquez L.M., et al., "A cryptographic study of Tokenization systems", International journal of Information Security, Springer-Verilog Berlin Heidelberg (2014), <Available URL: http://link.springer.com.sci-hub.io/article/10.1007/s10207-015-0313-x> pg. 2-3 [Accessed 03.02.2016]

[4] Corella F., Lewison K., "Interpreting the EMV Tokenization Specification", (2014), <Available URL:https://pomcor.com/whitepapers/EMVTok.pdf> pg2-6 [Accessed 03.02.2016]

[5]Mathur A., "An ASCII value based data encryption algorithm", International Journal on Computer Science and Engineering, (2012), <Available URL: http://www.enggjournals.com/ijcse/doc/IJCSE12-04-09-103.pdf>, Vol. 4, No 9, pg. 1-8 [Accessed 03.02.2016]

[6] Shazmeen S., Prasad S., "A Practical Approach for Secure Internet Banking based on Cryptography", (2012), <Available URL: http://www.ijsrp.org/research-paper-1212/ijsrp-p12122.pdf >, Volume 2, no 12, pg. 1-2 [Accessed 03.02.2016]

[7] Securosis L.L.C., "Cracking the confusion: Encryption and tokenization for data center, Server and application", (2015), <Available URL: https://securosis.com/blog/cracking-the-confusion-encryption-and-tokenization-for-data-centers-servers > pg. 1 [Accessed 26.01.2016]

[8] Securosis L.L.C., "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization", (2015), <Available URL: http://www.smartcardalliance.org/wp-content/uploads/EMV-Tokenization-Encryption-WP-FINAL.pdf >pg.4-6[Accessed 03.02.2016]

[9] Cambridge D.M., Kean B., et al, "Systems and Methods for Tokenizing Financial Information", (2012), <Available URL:https://www.google.com/patents/US20120303503> [Accessed 05.02.2016]

[10] Mattsson U., "Method and Apparatus for Tokenization of Sensitive Sets of Characters" (2013), pg <Available URL:https://www.google.com/patents/US8578176> [Accessed 05.02.2016]

[11] http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=81920

[12]http://www.colombopage.com/archive_14B/Jul16_1405526550CH.php

AUTHORS

First Author – S.J. De Silva, BSc. in Information Technology (I.T.) student at SLIIT, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-(SLIIT) and email address-jinaathdesilva@gmail.com.
Second Author – D.C. Amarasinghe, BSc. in I.T. student at SLIIT, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd and email address- devindrachamindi@gmail.com.
Third Author – D.C. Jayasuriya, BSc. in I.T. student at SLIIT, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd and email address- deshanijayasuriya@gmail.com
Fourth Author – Ranatunga R.M.H.N**.**, BSc. in I.T. student at SLIIT, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd and email address- nuwanthika02@gmail.com
Fifth Author – K.D.D.P. Premarathne, BSc. in I.T. student at SLIIT, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd and email address- dumalapremarathne@gmail.com

Correspondence Author – Dhishan Dhammearatchi, email address-dhishan.d@sliit.lk