ISSN 2319 - 5975

Volume 13, No.1, December 2023 – January 2024

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns061312024.pdf

https://doi.org/10.30534/ijns/2024/061312024

# Review On E-Commerce Application with Leveraged Cryptosystems and Big Data

**Adarsh Suresh Ajila, Shaswat Shetty, Shivaprasad H S, Mr. H Harshavardhan**

CSE, Alva's Institute of Engineering and Technology, Mangalore, India, adarshajila1307@gmail.com

CSE, Alva's Institute of Engineering and Technology, Mangalore, India, shaswatshetty488@gmail.com

CSE, Alva's Institute of Engineering and Technology, Mangalore, India, shivaprasad110420@gmail.com

CSE, Alva's Institute of Engineering and Technology, Mangalore, India, harshavardhan@aiet.org.in

Received Date : November 18, 2023 Accepted Date : December 16, 2023 Published Date : January 07, 2024

**ABSTRACT**

The fast improvements in technology and the growing desire for safe and easy online purchasing have caused a dramatic shift in the e-commerce market in recent years. The merging of big data analysis and encryption, two potent instruments that are transforming how companies run and customers interact in the digital marketplace, is at the core of this change. In e-commerce applications, cryptography, the study of secure communication, is essential for maintaining transaction integrity, protecting user privacy, and securing sensitive data. Businesses may optimize pricing strategies, improve auction efficiency, and obtain important consumer insights by practicing big data analysis, which is the art of gleaning insights from large volumes of bidding data. This in-depth analysis explores the diverse applications of big data analysis and cryptography in the e-commerce industry, delving into their complex worlds. We look at the underlying ideas behind these technologies, the range of applications they can be used for, and how they affect the entire e-commerce ecosystem.

**Key words:** Cross-border, data process, legacy, Blockchain, Attack detection model.

## 1. INTRODUCTION

The e-commerce industry is thriving because the introduction of the internet completely changed how we conduct business. This international phenomenon has completely changed the way business's function, giving them the ability to access a larger customer base and offer flawless online purchasing experiences to customers all over the world. But as e-commerce has expanded, it has also presented new difficulties, namely with regard to guaranteeing the effectiveness and security of online transactions.

The manner that consumers and organizations do business has changed dramatically as a result of the explosive expansion of e-commerce. Alongside this expansion, there has been a rise in the demand for effective and safe e-commerce solutions. In order to meet these demands, big data analysis and cryptography are essential.

Big data analysis and cryptography have become crucial instruments for overcoming these obstacles and advancing e-commerce. Big data analysis delivers insightful information on customer behavior and market trends, while cryptography offers a strong basis for secure communication and data security.

## 2. THE DEVELOPMENT OF CROSS-BORDER APPLICATION

Cross-border e-commerce application is an activity in which the transaction is proceeding through electronic transaction platforms accomplished by delivering commodities through logistic service among the dealers [1].

As one of the Backbones of international trade, the logistics industries worldwide was over 8.4 trillion euros in 2021 and is expected to be 13.7 billion euros by 2027. Parallel to this the global total logistics costs soared to 9 trillion U S dollars in 2020, by this there is still room for the development of cross-border import.

Cross-border e-commerce has 6 characteristics including global, invisible, anonymous, instantaneous, paperless and evolves [1].

## 3. THE PROCEDURE OF APPLYING BIG DATA INTO MARKETING OF E-COMMERCE

The application of big data to marketing of E-commerce are divided into four procedures [4]

### 3.1 Data Collection

Firstly, data collection plays a major and important part in data processing. In the model of B2C e-commerce enterprises, the usefulness of data, whether and where to collect should be confirmed in this stage other irrelevant data such as work, age and gender of the uses will become key elements for the successful and accurate implementation of market model [5].

Therefore, the legacy model of data collection cannot meet the characteristics of Internet era.

### 3.2 Data processing and Integration

This part of data processing is to sort out all the redundant values and useless values and to screen effective information based on the requirement of marketing from the huge amount of information.

The large amount of data should further screen, reduce noise, and sorted. The way of processing and screening the data will determine the usefulness of data, therefore this step is of great importance in data processing.

### 3.3 Data Analysis

This is the core part of e-commerce as well as big data, the value of data in accurate marketing can be understood from analysis. Take an example of Udemy.com, initially the main motto of this platform is to prove On-Line Courses and at the end of each course upon hundred percent completion he/she can get a verified certificate.

This made less efficient in terms of Business so they taught of more efficient model that is Black Friday which is held twice or thrice in a month where the courses are available at lower price and he/she is able to purchase courses and do their certification.

## 4. INTERPRETATION AND APPLICATION OF DATA

Data Interpretation is also one of the main areas in whole data analysis procedure. For the accurate marketing

### 4.1 Data Interpretation

Data is very humongous and it keeps changing very quickly. Its analysis result is more complex, the legacy way of displaying data is inefficient and inappropriate, so most of the company uses a method called “Data Visualization technology”. Through the application of this technology the user as well as company can easily understand trends in a visualized way.

### 4.2 Data Interpretation

Information obtained by interpreting data can be used in the specific marketing of cross-border e-commerce application, this involves 3 stages [1][6].

The first stage of drawing portrait of the user through the grasped information.

The second stage is to keep perfecting the users’ information in the process of drawing the portrait and form well-connected network.

The third state is that to make the different sales strategies regarding the personalized needs of the users [6][7].

## 5. CRYPTOGRAPHY: THE GUARDIAN OF E-COMMERCE SECURITY

Security is critical in the dynamic and always changing world of e-commerce. Because so much sensitive data is transmitted online including credit card numbers, customer addresses, and personal information—both customers and companies need to feel secure knowing that their data is shielded from abuse, illegal access, and breaches. This is where cryptography intervenes, serving as a watchful defender to preserve the secrecy and integrity of data in the context of e-commerce.

The discipline of secure communication, known as cryptography, uses a broad range of advanced strategies to safeguard private data in the digital sphere. It acts as a trustworthy middleman, keeping private information safe from prying eyes and guaranteeing that only authorized parties can access and decode data.

The Pillars of Cryptographic Security are:

### 5.1 Confidentiality

Keeping data private and making sure that only people with permission may access and decode it.

### 5.2 Integrity

Preventing unwanted changes to data is order to maintain its validity and prevent any alterations.

### 5.3 Non-Repudiation

Supplying evidence of a message's origin so the sender is unable to refute it.

## 6. METHODOLOGY

Blockchain is one of the encouraging and disruptive emerging technology used in the field cryptography. It protects the data from damaging and preserves track of transaction [3].

Figure 1 shows transaction processing system is proposed which uses a blockchain technology, zero-knowledge proof (ZKP) and modified elliptic curve cryptography (MECC) encryption method [3]. Also, a prototype will develop to establish the functionality of the blockchain based TPS, fraud prevention and continuous monitoring. First, the blockchain technology is processed. A method sharing the database among the participants is provided by the blockchain technology even if they do not trust each other. On the basis of peer-to-peer network it generates a marketplace to transfer assets without a central authority. Then the zero-knowledge proof method is processed, based on this only a Blockchain based TPS (Bb-TPS) is treated and demonstrates its functionalities of continuous monitoring, accounting, and permission management in the real time applications. The ZKP is also known as cryptographic method, here one user can show to other user that the first transaction is authentic one without showing any sensitive data [3].

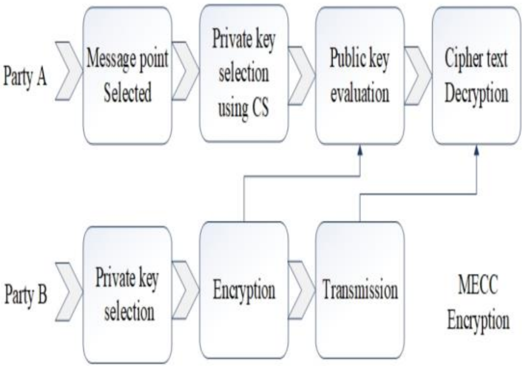

**Figure 1:** Blockchain based Transaction Processing System

By modifying the elliptic curve cryptosystems used to encrypt the data by using the optimization method cuckoo search (CS) algorithm. Private key and public key are the two keys used in ECC. The CS algorithm in ECC is used to optimize the private key.

The confidentiality and security of Bb-TPS is improved by configure the ZKP and MECC encryption also the performance is evaluated. As ECC is used instead of other cryptography mechanism it provides the benefits of less storage requirement, fast computation and high security level with less key size. While Implementing ECC various elliptic curve are available with different specifications and different speed of operation [8].

## 7. ATTACK DETECTION MODEL

The proposed attack detection model includes the detection and mitigation of DoS attacks. In this paper design of a technique for detection of DoS attack is proposed. The proposed techniques perform the task of DoS attack detection through authentication and authorization techniques.

Figure 2 below shows the proposed DoS attack detection model.

The first phase in proposed technique is registration phase. During the registration process user and server need to be registered under authorization center (AC) for the authentication. After the authentication of user and the server is over, the authorization mechanism will be performed to mitigate the DoS attack during the E-commerce transactions. Here, the user behavior will be recorded based on several parameters, in the web log file. Then, the important features will be extracted from the web log file during the feature extraction process. Once the features are extracted, it will be fed as input to the proposed model of DoS attack detection which uses the Glowworm Swarm Optimization based Support Vector Neural Network (GSO-SVNN). The implementation of proposed GSO-SVNN based DoS attack detection model will be done using the MATLAB with a system having windows 10 as operating system and 4 GB of RAM. The attack analysis will be performed to signify the efficiency of the proposed technique [3][9].

This section explains the results of comparative analysis of Neighbor Similarity Trust [10], QADE [11], BARTD [12], and proposed ECC+ GSO-SVNN. It describes the overall performance of the proposed method in terms of its accuracy and precision as given in equation 1 and 2.

Table 1 describes the comparative analysis of the existing and proposed methods of DoS attack detection. The accuracy attained by the existing Neighbor Similarity Trust, QADE, and BARTD is 0.908, 0.914, and 0.919. The results achieved by proposed ECC+GSO-SVNN in terms of accuracy is 0.951. From the table observation, it is clear that the proposed method shows better accuracy, precision as compared to other techniques [3].

### 7.1 Accuracy (ACC)

It refers the degree to which the result of a measurement, calculation, or specification conforms to the correct value or a standard.

$$ACC = \frac{T^P + T^N}{T^P + T^N + F^P + F^N} \qquad (1)$$

### 7.1 Precision (P)

$$P = \frac{T^P}{T^P + F^N} \qquad (2)$$

where, TP, TN, FP, FN and represent true positive, true negative, false positive, and false negative.

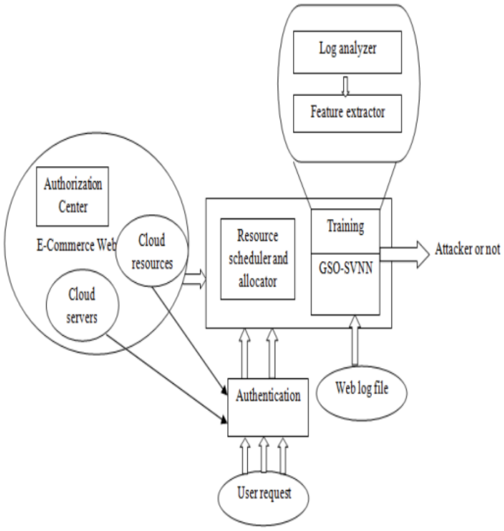

**Figure 2:** Proposed Attack Detection Model.

**Table 1:** Comparative Analysis

| Methods | Accuracy (%) | Precision (%) |
|---|---|---|
| Neighbor Similarity Trust | 90.8 | 95.4 |
| QADE | 91.4 | 96.7 |
| BARTD | 91.9 | 97.8 |
| Proposed technique | 95.1 | 98.2 |

## 8. CONCLUSION

In this Review paper, big data, cross border, accurate marketing and detailed interpretation of applying big data technology to analyses all the customer relationship with the organization as well with the application which is electrically ran on the internet along with big data providing safe and secure environment to the e-commerce application with some of the classical cryptography systems.

But there always an improvement made to any system that is instead of classical crypto systems we can go foe lightweight cryptography which require less resource of the system with the very good security.

## ACKNOWLEDGEMENT

The authors would like to express their gratitude for the support and contributions that have enriched this research endeavor. F. A. Author acknowledges the insightful work of colleagues and the valuable resources provided by Mr. H. Harshavardha. This research was made possible through the financial support received from Alvas Institute of Engineering and Technology, Mijar. The authors extend their appreciation to all those who have played a role in advancing this work.

## REFERENCES

1. Huiqun Liu, xiao Wang, **"Study on the application of Big Data in Accurate Marketing of Cross-Border E-Commerce in China"**, March 2018.
2. Akcaoglu, E., & Ozturk, C. (2017). **"A review of big data analytics in e-commerce".** International Journal of Information Management, 37(5), 663-674.
3. Javed R. Shaikh, Georgi Iliev, **"Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security"**, Nov. 2018.
4. China Electronic Commerce Research Center, **"China electronic commerce market data monitoring report 2016"**, may .2017.
5. Yang Yongbin, **"On the realization of precision marketing"**, HENAN SOCIAL SCIENCES, April. 2012, pp. 102-103.
6. Yang Chunhua, **"The application of data in B2C electronics commerce Chinese precision marketing in Jing Doing mall"**, Social forum Dec. 2007, pp. 104-107.
7. Chen Zhiyong, Lan Yun, Ke Chang, Huang Guomei, **"Research on the application pf large data technology in cross-border e-commerce"**, International Trade, Mar.2016, pp. 126-128.
8. Javed R.Shaikh, Maria Nenova, Georgi Iliev, and Zlatka Valkova Jarvis, **"Analysis of Standard Elleipic Curve for the Implementation of Elliptic Curve Cryptography in Resource Constrained E commerce Applications"**, in Proceedings of the IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) , pp. 1-4, 2017.
9. Javed R.Shaikh, **“ECC Based Authentication and Optimized Support Vector Neural Network Based Authorization for Detection of DoS Attack Detection in the E-commerce Trasactions”**, International Journal of Current Engineering and Scientific Research, Vol. 5, no. 2,pp. 47-54, 2018.
10. F. Musau, G. Wang, S. Guo, and M. B. Abdullahi, **"Neighbor similarity trust against sybil attack in p2p E-commerce"**, Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing, pp. 547-554, IEEE, 2012.
11. E. Zupancic and D. Trcek, **"QADE: a novel trust and reputation model for handling false trust values in e–commerce environments with subjectivity consideration”**, Technological and Economic Development of Economy, vol. 23, no. 1, pp. 81-110, 2017.
12. K. M. Prasad, A. R. M. Reddy, and K. V. Rao**, "BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web"**, Journal of King Saud University-Computer and Information Sciences, pp. 1-15, 2017.