Security To E-commerce Transactions Using Aadhar

[1]Pallavi Kosare, [2]Vidya Atre, [3]Monika Dahat, [4]Utkarsha Bhose, [5] Sugandha Satija
[1]Final year Student, [2] Final year Student, [3] Final year Student, [4] Final year Student, [5]Assistant Professor
[1]Information Technology,
[1]Kavikulguru Institute of Technology and Science Ramtek, Nagpur, India

Abstract: "Security to E-commerce transactions using Aadhaar" is a web based application. It is an Aadhaar Enabled Payment System. This payment system empowering an online transactions for buying any products from online shopping sites. This payment system is used by the online customer. Online user uses his/her aadhaar as identity to access his/her respective aadhaar enabled bank account and perform basic banking transactions for buying online products. It is developed to build the foundation for a full range of aadhaar enabled banking services for online shopping.

Keywords: *E-commerce site, secure Transactions, Aadhar card.*

I. INTRODUCTION

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area of application. Design is the first step in the development phase for any engineered product or system. The designer's goal is to produce a model or representation of an entity that will later be built. Beginning, once system requirement have been specified and analyzed, system design is the first of the three technical activities -design, code and test that is required to build and verify software. The importance can be stated with a single word "Quality". Design is the place where quality is fostered in software development. Design provides us with representations of software that can assess for quality. Design is the only way that we can accurately translate a customer's view into a finished software product or system. Software design serves as a foundation for all the software engineering steps that follow. Without a strong design we risk building an unstable system one that will be difficult to test, one whose quality cannot be assessed until the last stage. Advance technology has brought a lot of innovation and improvement to this sector and still there is scope for lot of advancement. Thus, "" is an important social need of today. Due to rapidly increase number of e-commerce transaction online day by day. In India "Aadhaar Number" is the best way to perform all activities in country through "One Identity".

Impact on Customers: With the existence of e-commerce, it brings convenience for customers as they do not have to leave home and only need to browse website online, especially for buying the products which are not sold in nearby shops. It could help customers buy wider range of products and save customers' time. Then, the online shopping often provides sales promotion or discounts code, thus it is more price effective for customers. Moreover, e-commerce provides products' detailed information, even the in-store staff cannot offer such detailed explanation. Customers can also review and track the order history online. However, e-commerce is lack of human interaction for customers, especially who prefer face-to-face consumption. When the customer regrets to purchase the product, it involves returning goods and refunding process. This process is inconvenient as customers need to pack and post the goods. If the products are expensive, large or fragile, it refers to safety issues.

Security: E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex Endeavour due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce in e-commerce B2C and C2C websites from both customer and organizational:

a) Purpose Of Security-

1. Data Confidentiality – is provided by encryption decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.

3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase

b) Security Issues-

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system.

Security features have four categories:

· Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.

· Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.

· Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.

· Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.

· Integrity: prevention against unauthorized data modification

· Nonrepudiation: prevention against any one party from reneging on an agreement after the fact

· Availability: prevention against data delays or removal.

c) E-Commerce Security Tools-

· Firewalls – Software and Hardware
· Public Key infrastructure
· Encryption software
· Digital certificates
· Digital Signatures
· Biometrics – retinal scan, fingerprints, voice etc
· Passwords
· Locks and bars – network operations centers

d) Security Threats-

· Three types of security threats

1. Security (DOS): Denial of Service (DOS) : Two primary types of DOS attacks: spamming and viruses

Spamming:

Sending unsolicited commercial emails to individuals. E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target. DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target

Viruses:

self-replicating computer programs designed to perform unwanted events. There are specially two types of viruses namely Worms and Trojan horses. Worms: special viruses that spread using direct Internet connections.

Trojan Horses: disguised as legitimate software and trick users into running the program

2. Security (unauthorized access):

Illegal access to systems, applications or data. Passive unauthorized access listening to communications channel for finding secrets. It May use content for damaging purposes. Active unauthorized access. Modifying system or data. Message stream modification. Changes intent of messages, e.g., to abort or delay a negotiation on a contract. Masquerading or spoofing –sending a message that appears to be from someone else. Impersonating another user at the name (changing the ―From‖ field) or IP levels (changing the source and/or destination IP address of packets in the network) Sniffers–software that illegally access data traversing across the network.

3. Software and operating systems,, security holes Security (theft and fraud):

Data theft already discussed under the unauthorized access section. Fraud occurs when the stolen data is used or modified. Theft of software via illegal copying from company servers. Theft of hardware, specifically laptops.

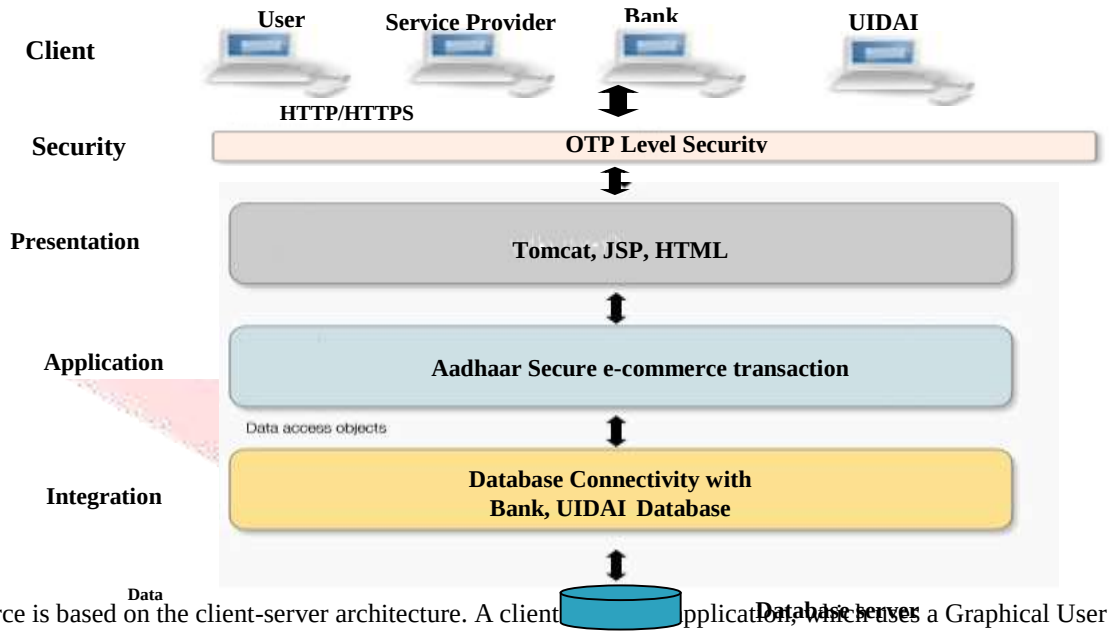
II. Related Works

In [1], Electronic commerce, commonly known as e-commerce is trade in products using the internet. The main concern in online shopping is secure. Security at the e-commerce becomes more and more important. In this proposed paper, improve the secure electronic transaction by using biometric identification payment system. For security purpose use of AES and stenography. By this encryption and decryption time reduced with the adoption of multithreading. The graph shows the comparison between base paper and the proposed paper in terms of time.

In [2], "Directions for web and e-commerce security" This paper has described direction for web and ecommerce security. We believe that the main building blocks for secure e-commerce and web applications are the following: Tools and mechanisms supporting the specification of access control policies suitable for the ecommerce, Environment Secure federations of collaborating organizations, Secure Workflow Management Systems.

In [3],This paper presents a new secure hash algorithm based on static structure algorithm called Secure Hash Algorithm (SHA-192).It can provide many choices for practical applications with different level of enhanced security to resist the advanced SHA attacks such as pre-image, second pre-image and collision attacks. The security analysis of SHA-192 is compared to old SHA-1 and it gives enhanced security and excellent results. The proposed SHA-192 hashing algorithm has been observed to be better than the already existing SHA-1 hashing algorithm in terms of the number of brute force attacks needed to break it and moreover it is fast when compared to the other secure hash algorithms. The proposed method has advantage of portability on mobile devices, which are currently embed Security enhancement of proposed system is more than the existing one but there the time delay is more since it generate 192bits of message digest.

III. Proposed Methodology



E-commerce is based on the client-server architecture. A client application, which uses a Graphical User Interface (GUI) that sends request to a server for certain services. The server is the provider of the services requested by the client. In E-commerce, a client refers to a customer who requests for certain services and the server refers to the business application through which the services are provided. The business application that provides services is deployed on a Web' server. The E - Commerce Web server is a computer program that provides services to "other computer programs and serves requested Hyper Text Mark-up Language (HTML) pages or files. In client-server architecture, a machine can be both a client as well as a server.

IV. Implementation Details:

For the implementation of this project the following modules required for develop the project. The implementation of the project modules are mentioned below:

- **User Registration:** This module allows the user to register using unique identity. The citizen provides his personal information.
- **Login & Security:** This module allows only authorized users to use the application.
- **Process & Transactions using Unique Identity:** This module use unique identification number for each online transaction.

- **OTP Service Integration:** This module is used to send the otp for transactions using aadhaar number of the user.
- **Verification Module:** This module is used for verification of the users to use the application.
- **Database Connectivity & Designing :** This module is used for designed back-end structure of application

V. CONCLUSION

The final aim of project is this system develop for care of security during online shopping for transactions with features like efficient and less time consuming. This project will help us in gaining valuable information and practical knowledge on several topics like designing web pages using html, css, java, databases & web server. This project has given us great satisfaction in having designed an application which can be implemented for any online shopping and buy various kinds of products online by using simple technique i.e. aeps (aadhaar enabled payment system using otp through aadhaar number of user).

VI. ACKNOWLEDGMENT

We express our special thanks to Mrs. Saroj A Shambharkar, Head of Information Technology department, for her kind support and allowing us to use all the facilities that are available in the department during this project. Our sincere thanks to Dr. B Ram Ratanlal, Principal, KITS Ramtek for extending all the possible help and allowing us to use all the resources that is available in the institute.

REFERENCES

[1] Thulasimani Lakshmanan and Madheswaran Muthusamy, "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes" The International Arab Journal of Information Technology, Vol. 9, No. 3,2012.

[2] Dr. Nada M. A. Al-Slamy, "E-commerce security" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, 2008.

[3] Rhavani Chris Clifton, "Directions for Web and E-commerce Applications Security" IEEE, ISSN 0-7695-1269-0101 1- 2001, 2001

[4] Yu Xin, Xia Ming Ping &Bai Yu, "Research on the Security Model for E-business Process Management," Published in IEEE computer society 2008, pp.369-371.