Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security

Javed R. Shaikh ,Georgi Iliev
Faculty of Telecommunication Technical University of Sofia Sofia, Bulgaria
javedsheikh1987@gmail.com ,gli@tu-sofia.bg

Abstract— **In recent years, Electronic Commerce (E-commerce) applications are attracting many users and merchants to conduct their daily business online which includes payment of bills, online banking, buying tickets and purchasing goods etc. E-commerce transaction security is a major concern for E-commerce websites along with its customers. The basic requirements for any E-commerce transaction are privacy, authentication, integrity and non-repudiation. In this paper, a transaction processing system (TPS) for E-commerce by using a Blockchain technology, zero-knowledge proof and modified elliptic curve cryptography encryption is proposed. Also a denial of service attack detection model for the E-commerce system is proposed which take care of the DoS attack during E-commerce transactions.**

Keywords— Bolckchain, DoS, ECC, E-commerce

I. Introduction

As services provided by E-commerce applications are simple and cost effective, many customers are regularly using their personal computers to daily shopping. E-commerce is said to be intuitive, simple to handle and less menacing. There is an increasing trend to make E-commerce “smarter” and this is happening to add more and more automation in E-commerce activities [1] [2] [3]. With E-commerce web sites users are searching for various products over the Internet, they also order the items and make online or offline payments. Use of online business allows processing a huge number of orders with little manpower and, therefore, extends small businesses ability of to compete with giant companies [4] [5] [6].

The rapid growth of the Internet in last few years facilitated an increase in the variety of attacks such as increased unauthorized access, theft of resources, disclosure of information, corruption of information etc. Out of these many attacks one most harmful and powerful attack is the denial of service (DoS) attack. A DoS attack which is launched in distributed manner by a mechanism called Botnet through a network of controlled computers is referred as distributed denial of service attack (DDoS) attack [7] [8] 9]. In a cloud computing environment DoS attacks are prime security threat as resources are frequently shared by users. The primary goal of such attacks is to consume various resources such as central processing unit (CPU) processing space, memory, or network bandwidth so that end users/ legitimate user will not get access to these resources. This can be done by breaking network communication or denying services to the legitimate user. DDoS attacks generally block the resources used by the network services. DoS attacks are becoming significant disturbance factor on all the sites that are associated to the Internet. Some types of these attacks are easy to execute and others are more difficult to deploy [10]. DDoS attack is basically a resource overloading problem. With few keystrokes attacker can launch DDoS attacks on the victim machine.All available security solutions are not that efficient so robust mechanism is required which can provide confidentiality and integrity services along with the protection against DoS attack.

II. Related Work

The number of security mechanism are used to prevent the attacks in E-commerce system. The victim can prevent from various attacks using some sort of traditional security tools like access list, firewall, or intrusion detection system at its end [11]. With the advent of time after the launch of DoS attacks, the attackers became aware of defense mechanisms that were implemented to prevent and mitigate DoS attacks and to trace the identity of attackers [12] [13].

The available security mechanisms are security primitives, key management and secure channels, network core protocols, self-management and self-healing protocols, privacy and anonymity, Software based protection and testing. These security mechanisms are devised according to a set of security requirements [14].

Huasong Shan et al. [15], presented a application layer DDoS attack, which is known as very short intermittent DDoS (VSI-DDoS). A VSI-DDoS attacker sends a seasonal explosion request to the target system when the DoS was extreme for short time period. The goal of this was creating “Unsaturated DoS”. VSI-DDoS attacks were utilized to lower down the quality of service (QoS). Occasionally legitimate users were utilized the intolerable delays, it was finally affected the target system’s long-term business goal. In this article, percentile response time also utilized as the evaluation metric and the effectiveness of an adversary’s VSI-DDoS attacks measured.

David Beckett et al. [16] proposed the back-end system with a new sensor located inside and with this method additional database features were produced. Real-time insight into the actual database workload was utilized in this method, which was caused by the detection of DDoS attacks enabled by the user. Extraordinary database consumption resources were targeted by this attacks. Decision tree classification engine was utilized in the resource matrices and the real-time analysis is performed with them. In this method a strategy is designed for detecting application layer DDoS attacks, here large database queries were placed in the targeting resources. For an each individual, the queries were monitored, traced and also database usage profile was build. The contribution of this technique was sensing.

Chaker Abdelaziz Kerrache et al. [17] introduced a hybrid trust establishment scheme which is also known as trust-based framework for reliable data delivery (TFDD) and

978-1-5386-5201-5/18/$31.00 ©2018 IEEE

VANETs for DoS defense. The method was utilized for facing the attacks of DoS and also the trusted and reliable connections among vehicles were ensured with respect to overhead of minimal network. Modular architecture was the basics of TFDD which builds three components namely a distributed and collaborative components for the detection of fraudulent nodes, a data centric verification component for filtering malicious data and a component for the detection and prevention against DoS and DDoS attack.

DDoS attack mitigation solutions in the cloud was proposed by Gaurav Somani et al. [18]. Particularly, detailed view of mitigation mechanisms, detection, prevention, and characterization of these attacks were comprehensively surveyed. In addition to this, a comprehensive solution taxonomy of DDoS attacks solutions was presented. Finally, an effective guideline was provided for effective solution building which will be helpful for the research community while designing a defense mechanisms.

Khundrakpam Johnson Singh and Tanmay De [19], were introduced a strategy of unique characteristics of such attack and identifies the main highlighted parameters of the protocols, which was accompanying in every layer attacks. In this method, based on the input attribute set we classify the incoming packets as either normal category or attack category. The DDoS attack dataset of CAIDA, EPA-HTTP dataset were utilized to study the features of the protocols. After that the attribute sets were tested across the known statistical classifiers, which were utilized to compare the accuracy rate, sensitivity, specificity and time for classification. The experimental results were shown for the usability and viability of some of the classification algorithms.

III. MOTIVATION

Now-a-days, in terms of business E-commerce is an essential one which is able to compete in the marketplace. For commerce the privacy and security are a major concern. Unauthorized access, leakage of client information, clowning of credit card etc. are the several security concerns in E-commerce. Without the knowledge and cooperation from victim the crimes will be committed in the sense of more alarming future. Rather than plain human prudence a strong E-security is required to prevent the cyber-crime in future. Due to security and privacy problems (e.g. hacking customers' information) customers are vigilant to engage in E-commerce. Also, in terms of open network many more attacks are exist which is alarming to the customer information. For most organizations the significant security and privacy risk is the public disclosure of all transactions.

Integrity violation, access control, DoS and DDoS attack and infrastructure attacks are the some of the security threats, available over the Internet and these dangers has become digital terrorism in today's world. As security & privacy are the main issues on the Internet to develop the E-commerce. Hence, we should have some protected conditions to overcome the security problems related to all entity in E-commerce transaction, which should provide the strong protection for transaction information.

For sensitive applications like E-commerce the secure socket layer (SSL) protocol is used today and it is confidential in this respect to secure E-commerce. The major drawback of SSL protocol is the slow response time on the server and it is a primary cause of frustration for E-commerce users. The existing protocols does not meet the comprehensive security necessities of E-commerce applications, while the communication among customers and vendors wants more enhancements. Designing an appropriate authentication system is a challenging task, because of the complex nature of E-commerce applications and diverse security requirements. This protocol when used inside a closed and secure network is known as private blockchain.

IV. PROPOSED MEHODOLOGY

Blockchain is one of the promising and disruptive emerging technologies used in the field cryptography. It is a publicly shared database and it is freely availbale, which protects the data from damaging and preserves track of transactions. It is practically immutable and irreversible once a transaction is committed except the majority of the blockchain users collude.

In this paper, transaction processing system is proposed which uses a blockchain technology, zero-knowledge proof (ZKP) and modified elliptic curve cryptography (MECC) encryption method. Also, a prototype will develops 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.

Finally, the modified elliptic curve cryptography is 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 evaluate. 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 curves are available with different specifications and different speeds of operation [20]. Figure 1 below shows the proposed transaction processing system.

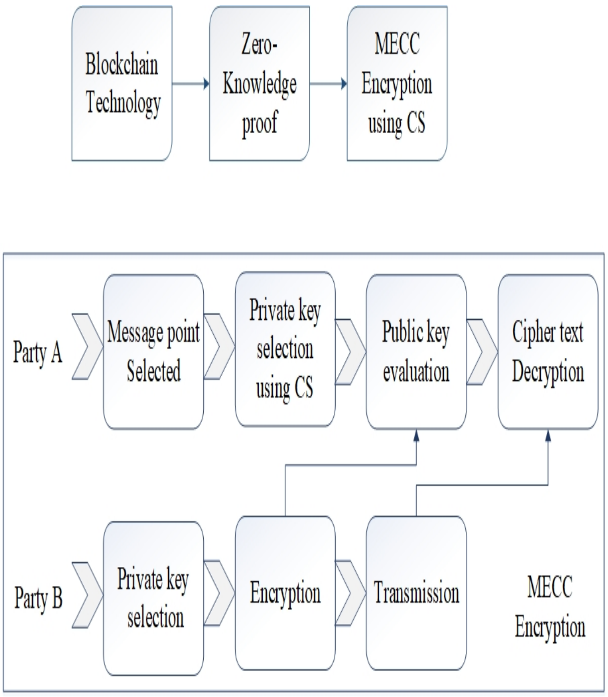

Fig. 1. Blockchain based Transaction Processing System.

V. 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 centre (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) [21]. 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.

This section explains the results of comparative analysis of Neighbor Similarity Trust [8], QADE [22], BARTD[23], 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 I 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.

- Accuracy (ACC): It refers the degree to which the result of a measurement, calculation, or specification conforms to the correct value or a standard.

$$ACC = \frac{T^P + T^N}{T^P + T^N + F^P + F^N} \tag{1}$$

- Precision (P): It refers to the closeness of two or more measurements to each other.

$$P = \frac{T^P}{T^P + F^N} \tag{2}$$

where, T^P, T^N, F^P, F^N and represent true positive, true negative, false positive, and false negative.

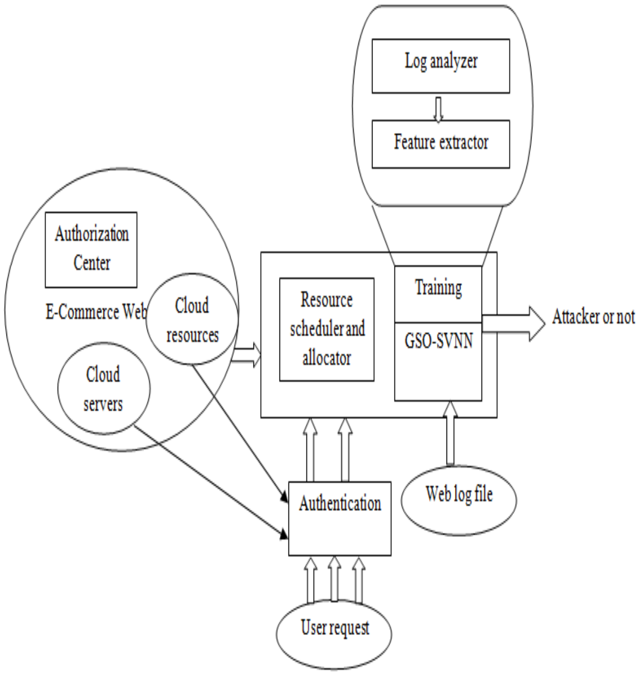

Fig. 2. Proposed Attack Detection Model.

TABLE I. 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

VI. Conclusion

In this paper transaction processing system is presented which provides secure transaction in E-commerce and attacker model is presented which protects E-commerce transaction against DoS attack. A transaction processing system is designed using a blockchain technology, zero-knowledge proof and modified elliptic curve cryptography encryption. The transaction processing system enhances the security of overall E-commerce transactions by providing confidentiality and integrity services. The DoS attack detection technique is proposed which uses the Glowworm Swarm Optimization based Support Vector Neural Network authorization for DoS attack detection. The GSO-SVNN design will overcome all the drawbacks mentioned in the literature survey. The proposed method of DoS attack detection shows better performance in terms of accuracy and precision as compared to other exiting methods. With the presented two models of security solution it is easy to preserve the confidentiality and integrity of E-commerce transactions.

REFERENCES

[1] K. Chatterjee and A.De "A Novel Multi-Server Authentication Scheme for E-commerce Applications Using Smart Card", Wireless Personal Communication, vol. 91, no.1, pp.293-312, 2016.

[2] T. Efraim, J. Outland, D. King, J.K. Lee, T.P Liang, and D.C. Turban, "Intelligent (Smart) E-commerce", In Electronic Commerce 2018, pp. 249-283, Springer, Cham, 2018.

[3] K. Tripathi, "M–Commerce: A Recent Trend in Business and Management", Journal of Arts, Science and Commerce, vol. 3, no. 4 pp. 25-28, 2012.

[4] S. H. Lee, D. DeWester, and S. R. Park, "Web 2.0 and opportunities for small businesses", Service Business, vol. 2, no. 4, pp. 335-345, 2008.

[5] M. Niranjanamurthy and D. Chahar, "The study of E-commerce security issues and solutions", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no.7, 2013.

[6] P. B. Rane and B. B. Meshram, "Transaction security for E-commerce application", International Journal of Elecronics and Computer Scince Engineering, vol. 1, no. 3, pp. 1720-1726, 2012.

[7] T. H. Chen, H.C. Hsiang, and W. K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards", Future Generation Computer System, vol. 27, no. 4, pp. 377-380, 2011.

[8] 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.

[9] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art", International Journal of Computer Applications, vol. 49, no. 7, 2012.

[10] P. Francesco, S. Ricciardi, and U. Fiore, "Evaluating network-based DoS attacks under the energy consumption perspective: new security issues in the coming green ICT area", IEEE International Conference on Broadband and Wireless Computing,Communication and Application pp.374-379, 2011.

[11] B. B. Gupta, R. C. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, vol. 2, no. 2, pp. 268-276, 2012.

[12] K. Arora, K. Kumar, and M. Sachdeva, "Impact analysis of recent DDoS attacks", International Journal on Computer Science and Engineering, vol. 3, no. 2, pp. 877-883, 2011.

[13] M. Uma, and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification", International Jounal of Network Security, vol. 15, no. 5, pp. 390-396, 2013.

[14] Y. Yanli, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012.

[15] S. Huasong, Q. Wang, and Q. Yan, "Very Short Intermittent DDoS Attacks in an Unsaturated System", 13th Internationl Conference on securiy and privacy in Comminication Systems, Springer, Niagara Falls, Canada, 2017.

[16] B. David, S. Sezer, and J. McCanny, "New sensing technique for detecting application layer DDoS attacks targeting back-end database resources", IEEE ICC Communication and Information Systems Security Symposium, pp. 1-7, 2017.

[17] K. C. Abdelaziz, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs", Vehicular Communications, vol. 9, pp. 254-267, 2017.

[18] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions", Computer Communications, vol. 107, pp. 30-48, 2017.

[19] K. J. Singh, and T. De, "Analysis of Application Layer DDoS Attack Detection Parameters Using Statistical Classifiers", Internetworking Indonesia 9, no. 2, pp. 23-31, 2017.

[20] 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.

[21] 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.

[22] 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.

[23] 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.