An Improvement of Scalability and Security in E-Commerce Application Using Bcrypt Encryption Algorithm

[1]K.V.K.SASIKANTH, [2]K.SAI PRASANNA LAKSHMI, [3]K. RAVI TEJA, [4]G. KEERTHI SRESTA, [5]P.SAI SRI RAMULU
[1]Assistant Professor, [2,3,4,5]UG Student, Department of Computer Science and Engineering,
Godavari Institute of Engineering & Technology, Rajahmundry, AP

ABSTRACT: E-commerce is a type of business model that focuses on doing commercial transactions through electronic networks like the web. Most of the company sales come through the popular e-commerce web site that has a very effective search engine ranking, however scalability and security are being major issues in present E-commerce. We implemented an e-commerce web site to cope with the issues related to scalability and security. In particular our top priority in this re-engineering effort are performance and user experience. This paper is proposes to launch a new e-commerce application as part of this re-engineering effort by retaining the existing interface of the current application that is being used to manage product catalogue and inventory are works fine for now and we will continue to use it with the new customer-facing application. The new application should integrate well with existing database. However, if the database design of the existing application imposes a negative impact on new application performance, it is good to duplicate this data in the new application database. The proposed work provides high security to the user's personal data using BCrypt encryption algorithm to enhance the security level of system.

Keywords: E-commerce, issues in Scalability, Security, Proposed Architecture, Bcrypt Encryption,

I.INTRODUCTION

E-commerce stands for ELECTRONIC COMMERCE. E-commerce is quick gaining ground as an accepted and used business paradigm. More and more business houses are implementing web sites providing functionality for performing commercial transactions over the web. It is affordable to mention that the process of shopping on the web is becoming common place.

The objective of this paper is to develop a general purpose e-commerce store where ever any reasonably product is often bought from the comfort of home through the Internet. However, for implementation purposes, this project will deal with online shopping for women's clothing. An online store is a virtual store on the Internet where customers can browse the catalogue and select products of interest. The selected things may be collected in a shopping cart. At checkout , the items in the shopping cart will be presented as an order. At that point, more information will be needed to complete the transaction. Usually, the customer will be asked to fill or select a billing address, a shipping address, a shipping option, and payment information such as Cash on Delivery or Online Payment.

With increasing demand for online purchasing, more and more businesses are moving to e-store from brick and mortar stores. In the US, more than 60% of individuals are buying goods online from the comfort of their home and this figure is increasing perpetually. By considering this percentage, we are able to say that e-commerce is increasing tremendously because of its complete range of benefits that any industry vertical can enjoy.

Today, e-Commerce has revolutionized the approach in which the companies are doing business. Now, consumers can buy almost anything online 24*7 a day and get an ultimate shopping experience. For many individuals within the world, e-Commerce becomes one of the preferred ways of shopping as they enjoy their online shopping because of its easiness and convenience. They are allowed to buy products or services from their house at any time of day or night.

One of the most foremost necessary advantages is that ecommerce merchants can enjoy is store timings are currently 24/7/365 as they can run e-commerce websites all the time. By this approach, they can increase their sales by boosting their number of orders. However, it is also beneficial for consumers as they can purchase products whenever they need regardless of whether or not it's early morning or mid-night.

II. LITERATURE REVIEW

According to [2]accomplishing the shopping trip at the earliest opportunity refers to the time-saving oriented shoppers and that they like store selections favouring active shopping people who don't love shopping and approaching for time saving retail stores refers to the economic shoppers or also known as "problem-solvers".

As stated by [2] it requires less effort and better decision making for consumers who opt to purchase at the e-store. Shoppers might save their time in e-shopping because they do not have to undergo any effort on travelling to a mall or saving their time in other psychological factors such as traffic jam etc

Online shopping increases search efficiency by eliminating travelling charges and psychological prices brings convenience in e-shopping Comparing online and traditional shopping [1].This statement is given by [5] found that internet shopping was viewed as saving more time.

According to [5] the main drive of online shopping is that the internet is time saving and accessible 24 hours a day. Shopping in the internet saves time and effort because consumers are able to shop any time in the comfort of their home; especially for consumers who have little amount of free time because of extended working hours.

Online payment is a form of electronic payment, which is provided by a third party payment interface between banks for real-time payment. Compared with the traditional payment, online payment systems are more convenient, fast, efficient and economical. Users will use their own computers or mobile phone with Internet to complete the whole payment method in a very short time.

As stated by [2] it describes about the blind decoding schemes are proposed as tools for protecting customers' privacy in on-line shopping for electronic documents such that the company has no means of knowing that documents the consumers have purchased. Most of the blind decoding schemes suffer from the oracle drawback. Schemes utilizing the transformability of digital signatures were planned to ensure the correctness of the requests from the customers. In this paper, a secure blind decoding scheme is proposed based on RSA scheme . It doesn't utilize the transformability of RSA digital signature.

Niels Provos and David Mazeries, proposes ways that of building systems during which secret security keeps up with hardware speeds. We formalize the properties desired in an efficient password system and show that the computational price of any secure password theme should increase as hardware improves. We present two algorithms with variable costeksblowsh a block cipher with a purposefully expensive key schedule and bcrypt a related hash function. Failing a significant breakthrough in complexity theory these algorithms should be able allow password based systems to adapt to hardware enhancements and stay secure well into the future [3].

The Existing system has following problems:

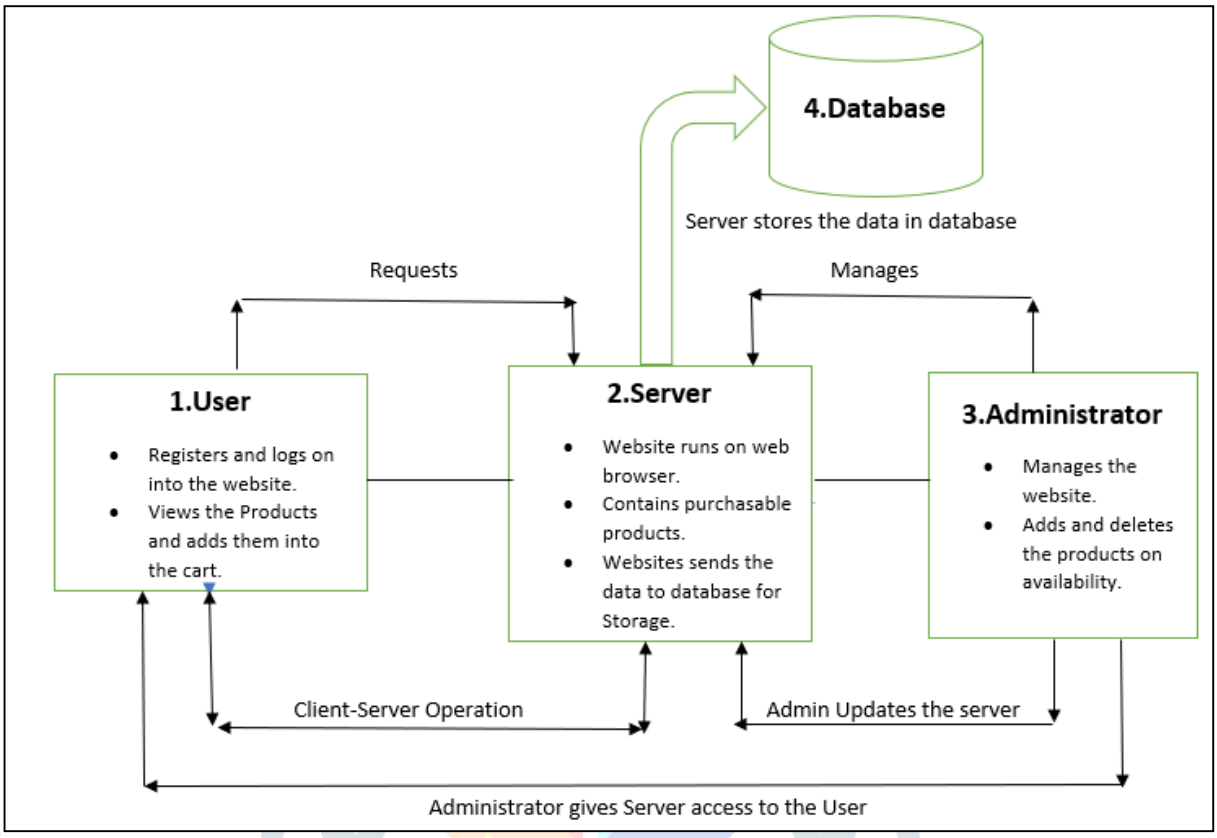
a) Many users are facing problems while loading a website during the offer period which leads to scalability issues.
b) Due to scalability issues, the number of users will decrease in time.
c) In existing system, users passwords will be decrypted very easily which leads to less security.
d) Most of the user's accounts are being hacked due to less security for the user's personal information.

To overcome the existing problems the proposed system is:

a) In this proposed system the website scalability was increased by using Tomcat server which reduces scalability issues.
b) For fast accessing of the website we are using Tomcat server which increases the number of customers day by day.
c) To overcome security problems regarding password we use BCrypt algorithm which provides high encryption facility. By this algorithm intruders will be unable to decrypt the password and misuse user's personal information.
d) By using BCrypt algorithm user's personal information can be secured.

III. PROPOSED ARCHITECTURE

The following figure shows the system architecture of the website. The figure depicts the client-server architecture where user send request to the server and then server responds to the user's request. Admin manages the website by making changes in the website by adding or deleting the products. user's personal information will be stored in the database.



2

IV. BCRYPT ALGORITHM:

Bcrypt is a hashing algorithm which is scalable with hardware (via a configurable number of rounds). Its slowness and multiple rounds ensures that an attacker must deploy massive funds and hardware to be able to crack your passwords. Add to that per-password salts (bcrypt requires salts) and you can be sure that an attack is virtually unfeasible without either ludicrous amount of funds or hardware.

Bcrypt uses the Eksblowfish algorithm to hash passwords. While the encryption phase of Eksblowfish and Blowfish are exactly the same, the key schedule phase of Eksblowfish ensures that any subsequent state depends on both salt and key (user password), and no state can be pre computed without the knowledge of both. Because of this key difference, bcrypt is a one-way hashing algorithm. You cannot retrieve the plain text password without already knowing the salt, rounds and key (password).

```
bcrypt(cost, salt, pwd)
state←EksBlowFishSetup(cost, salt, key)
ctext←"OrpheanBeholderScryDoubt"
repeat(64)
ctext←EncryptECB(state, ctext)
return Concatenate(cost, salt, ctext)
```

In the first phase, *EksBlowfish Setup* is called with the cost, the salt, and the password, to initialize *eksblowfish*'s state. Most of bcrypt's time is spent in the expensive key schedule. Following that, the 192-bit value ``OrpheanBeholderScryDoubt'' is encrypted 64 times using *eksblowfish* in ECB mode with the state from the previous phase. The output is the cost and 128-bit salt concatenated with the result of the encryption loop.

V. CONCLUSION

E-commerce business has bloomed over years and is one of the quickest developing areas in the online world. Though it took some time for this to be accepted by the end users, today we are at a point where majority of the people love to shop online. There were various concerns revolving around online shopping at its dispatch, however over years, people started to trust E-commerce for all their shopping needs.

There is an immense acceptance of e-commerce in world due to the internet facilities available. The countries such as India, Brazil, and China etc which are on the path of development are using e-commerce for carry out various transactions. The e-commerce can exceed geographical limits and can prove to be reliable by reaching to customers. Experiences in increasing the demand for broadband services, rising standards of living, convenience of wider product ranges, reduced prices and busy lifestyles reveal this truth a lot of conspicuously thereby giving an approach to online deals on gift vouchers. This meets electronic orders and will be in touch with the customers all the time. Therefore, E-Commerce is a good opportunity.

VI. REFERENCES

[1]. Anil Khurana," Prospect of E-Commerce: M-Commerce", International Journal of Advance Research in Computer Science and Management Studies [5] , Issue 2,2017 February , P No: 13-17

[2] Y.C. Chen, G. Horng and C.C. Huang,"Privacy protection in on-line shopping for electronic documents",5th International Conference on Information Assurance and Security[2],Issue 2009, P No: 105–108.

[3] Niels Provos and David Mazeries, "A future – adaptable Password Scheme", Proceedings of the FREENIX Track USENIX Annual Technical Conference, Issue 1999 P No:6-11.

[4] P. Sriramya and R. A. Karthika, "PROVIDING PASSWORD SECURITY BY SALTED PASSWORD HASHING USING BCRYPT ALGORITHM",ARPN Journal of Engineering and Applied Sciences[10] ,Issue 13,2015 JULY , P No: 1819-6608

[5]. https://www.ukessays.com/essays/information-technology/e-business.php

[6].https://medium.com/@danboterhoven/why-you-should-use-bcrypt-to-hash-passwords-af330100b861

[7]. https://www.quora.com/What-is-the-function-of-Apache-Tomcat-and-how-do-I-use-it

[8]. https://www.quora.com/What-is-the-greatest-advantage-of-using-Tomcat-over-other-servers

[6] Abu Bakar, F. & Osman, S. (2005), 'TOWARDS THE FUTURE OF MOBILE COMMERCE (M-COMMERCE) IN MALAYSIA', Proceeding of IADIS: IADIS international conference web based communities, Algeria, Portugal

[7] Felicita J & Gnana Jayanthi J. (2013), 'MOBILE COMMERCE: THE NEXT DRIVER OF MARKET GROWTH', Elixir international Journal, Arts 56A, pp 13607-13612

[8] Feng H., Hoegler, T. & Stucky, W. (2006), 'EXPLORING THE CRITICAL SUCCESS FACTOR FOR MOBILE COMMERCE', Proceedings of International Conference on Mobile Business, Copenhagen, Denmark

[9] Jain N, Dixit K., (2014), How Multi Screen Consumption is Altering Online Behaviour, Business World, Sept. 19, 2014 can be http://businessworld.in/news/economy/how-multi-screen-consumption-is-altering-online-behaviour/1538145/page-1.html#sthash.bTlL23Ge.dpuf

[10] Paavilainen J., (2002), 'MOBILE BUSINESS STRATEGIES: UNDERSTANDING THE TECHNOLOGY & OPPORTUNITIES', Addison Wesley

[11] Sachin Gupta & Anand Vyas (2014), 'BENEFITS AND DRAWBACKS OF M-COMMERCE IN INDIA: A review', International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4

[12] Sandhu 2012, 'MOBILE COMMERCE: BEYOND E-COMMERCE', International Journal of Computer Science and Technology, Vol. 3, Issue 1, March 2012 pp 759-763

[13] Singh Shelly (2014), COMPANIES DEVISE NEW STRATEGIES TO KEEP PACE WITH RAPID RISE OF MOBILE COMMERCE, Economic Times, Oct. 21, 2014.

ACKNOWLEDGEMENT

We have great pleasure in expressing our gratitude to Sri K.V.V.Satyanarayana Raju, Founder & Chairman, Chaitanya Group of Institutions, Sri K. Sasi Kiran Varma, Vice Chairman, GIET Group of Institutions, Smt. Lakshmi Raju Executive Director, GIET, for their kind support in providing us an opportunity to do research in this college.