THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Issues and Advantages of Biometric In Online Payment of E-Commerce

Ekta Saharan [#1], **Sumit Bansal** [*2]

[#1]ktsan313@gmail.com

[#1]Assistant Professor, Lovely Professional University
Jalandhar, India

[*2]sb002@ymail.com,

[*2] Assistant Professor, Gurukula Kangri Vishwavidyalaya
Haridwar, Uttarakhand

Abstract— Internet is an incredible tool and it has changed the lifestyle of individuals considerably. It is the simplicity, time factor and efficiency, which have contributed to the popularity and growth of e-commerce [1]. Most of the problems that occur during payment are durability, security etc. Now a day's mobile phones, tablet or laptops are widely used for online transactions in E-Commerce websites.

The security for online business is very much required in cyber space, Because the technology is rising day-by-day. Frauds like using calls, card cloning, phishing attack, hacking the internet enabled devices etc. are rising eventually [2]. Various techniques utilized by researchers/authors include Password, PIN, OTP to reduce these types of problems. Since the password or PINs used for online payments, e-commerce can be hacked in cyber space, so alternate security methods are required. Therefore, it is very important to develop a safe Authentication and verification method which is difficult to hack or steal. We can use Biometric to enhance the security. This research paper use of biometric techniques and biometric system to overcome these kinds of misuse of information and unauthorized accesses.

Keyword: *Biometric, Security, E-commerce, CIA*

I. Introduction

A. E-Commerce

In wireless trading (Pre scale, post scale, buy) e-commerce pays an important role. It satisfies the growing needs of organization, business purpose etc. in our daily lives. E-commerce is selling or buying goods or services with the help of internet enabled devices. E-commerce is really a fast and simple to use method in these days. E-commerce provide many services like ticket booking, mobile banking, mobile purchasing, online transactions, online shopping etc. Because of these types of services, it gives a way to users for universal devices to be used anywhere freely. [3]

B. Issues

1. Password hacking is among the commonly faced problem in these days. Hackers hack a code of an individual and misuse its services.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

2. Phishing Attacks: - Phishing identifies the method of acquiring login details password, PIN, user name in an electric communication. Various kinds of phishing attacks are following: -

3. Fake calls are among the latest trending problem. An unauthorized person calling and wish to know your password, PIN and other important information.

4. Spam E-mails is the web mails that has any electronic mail to lure the consumer into trap where user gives confidential details and information.

5. Messages Phishing: - Various types of forges are done by sending false messages to different users. It requires the benefit of confidential details written by user.

6. Card Cloning: - Whenever we swipe the card on machine it captures the cards details like number, pin code, CVV number which could result in misuse of card.

7. Sniffing Devices: - You will find devices that monitor the information travelling on the network. [5]

II. BACKGROUD

A. *The CIA principle*

The essential principal for security analysis is CIA triad. It represents confidentiality, integrity & availability. In just about any secure system these three parameters are necessary. These principals are applicable beginning with the user's internet history to the complete encrypted data of internet. They are elaborated the following: -

- *Confidentiality*

It involves pair of rules of promises that limit access on certain kind of information. Cryptography and encryption are normal to the confidentiality of transferring data in one device to another.

- *Integrity*

In simple words integrity means data in model is accurate and representation of original information in encrypted.

- *Availability*

A means information is easy to get at to any or all the authorized viewer most of the time. [6,13]

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

B. Biometric

Biometric includes methods for uniquely recognizing humans in relation to more than one intrinsic Physical or behavioral traits [3,4,12]. In computer science biometric is useful for access control and identification/authentication. In biometric unique characteristics of an individual is identified and solved and later in verification phase are re-checked upon the effect i.e., if the person's traits match or not then a access is given.

These biometric features widely useful for verification and identification purposes in securing online transactions.

- *Fingerprint*

This method is one of the widely used identification of a user or an individual. Fingerprint is used for security in biometric. Fingerprints of each and every person is unique. It is not possible to match finger print of two different persons. Fingerprint is also one of the good security ways. We can extract the useful information by using minutiae in fingerprint. It is a cheap and easy to implement. [5,11]

- *Face Recognition*

Face Recognition is another idea that is used in biometric devices for identification. In face recognition all the faces match with database and it is accepted or rejected by biometric device.

- *Iris Recognition*

Iris contain pupil and outer responsible for identification of an individual. Pupil is dark colour centred surrounded by another in which into is stored and extracted afterword by a ring and matched with database.

C. Advantages of Payment by Biometric Methods:

Some of the advantages over the biometric payment as compare to the other methods of payment defined below: -

- *Security*

  In the other security techniques, the data is easily copied but in biometric payment systems data or keys cannot be copied easily.

- *Uniqueness*

  All the biometric data is unique. In other security methods password, PINs may be same (like A=12345678, B=12345678 etc.) for two or more than two persons but in the Biometric authentication method it is not same.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

- *Performance*

Performance of biometric data is good as compare to others ways of payment. In this user first enter the password or PIN then system access granted but in biometric, only the mandatory parameter is to the touch the screen and access is granted. Because of this method performance of the machine can also be increased.

- No Need certainly to Change

In biometric security, user will not need to alter password or keys time and energy to time. In PIN and passwords security user change their security codes/keys to guard their system from hackers or unwanted issues that will come in the system.

III. LITRATURE SURVEY

Different researches carried out and different ways were found in e-commerce using biometrics. This paper represents various techniques to secure e-commerce and e-payments in a better and a reliable method. These methods are elaborated in various section with this paper.

A. In this research paper authors Simon Liu and Mark Silverman proposed different kind of authentication approaches for e commerce/Payments. [8,14]

In these techniques some personal number or password that's set by an individual is entered to accomplish the transaction. In other methods/techniques a Password that could be lots or word delivered to user's cellular phone and after receiving the PIN the transaction is completed.

One of many other techniques that's discussed is biometric technique. In these different biometric methods are accustomed to complete the transactions. Biometric technique provides a distinctive authentication for payments in the e-commerce. Many biometric techniques like face, fingerprint, iris, signature is found in the e-commerce.

In 2001 silverman and liu discussed concerning the working of biometric system. In this technique firstly the biometric is captured that is chosen for authentication, extracting the biometric template then storing the template in repository and then matching the template from the stored template.

B. In this research paper ‘Rajendra Reddy Vangala Sreela Sasi Ph.D. used internet-based architecture to make use of encrypted iris patterns as biometric attribute for authentication of a person for e-commerce transaction.

In this method higher level resolution images are needed. Also discusses very efficient method for preventing charge card frauds. The iris images are processed, and normalized.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

The features are extracted from the image using principal component analysis and encrypted using RSA. [2]

C. In Conclusion of “Security role of biometric in Electronic Transactions” author Mr. Anshuman Tyagi, Mr. Piyush Bhustyhan Singh, Mr. Vikash Singh Yadav, Mr. Sang harsh Kumar Singh, Dr. Amod Tiwari says electronic communication is quite commonly found in all security requirements for example authentication, privacy/ confidentiality, integrity and non-repudiation. Cryptography isn't helpful against thefts but additionally helps in user authentication. [7,9,15]

In addition, it uses PIN, password and biometric for authentication. The rest of the kind of the security ways is challenging to keep in mind by any person however the biometric could be the permanent or unique identification of user. In biometric password, token, PIN, remember issues are removed or finished.

In addition, it discusses fraud detection by which every individual that performs the transaction registered in virtually any device the info of individual is stored in database and it may result in the misuse of stored information further.

D. Author’s Nikita Gupta, Devendra Mani Tripathi from International Journal of Computer Applications discussed the possible biometric identifiers. In this paper the accuracy of face print, voice is high but key stroke dynamic is medium. The survey reveals that two level authentication surpasses single level authentication. First one is PIN based authentication and second is biometric authentication. To implement the fingerprint in mobile payment system the writer used J2ME as a platform. It proposed water mark device for an additional security level for authorization process. [4,12]

E. In research paper “Enhancement of security with assistance from real-time authentication and one-time password in e-commerce transactions” the authors Z. Zareh Hosseini & E. Barkhordari use three various kinds of authentication for providing security in e-commerce transaction. From the authors viewpoint three identification are PIN based, OTP (one-time password) & biometric authentication.

In this research paper the researcher says we can offer robust identification and authentication to the e-commerce transaction by biometric sensibility techniques like iris, fingerprint authentication with one-time password. [9]

Utilizing the hash function, the feature extraction is hashed and then hashed template will undoubtedly be encrypted by utilizing public key and finally and it's transmitted to the merchant site and then decrypted at other side.

F. In research paper “Access control system with advanced security using fingerprints” the authors Younhee Gil, Dosung Ahn, sung bum Pan, Yongwha Chung discuses concerning the fingerprint

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

verification system consisting of two phases enrollment and verification. Additionally, it implements multiple fingerprint images and enhanced matching methods. It uses fingerprint verification algorithm using FVC 2002 database. Enrollment using multiple impression are accustomed to enhance the matching performance of fingerprint. [10]

IV. CONCLUSION

In all types of the security mechanisms in e-commerce some type of errors or security issues are involved. So, it is important to improve its security problems.

There are many security issues as discussed above in e-commerce. Some researchers have provided the solution and some methods are still being developed to resolve these issues and increase the performance, integrity, security and accuracy of the system. Instead of it there is need of more techniques of security in the biometric.

REFERENCES

[1] Bobde, M. S. S., & Satange, D. N. (2013). Biometrics in Secure e-Transaction. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2(2).

[2] Vangala, R. R., & Sasi, S. (2004, May). Biometric authentication for e-commerce transaction. In *2004 IEEE International Workshop on Imaging Systems and Techniques (IST)(IEEE Cat. No. 04EX896)* (pp. 113-116). IEEE.

[3] Sankaranarayanan, D. S. (2010). Biometric Security Mechanism in mobile Payment. *Published by the IEEE Computer Society*.

[4] Gupta, N., & Tripathi, D. M. Comparative Study of Different Biometric Authorization for Mobile Payment System.

[5] Raina, V. K. (2011). Integration of biometric authentication procedure in customer oriented payment system in trusted mobile devices. *International Journal of Information Technology Convergence and Services*, *1*(6), 15.

[6] Shahzad, A., & Hussain, M. (2013). Security issues and challenges of mobile cloud computing. *International Journal of Grid and Distributed Computing*, *6*(6), 37-50.

[7] Tyagi, A., Singh, P. B., Yadav, V. S., Singh, S. K., & Tiwari, A. (2012, December). Security role of biometrics in electronic transactions. In *2012 IEEE International Conference on Computational Intelligence and Computing Research* (pp. 1-3). IEEE.

[8] Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, *3*(1), 27-32.

[9] Hosseini, Z. Z., & Barkhordari, E. (2013, May). Enhancement of security with the help of real time authentication and one time password in e-commerce transactions. In *The 5th Conference on Information and Knowledge Technology* (pp. 268-273). IEEE.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[10] Gil, Y., Ahn, D., Pan, S., & Chung, Y. (2003, October). Access control system with high level security using fingerprints. In *32nd Applied Imagery Pattern Recognition Workshop, 2003. Proceedings*. (pp. 238-243). IEEE.

[11] Chopra, J. (2013). The Role of Security Techniques in Biometric System. *International Journal of Computer Applications in Engineering Sciences*, *3*(1), 41.

[12] Zhu, H., Zhang, Y., & Wang, X. (2016). A Novel One-Time Identity-Password Authenticated Scheme Based on Biometrics for E-coupon System. *IJ Network Security*, *18*(3), 401-409.

[13] Eyeh, S. O. (2018). *Web-Based Biometric Application Development with Performance and Security Evaluation* (Doctoral dissertation, Federal University of Technology, Owerri).

[14] Gordon, M., & Sankaranarayanan, S. (2010, September). Biometric security mechanism in Mobile paymentts. In *2010 Seventh International Conference on Wireless and Optical Communications Networks-(WOCN)* (pp. 1-6). IEEE.

[15] Campisi, P. (2013). *Security and privacy in biometrics* (Vol. 24). London, UK:: Springer.