

AN Analysis of Security using ECDH in E-Commerce

Bhupinder Singh¹ Ashwani Sethi²

^{1,2}Department of Computer Science & Engineering

^{1,2}Guru Kashi University, Talwandi Sabo, Punjab, India

Abstract— This paper illustrates the power of internet and other online source proof like a boon for e-commerce market. The e-commerce not only revolutionized the way of business and shopping but also gifted number of new opportunities, advantages to the masses. We also discuss about the SWOT analysis of e-commerce which will depicts its strengths, weaknesses and threats. This research paper tells about the overall development of e-commerce in India and discusses the future trends of India’s e-commerce in comparison to developed countries. In this paper, we found that in coming time the e-commerce will surely the creams of the crop in business world for the people of India.

Key words: Online Marketing or E-Commerce, Digital Locker, Elliptical Curve Cryptography (ECC)

I. INTRODUCTION

Mainly, e-commerce is the term used for the process of buying and selling of goods and services on the internet by using numerous different online networks especially World Wide Web. The development of e-commerce has provided the wonderful opportunity to the companies moving their business up to the global level with help of the online environments. Dot com craze has stimulated a global commercial environment which is now being exploited by many firms who are engaged in e-commerce.

A. Types of E-Commerce

The major different types of e-commerce are: business-to-business (B2B); business to- consumer (B2C); business-to-government (B2G); consumer-to-consumer (C2C); and mobile commerce (m-commerce).

II. DIGITAL LOCKER

DIGILocker is simply a website where people can store their various government issued documents, using their Aadhaar card as their identification. While it hasn’t been stated as such, to us, it also looks like a good way of bringing data from different government agencies together under the aegis of the Aadhaar card, potentially making the document more useful to people carrying it.

III. HOW TO ACTIVATE DIGITAL LOCKER SYSTEM

To access this facility there is need to perform following steps one by one and all these steps are explained follow:

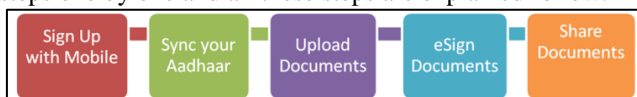


Fig. 1: Flow to Activate Digital Locker System

IV. FLOW CHART OF DIGITAL LOCKER

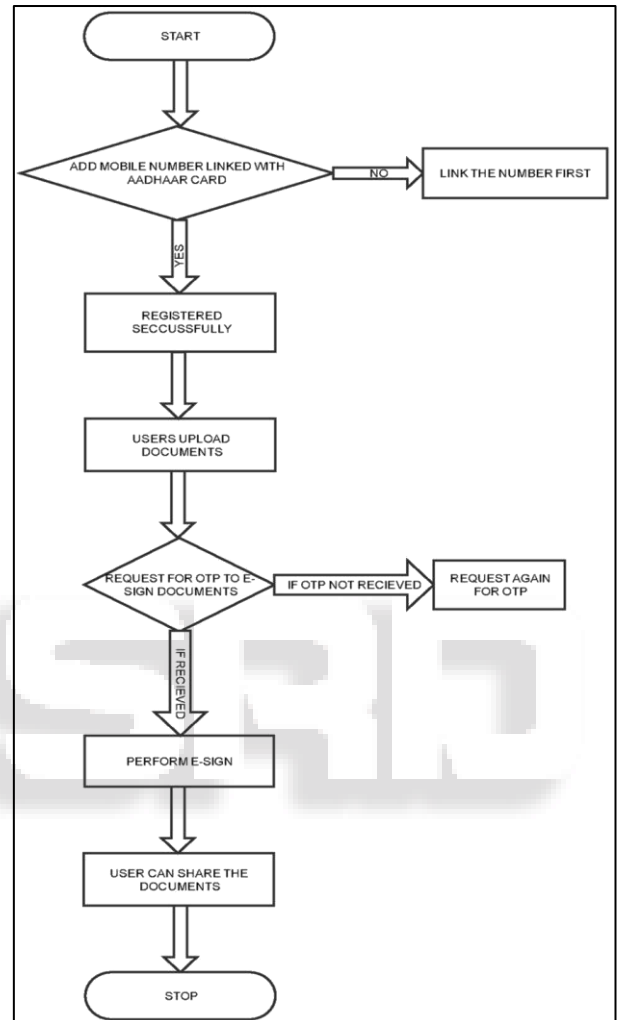


Fig. 2: Flow Chart of Digital Locker

V. SECURITY ANALYSIS OF DIGITAL LOCKER

As it is palpable that security is must to secure the data of people but the main problem is the proxy signer which can easily copy the message that is e-sign of any user. To overcome this hurdle there is well developed algorithms which not only secure the data from proxy signer but also define all type of attacks on the data. These algorithms consist of four different phases and these are the system initialization phase, the key generation phase, the proxy multi-signature generation phase and the proxy multi-signature verification phase.

VI. WORKING OF SECURITY ALGORITHM OF E-SIGN IN DIGITAL LOCKER

A. Create Digital Signature

Here, put values of a and b to generate the digital signature. Suppose we put value of a and b is 7 and 11 respectively and then after that digital signature is created successfully with these values.

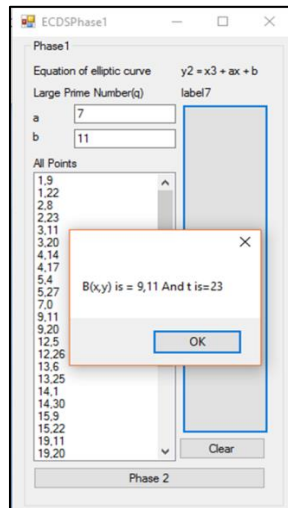


Fig. 3: Digital signature is created successfully

B. Verify proxy signer and analysis the attackers

Here it is clearly seen that in the phase two of security algorithm proxy signer is successfully Copt and create the same digital signature by copy the same values. In then in the next phase attackers are verified and after that verification is done by the phase 4.

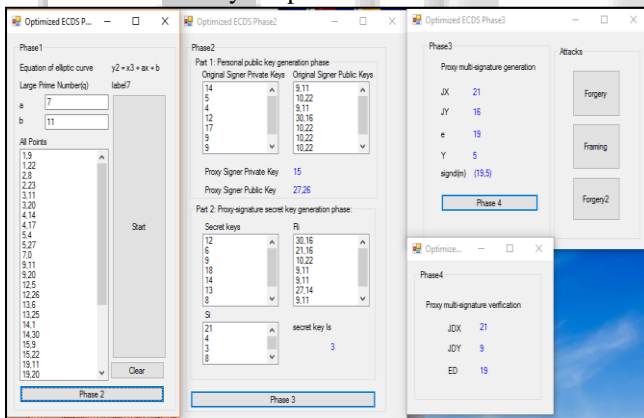


Fig. 4: Verify proxy signer and analysis the attackers

VII. DISADVANTAGES OF DIGITAL LOCKER

A. Lack of Knowledge

Populations of India is digitally divide so only limited numbers of people are aware about this concept and know how to use it. So this is the very big hurdle in the success path of digital locker.

B. Lack of Security

The only problem remains is the trust that their data will not be breached by government or anyone else. Earlier we have seen that government had breached their data. Still there is a doubt over the security whether it is fully secured or not. I felt that there is still lacuna left in this service, so people might think uploading their documents once again.

C. Challenge to Verify Documents

Due to the lack of verify process within the digital locker people faces numerous problem while applying their digital documents in any process and all this happens only because of proper verification procedure.

D. Acceptability Issues

This big issue which cannot be solved without proper information is that some people in various departments still not agree to accept softcopies over the hardcopies.

E. Not Mandatory in Every Field

As it is seen that nowadays CBSE and RTO any many other offices fully adopt the procedure of digital locker and also perform it but there are still offices of government which are not using and also follow it

VIII. SUGGESTIONS

A. Mandatory in Every Government Office

Government ministries and departments should start using digital locker. Citizens who want to hold their important documents in digital format, like PAN card, driving license and many more should receive them directly in digital locker account.

B. Save History

Digital locker also should save all the record of submission and sending documents so that people can easily check all their sending's and belongings of documents.

C. Changes in Verification Process

Currently, documents are verified through AADHAR. There is a need to create a centralized repository of Universities, HR departments of all major companies/ Government department and Financial institutions, through which the authenticity of a document be verified in a little frame of time.

D. Automatic Process is required

For any document generated by government in any person's name then that document copy should be directly loaded to that person digital locker with government label. So no duplicate its real, original and can be blindly accepted for any other reference. Simple and efficient solution.

E. More Secure

There should be any mark of the govt. on the document which can prove that such document has been authenticated by the govt.

F. Extra Facilities

There should be facility to share more than one document from digital locker account at once.

IX. CONCLUSION

It is not gain saying that the main of digital India is to implement the new and technical procedures. The Hon'ble Prime Minister Narendra Modi's vision to transforming the nation by creating new opportunities by using and exploring the internet for field of commerce or other too and the cream of the crop from all those is the Digital Locker. Digital Locker is a ideal scheme which is release by the Digital

India Campaign by the higher authorities of India to provide a platform to save documents digitally under full protection and security of the documents. This is a like turning new leave life for the e-commerce as well as economy of India. It also act like a boon for rural areas and local citizens as this program not only store documents digitally but also offer numerous other amenities and only because of these the program touches the astronomic success.

X. FUTURE WORK

From this study it is crystal clear that regarding the comparative study of e-commerce successful implementation and use in order to make profit in developing countries following work must be done.

- Create awareness of what electronic commerce basically is and how to make effective use of it
- Create a legal framework conducive to e-commerce
- Address financial and bank regulatory issues to help the people. Address financial and bank regulatory issues to help the people.
- Advance implementations in Digital Locker to improve its quality.
- More facilities are provided under digital India procedure as well as in digital Locker.
- At present only verification of attackers are possible so further more development can be done to control these attacks so that users can easily control proxy signers

REFERENCES

- [1] Alev M. Efendioglu, Vincent F. Yip, William L. Murray(2011), "E-Commerce in developing countries: issues and influences", *Journal of Management Information Systems*, Vol. 8, No. 2: 31-52
- [2] Ba, S. and P. A. Pavlou "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior," *MIS Quarterly*, Vol. 26, No. 3: 243-268, September 2002.
- [3] Chua, C. E. H., L. Cao, K. Cousins, and D. W. Straub "Measuring Researcher-Production in Information Systems," *Journal of the Association for Information Systems*, Vol. 3, No. 6: 145-215, January 2003.
- [4] Cohen, L. E. and R. Machalek "A General Theory of Expropriative Crime: An Evolutionary Ecological Approach," *American Journal of Sociology*, Vol. 94, No. 3: 465-501, November 1988.
- [5] Cecil Eng Huang Chua, Detmar W. Straub and Savitha Kadiyala(2008), "The Evolution of E-Commerce Research: A Stakeholder Perspective", Levin et al.: Online/Offline Shopping Preferences
- [6] D. K. Gangeshwer(2013), "E-Commerce or Internet Marketing: A Business Review from Indian Context", *International Journal of u- and e- Service, Science and Technology* Vol.6, No.6 (2013), pp.187-194
- [7] DeLone, W. H. and E. R. McLean "Information Systems Success: The Quest for the Dependent Variable," *Information Systems Research*, Vol. 3, No. 1: 60-95, March 1992.
- [8] Freeman, R. E. (1984) *Strategic Management: A Stakeholder Approach*. Boston, MA: Harper-Collins.

- [9] Frooman, J. "Stakeholder Influence Strategies," *Academy of Management Review*, Vol. 24, No. 2: 191-205, April 1999.
- [10] Nisha Chanana and Sangeeta Goele(2015) "Future of e-commerce in India", *International Journal of Computing & Business Research*
- [11] Muhammad Awais and Tanzila Samin (2012), "Advanced SWOT Analysis of E-Commerce", *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 2, No 2, March 2012
- [12] Ms.Mehek Gulati, Ms.Kanika Verma "Digital Locker", *International Journal of Emerging Technologies and Innovative Research* (www.jetir.org), ISSN:2349-5162, Vol.3, Issue 6, page no.205-206, June-2016
- [13] Mr. Petare Purushottam Arvind, Dr. Mohite Pratapsinh Vitthalrao, Ms. Joshi Mugdha Mukund," digilocker (digital locker-ambitious aspect of digital india programme), *GE-international journal of management research volume-3.issue-6(June 2015)* IF-4.316 ISSN: (2321-1709)
- [14] Zwass, V., (1996). "Electronic commerce: Structure and issues." *International Journal of Electronic Commerce*, 1(1), 3-23.

Websites

- [15] E-Commerce Guide.Com
- [16] E-Commerce Times
- [17] www.business.com
- [18] www.imwire.com
- [19] www.statista.com