

## Survey on E-commerce web application & login security

Pooja K. Pinjare, Shradha D. Labhshetwar ,Gauri D. Jagtap, Kirti S.Kulkarni

Under the Guidance of MS. Renuka Kajale

Student, Computer Department,PES Modern College Of Engineering , Pune

**Abstract-**The e-commerce provides the number of services for buying and selling products online, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. MD5 (Message Digest Version-5) algorithm is an encryption algorithm for providing security for password authentication. MD5 algorithm depart password into number and character form, then number is respectively added 1,2,3, , at the meantime, the character is added 1 in ASCII, by encryption combination of numbers and characters form the final password.

**Keywords:**E-Commerce, E-Services, Improved MD5

### I. Introduction:

Now-a-days internet evolution changes the business model from traditional market to electronic commerce/market or calls it as E-commerce. Commonly known as Electronic Marketing. E-commerce is a transaction of buying or selling online e-commerce is the new way of how business meets the customer via online and using technology as critical component that supports the commerce.

In various applications of e-commerce are continually affecting trends and prospects for business over the internet, including e-banking, e-tailing and online publishing/retailing. Today's world companies use e-commerce to support the marketing strategy as an effective tool to find their new customer.

There are so many benefits of E-commerce some them like expanded customer base and geographical reach, increase visibility through search engine marketing, provide customers information about your business, collection of customer data and reduction of marketing and advertising costs etc.

E-commerce is formed of three high levels:

1. **Infrastructure:** Consisting of network infrastructure, application platform and communicating devices.
2. **Services:** is a facility in supporting the customer to make decision making process.
3. **E-commerce products and structures:** consisting of product content, packaging, distribution, price and value network

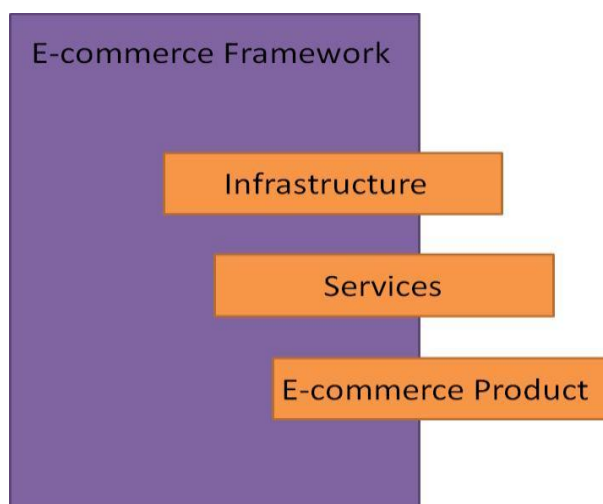


Fig-1: E-commerce Framework

In current E-commerce world the security of network communication has gradually become a research hotspot in which the key research problem is how to ensure the safety of the transmission data and stored data. There are many algorithms which applied to E-commerce system for security purpose. One of the mostly implemented algorithm is improved MD5 in E-commerce. By using MD5 algorithm for password encryption we can secure our system.

## **II. Literature review:**

Ratna sari. Cadelina Cassandra[2] has proposed MD5(message digest algorithm)is widely used in login authentication module in which password is encrypted by MD5 algorithm. The login process is to compare the encrypted password value and the password stored in database which is no longer the original password match or not. Because traditional MD5 algorithm cannot be very good against the collision attack, differential attack and dictionary attack.

And also has proposed E-commerce is being an important aspect in business that changes the business model from traditional market to electronic market. The purpose of this paper is to identify and learn how the companies build the application infrastructure to support e-Services satisfactory and build trusty commerce site. And as the result, a well-designed application infrastructure is provided for the e-commerce firm to adopt in order to achieve the satisfaction of e-service.

Yanmin Cheng ,Baotian Dong has explain about the campus e-commerce and demonstrates the campus e-commerce technology, economics and policy feasibility. The construction process of campus e-commerce system is studied in detail in this paper. Next, we concretely analyse the functional requirements of the

campus e-commerce system .It provide design and analysis of e-commerce functionality like Online payment system services, online shopping mall, travel service, second-hand commodity trading platform.

Priyanka Ora,Dr.P.R.Pal[]describe With the continuous advancement in technical field many technologies are evolving day by day, cloud computing is one of them. With the help of cloud computing user can easily share, store and retrieve their data from anywhere. Cloud computing provides hardware, software and infrastructural storage to many users at a time,It provides the security for the file reading present on cloud. No any stranger can able to see the file, only the intended person will able to see file using private key encryption. Keonwoo Kim, Un Sung Kyong[] has explain. In this paper, the optimized MD5 function for the password recovery of an encrypted PDF file. The cracking performance was improved by reducing the quantity of instructions to be executed during the hashing operation in the recovery process.

Xeoling Xeng.2. Jidong Jind. Describe The MD5 algorithm has resolved the transmission and storage by form of plain code and other security problems in traditional password though; it is also threatened by the collision attack and dictionary attack. It needs more secure methods. This has analysed the application of MD5 algorithm and security in the password authentication. It encrypt the contents of user password info and stores the encrypted password in database.

## **III. Improved MD5:**

We all know the MD-5 algorithm. We can understand that MD-5 algorithm uses one way encryption algorithm, this algorithm has two important characteristics, First is arbitrary at both ends of text encryption not be same; second is any section of text encryption is always same. So both ends of text cannot get encrypted with same text encryption. In other words, as original data & MD-5 encrypted value of premise to find with same MD-5 value of data is very difficult. As results, MD-5 algorithm is used in website login authentication. As we know MD-5 gets cracked in 2009 but even if attacker obtain the password is encrypted & attacker won't get the real password set by users. We know that MD-5 algorithm was still get used for login authentication. After some improvement the novel algorithm based on MD-5 get implemented, Flow chart shown in figure-2

**Flowchart:**

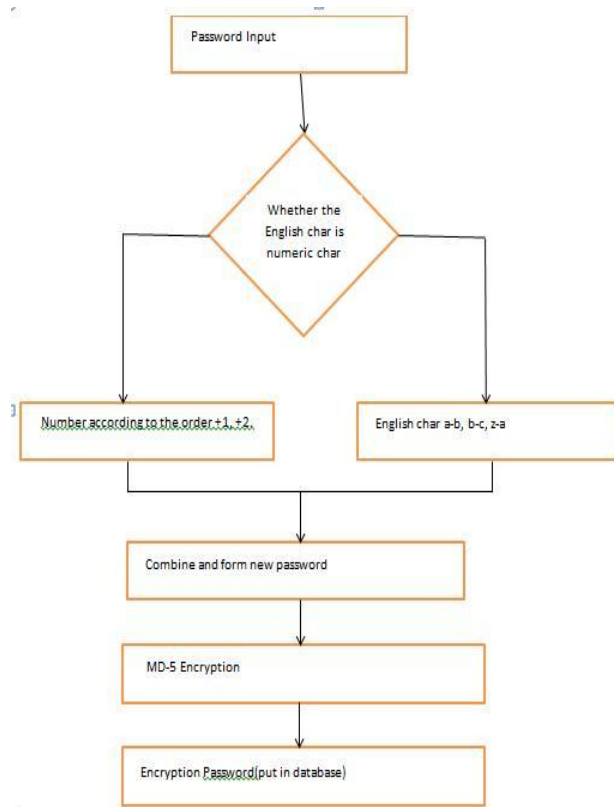


Figure-2: Improved MD5 Algorithm

Steps are as follows: Step1: Blocking Password

When user will enter password while registering, the spring MVC controller will get the password.

Step2: Processing digits After block processing the digital part, according to the order of occurrence, complete +1, +2, +3, ..... operations.  $n = (n+i) \bmod 10$

Step3: Processing character

The following transformation is performed for each character in the English character block i.e. a->b, b->c, ..., z->a, A->B, B->C, ..., Z->A. the encryption can be represented using modular arithmetic by first transforming letters in numbers.

Step4: MD-5 Encryption

The combination of number and character are used as input password which will be encrypted by MD-5 algorithm.

#### IV.E-Commerce:

As we know that e-commerce is biggest trend among now a days people to buy goods from internet. E-commerce system is mostly used by internet to do sale of products. E-commerce has made a global market place for business and customers to make trading and transaction all over the world. Research shows that e-commerce system is not only about trend but also can build with many benefits. E-commerce mainly has potential like cost reduction, wider accessibility, flexibility, transparency, easy to access, better decisions.

The below diagram shows the Ecommerce frame work.

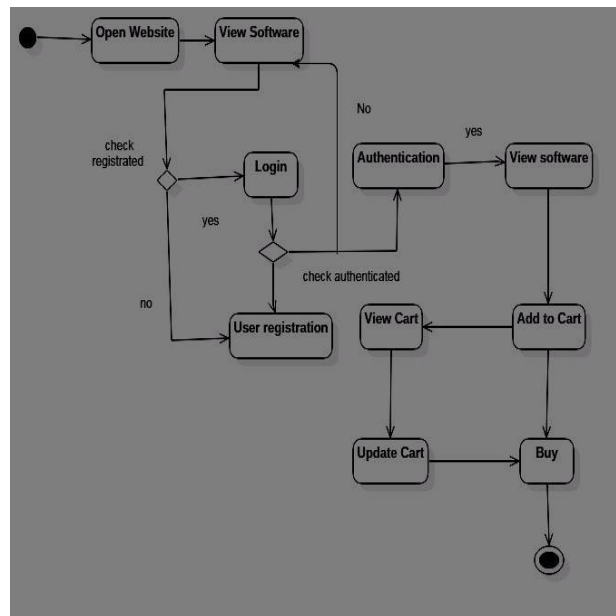


Figure-3: E-commerce System

### Conclusion:

After observing the e-commerce application infrastructure that was developed by the company, so it can conclude with nowadays implemented e-commerce application infrastructure must compete and follow with growth technology. Since customer was handle via online, company needs to support excellent e-services through stable and adequate of application. As per the previous add to cart process we add another specification which is e-mail notification which provides information about products in the cart.

### References:

- [1] Yanmin Cheng, Baotian Dong(s), Analysis and Design of Campus E-commerce System, in School of Traffic and Transportation- Beijing Jiaotong University Beijing, China , Year 2016.
- [2] Ratna Sari, Cadelina Cassandra, Build e-Services Satisfactory Through e-Commerce Application Infrastructure (A Case Study Approach), 2016 International Conference on Information Management and Technology.
- [3] Xiaoling Zheng, Jidong Jin, Research for the Application and Safety of MD5 Algorithm in Password Authentication,9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012),2012.
- [4]Ratna sari,Cadelina Cassandra,java web Login Authentication based on improved MD5 algorithm.(2016)