International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-4 (August 2020)
www.ijemr.net https://doi.org/10.31033/ijemr.10.4.2

A Review of Information Security from Consumer's Perspective Especially in Online Transactions

Mohammad Salman Husain[1] and Dr. Mohammad Haroon[2]
[1]PG Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA
[2]Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: salmank094@gmail.com

ABSTRACT

In the current internet technology, most of the transactions to banking system are effective through online transaction. Predominantly all these e-transactions are done through e-commerce web sites with the help of credit/debit cards, net banking and lot of other payable apps. So, every online transaction is prone to vulnerable attacks by the fraudulent websites and intruders in the network. As there are many security measures incorporated against security vulnerabilities, network thieves are smart enough to retrieve the passwords and break other security mechanisms. At present situation of digital world, we need to design a secured online transaction system for banking using multilevel encryption of blowfish and AES algorithms incorporated with dual OTP technique. The performance of the proposed methodology is analyzed with respect to number of bytes encrypted per unit time and we conclude that the multilevel encryption provides better security system with faster encryption standards than the ones that are currently in use.

Keywords-- Online Transaction, Blowfish Algorithm, AES Algorithm, Dual OTP, Banking System

I. INTRODUCTION

In order to provide security to the customer, existing banking system uses various levels of security mechanisms. Even though tough encryption standards are provided against network attacks, it is prone to be broken. Intruders are smart enough to retrieve the passwords of the customers through online transaction. As per the world payments report, in current technology people prefer to use cashless payments rather than the cheques or cash payments. As we all know that these kinds of e-transactions provide huge number of benefits to the customers for example, by making the transactions easier, faster and instant payments. Overall, as per the survey an Indian uses online transaction system once in a week for payment. This online transaction might be through credit/debit cards, e-wallets, UPI's, food cards, travel cards and some authorized e-payment systems.

Many security implementation methods like hardware level security, antivirus, anti- malware and antispyware programs, strong passwords, single time bound OTP system, virtual private network, secured site uses SSL certificate are used in practice. However, in spite of all these security mechanisms intruders go for brute force attempts to decrypt the PIN numbers and passwords etc. So, single level encryption standard is not sufficient to provide high level security for online transaction system. At present we need to have a multilevel encryption standard wherein even if anyone encryption standard is broken, the online transaction requested by the customer will be completed with the other Encryption standard. Our paper focuses on multilevel security with Blowfish and AES algorithm along with dual OTP scheme which may lead to stronger level of protection against threat encountered in online transactions. The paper has been organized as follows: Section II describes about the related work and section III depicts the proposed system of security. Section IV deals with experimental results and finally section V concludes the paper.

II. RELATED WORK

In [1], the different methodologies adopted for e-transactions security in mobile devices against security threat has been discussed which has severe drawback over multi-level transactions. Using longitude and latitude [2], according to the location high level authentication has been incorporated to overcome the intruder attack in network transactions. The various privacy risks and their impact [3] on mobile payment services are extensively focused and various limitations also depicted to create awareness among customers of online transactions. In [4], two factor security model based on QR based login system is discussed and it has limitation over scanning of QR code. Innovation in mobile wallets [5] has been arised in e-commerce services and its impact and security over the communication network and banking system is also under research against malicious attacks. At current scenario, a more secured mechanism is vital for online transaction and one such method is visual cryptographic methods [6] for e-commerce system which is less vulnerable to attacks. Apart from password-based authentication, more reliable future protection mechanisms against electronic payment attacks are discussed by the paper Jeffus et al [7]. A method of data mining security [8] using privacy preserving is another context of data extraction in the internet. In this paper [9], every transaction sent by the customer is wrapped around an image and has been shown with improved efficiency against security attacks.

In [10], a new methodology of steganography with images has been proposed which is shown to be having less amount of data transfer between merchant and the customer. A mobile based E-Wallet [11], is an innovative method incorporated in the e-world which is assumed to be less time consuming. Banking and financial institution [12] is actually influenced by the most of the advancements in science and technology.

III. PROPOSED METHODOLOGY

A. Blowfish and AES Algorithms

For the multilevel security implementation, blowfish algorithm found to be the better performance-oriented algorithm due to the low block size. In the context of this paper, as we use multilevel security mechanism, in the first level if there is any e-transaction between the intra banking system, then Blowfish algorithm has been incorporated which is found to be less time-consuming process. In the second level when there is a transaction between a host of one bank and the host of another bank then it is desired to incorporate high level of security and that is the place, we put in forth the AES authentication mechanism.

B. Dual OTP Strategy

Apart from the two-level authentication, one more security mechanism with respect to dual OTP also imposed in the proposed methodology. With this method, all the banking customers are supposed to have two mobile numbers. First primary number will be the customer number and the secondary number is the confidante that the customer provides when registering with the bank. Both these OTPs shall together validate the transaction. Failure to provide even one of them will see the transaction fail. Using this strategy an added measure of security can be incorporated into the system.

C. Transaction

When the client makes contact for a transaction, the server needs to check whether the transaction is intra-bank or inter-bank. If the transaction is intra-bank, blowfish is set as the encryption standard. However, if the transfer is to a different bank, the standard is set to AES.

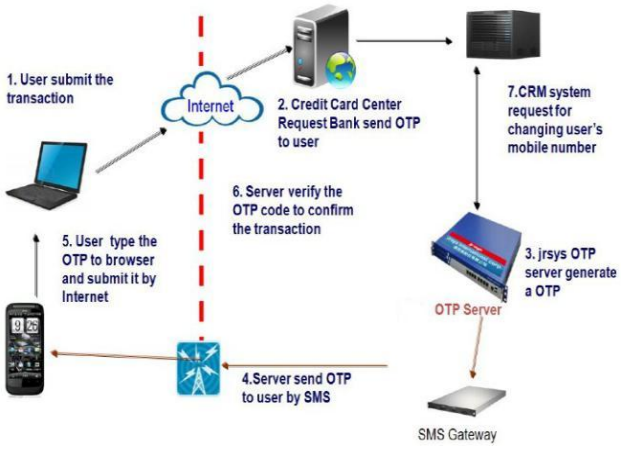

Figure 1: Banking Transaction

An example online banking transaction is shown in figure1 that involves server authentication. First step of transaction is user authentication followed by server verification and finally OTP generation. Then the user is allowed to make the payment for the e-commerce websites.

IV. RESULT ANALYSIS

The performance of the proposed algorithm is measured with the help of core i3,7th generation machine with JDK implementation and a database backend for storing user information.

The performance of the blowfish and AES encryption standards with respect to number of bytes encrypted is shown in table I and II.

Table 1: Blow Fish Performance

Time Elapsed(s)	Bytes Encrypted
136	137325
158	158959
162	1663634
176	191383
219	232398

The time taken for encryption is less and thus improves the performance of the banking system. Advanced encryption algorithms like RSA algorithm takes more time in the encryption process as it is involved with large prime number generation. In blowfish algorithm we use less rounds of computation and thus saves time of encryption and leading to fast access to banking system during online transaction.

Table 2: AES Performance

Time Elapsed(s)	Bytes Encrypted
136	137325
158	158959
162	1663634
176	191383
219	232398

Similarly, AES algorithm also provides greater time consumption in encryption process and thus gives speedy transaction. Although, AES is an ancient algorithm used for encryption the time elapsed for encryption still found to be better than the RSA algorithm.

The actual simulation of the transaction system starts with a new user registration page created wherein customers have to enter all the details about them and a new login will be created. When the customer wants to perform any online transaction, he has to go inside the login page. An implementation of the banking system is incorporated with a login page shown in figure2. Once the login page is created the customer details are registered in the banking system. All the user passwords are encrypted inside the database with blowfish algorithm.

Figure 2: Login Page

Once the user authentication is verified at the back end then the customer is allowed to access the entire features of banking system.

Figure 3: Transaction using OTP

While entering the customer details during registration, it is mandatory that two mobile numbers are required from the customer side: primary number and a secondary confidante number. The strategy of dual OTP is incorporated with these two phone numbers. The innovation in multi level encryption is the generation of this dual OTP. The dual OTP generated during the customer online transaction is shown in figure3. This security system improves the performance against threats that is a major concern in online transactions.

Figure 4: OTP Verification

As per the dual OTP strategy, first OTP will be generated to the customer primary mobile as shown in figure 4, which has to be initially validated against the banking server.

The main focus on this kind of new mechanism is to give the online transaction users the facilities to perform the transaction easily without any complexities [13]. As per our proposed system, we find performance improvement not only in security but also with respect to faster access of transaction over the online banking system.

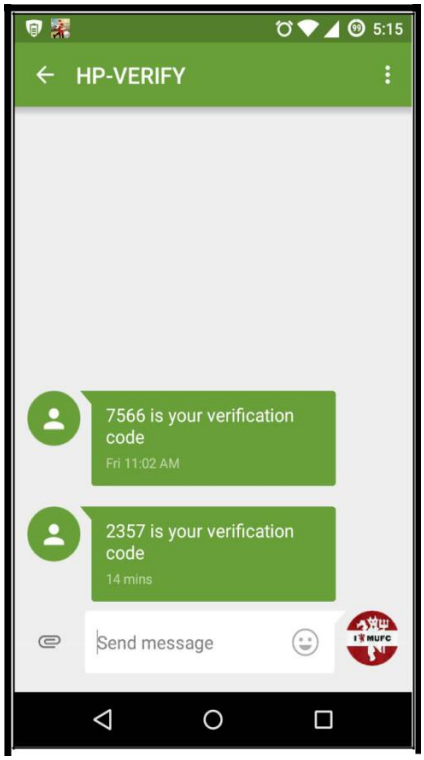

Figure 5: Dual OTP Verification

Later, the second OTP will be generated (figure5) to the secondary mobile and both will be verified by the banking system. Once after the authentication from the bank, then the online transaction will be initiated.

V. CONCLUSION

As in the world of digitization, lot of attacks over E-transactions has been a greatest threat for e-commerce sites. Altogether both customers and banking security systems are affected through various malicious attacks by the intruders. Although huge security algorithms through various measures and means have been incorporated but still more authenticated services needed for transactions on internet. One such multilevel security mechanism has been imposed in this paper and provides more than 10% performance over time and security compared to existing algorithms. Dual OTP scheme is also one of the identified high security over one-time OTP system. In future more reliable visual cryptographic and time consuming steganography methods can be used in e-transactions.

REFERENCES

[1] F. Gao, P. L. P. Rau, & Y. Zhang. (2018). Perceived mobile information security and adoption of mobile payment services in China. *Mobile Commerce: Concepts Methodologies Tools and Applications*, 1179-1198.

[2] Dr. A.L.N Rao, Silky Puri, & Shalini Rana. (2013). Review: Location based authentication to mitigate intruder attack. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(9), 336-339.

[3] V. L. Johnson, A. Kiser, R. Washington, & R. Torres. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior, 79*, 111-122.

[4] Soonduck Yoo, Seung-jung Shin, & Dae-hyunRyu. (2013). An innovative two factor authentication method: The QR login system. *International Journal of Security and Its Applications, 7*(3), 293-302.

[5] S. Mittal, V. Kumar. (2018). Adoption of mobile wallets in india: an analysis. *IUP Journal of Information Technology, 14*(1), 42-57.

[6] M. Suresh, B. Domathoti, & N. Putta. (2015). Online secure e-pay fraud detection in e-commerce system using visual cryptographic methods. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(8), 7519-7525.

[7] B. Jeffus, S. Zeltmann, K. Griffin, & A. Chen. (2017). The future of mobile electronic payments. *Journal of Competitiveness Studies, 25*(3-4), 216-223.

[8] R. Purohit & D. Bhargava. (2017). An illustration to secured way of data mining using privacy preserving data mining. *Journal of Statistics and Management Systems, 20*(4), 637-645.

[9] N. Shrivastaval & T. Verma. (2015). A survey on various techniques for generating image steganography with improved efficiency. *International Journal of Advanced Research in Computer Engineering & Technology, 4*(3), 1005-1009.

[10] S. Roy & P. Venkateswaran. (2014). Online payment system using steganography and visual cryptography. In: *Proceedings of the IEEE Conference on Electrical Electronics and Computer Science*, pp. 88-93.

[11] G. Kanimozhi & K. S. Kamatchi. (2017). Security aspects of mobile based e wallet. *International Journal on Recent and Innovation Trends in Computing and Communication, 5*(6), 1223-1228.

[12] Mr. Shakir Shaik & Dr. S.A. Sameera. (2014). Security issues in e-banking services in Indian scenario. *Asian Journal of Management Sciences, 02*(03), 28-30.