ECC BASED AUTHENTICATION AND OPTIMIZED SUPPORT VECTOR NEURAL NETWORK BASED AUTHORIZATION FOR DETECTION OF DOS ATTACK IN THE E-COMMERCE TRANSACTIONS

Javed R.Shaikh
Department of Communication Networks, Faculty of Telecommunication
Technical University of Sofia, Bulgaria

Abstract

In today's digital era Internet has become an important business medium and there are growing number of participants engaging in electronic commerce (E-commerce) .The use of e-payment system for various types tradings is on its way to make daily life more easy and convenient. At the same time, there are various security issues which need to be taken care; user anonymity and fair exchange have become important concerns along with authentication, integrity, confidentiality, and non-repudiation. Consumers are hesitant to carry out business over Internet due to concerns about trust and trustworthiness of participating entities. Protection using authentication service is not capable to detect entities that will provide ambiguous information or act dishonestly after entering the E-commerce system. To overcome this problem additional controlling mechanism should be implemented. The primary intention of this paper is to design and develop a technique to detect Denial of Service (DoS) attack in the E-commerce applications based on two mechanisms, namely authentication and authorization. The security will be provided with Elliptic Curve Cryptography (ECC) and hashing function to show the strength of the security protocol against a DoS and DDoS attacks. Once the authentication takes place between user and the server, the authorization will be done to diminish the DoS attack by deploying Glowworm Swarm Optimization based Support Vector Neural Network (GSO-SVNN).

Keywords: DOS; ECC; E-commerce; GSO; SVNN; Trust and reputation.

I. INTRODUCTION

Use of cloud computing is increasing rapidly as attractive model for computing, for the reason that it offers comparatively unlimited computing and network resources. The increasing demand of computing model allows providers to achieve improved resource utilization with statistical multiplexing and evade the costs of resource over provisioning with dynamic scaling [1]. On the other side the economic case for cloud computing is irresistible and the available security challenges are equally prominent [2]. Trust and trustworthiness of participating entities is main concern for consumers doing business over Internet [3]. Due to this concern robust security and trust mechanisms should be implemented to provide protection to communicating entities against malicious ones. Protection using well known security services, such as authentication, is known as hard security [4] and is not capable to find entities that will act dishonestly or provide ambiguous information. For that reason, additional robust control mechanisms should be designed to protect the system against such threats. Deployments of such control mechanism are known to as soft security [4]. Trust and reputation management systems are among the most important soft securities [5].

In cloud computing environment various resources such as computation, network resources, and storage are shared, because of this opponent may take benefit of this sharing

environment in order to launch attacks on the confidentiality, availability, accountability and integrity, of the service. Out of many attacks on these services DoS attack is a foremost security risk in cloud computing. It is a type of attack where, a malicious client (attacker) prevents legitimate clients partially or completely from gaining service from a server (victim). Another form of DoS attack is Distributed denial of service (DDoS) attack , which slowdowns the server in responding to the legitimate client or refuses the client request. Now-a-days, the impact of DDoS attacks on internet security is growing excessively. In general, this type of attack is launched explicitly from a group of compromised systems known as botnet by an attacker. The main goal of such attack is to exhaust server resources such as CPU, I/O bandwidth, sockets and memory etc. As the result, the resources available to other normal users/clients get limited or sometimes may not be available. As per the report of cloud security alliance DoS attack ranks fifth among cloud threats in the year 2013 [6] [2]. DoS attacks are common and can cause significant losses [7]. The recent familiar victims of DDoS attack are explored in [8] and [9] and strategies for successful attack mitigating are explored in [10][11]. The available defenses against such attacks are weak and not widely deployed [6].

II. LITERATURE SURVEY

Trust and reputation management systems plays very important role in promoting trust between unknown parties in online environments. In order to develop trust and reputation management techniques, many authors have proposed various computational models of trust [12] [13]. The reason behind this is to increase the number of good interactions between agents, evade bad interactions and reduce risk involved in transactions. Additionally, studies show that sellers having better reputations sell their items and with higher price [14] [15]. There are many open problems associated with trust and reputation management systems, out of which existence of unfair ratings in E-commerce systems is most important [16] [17]. This is the fundamental problem because an entity in an E-commerce system computes trust based on the ratings from other entities, of which it cannot control the honesty. The assessed trust value is misleading if false ratings from other entities are taken into the trust computation. It is clearly seen that the problem of unfair ratings should be resolved and is of great importance for E-commerce systems [5]. Table 1 shows literature of a variety of trust and reputation models proposed by the researchers.

TABLE I. LITERATURE SURVEY

Authors	**Contribution**	**Advantages**	**Disadvantages**
Eva Zupancic, and Denis Trcek [5]	Innovative (Qualitative Assessment Dynamics Extended) trust model	In order to correct the agent's trust attitude, it provides effective filtering of unfair ratings	Could not handle time-related issues
F. Al-Haidari *et al.* [18]	Analytical model based on Cloud Web Service Architecture	Scalability and availability of the cloud services, also suitable for other similarly behaving attacks such as DDoS attacks	Computation cost is high
Jiuxin Cao *et al. [2]*	Cloud dos attack detection architecture	Detection system can rapidly and precisely response to DoS attacks	Difficult to avoid all kind of attack flow
Gaik-Yee Chan *et al.* [19]	Predictive fuzzy associative rule model (FARM)	Adaptive, dynamic, predictive, sensitive, scalable and accurate in detection rate and prediction accuracy	Not suitable for bigger data sets on different data types

K. Munivara Prasad *et al.* [11]	Bio-Inspired Anomaly based App-DDoS detection model	Significantly minimized the computational overhead and retains the maximal prediction accuracy	Unable to identify the other significant attacks like Flash crowd
Guojun Wang *et al.[20]*	Sybil identification algorithm	Duplicated Sybil attack peers can be known as the neighbour peers become familiar and hence more trusted to each other	Unable to implement Sybil trust inside the context of peers which is there in many groups
Arunabha Mukhopadhyay *et al.*[21]	Cyber-risk assessment and mitigation (CRAM) framework	Improve information security, and effectively minimize security breaches to a particular level	The small size of the dataset makes it a bit difficult to train and test
Kamel Karoui [22]	Bit alternation method	Ensures the reversibility of the likelihood and impact metrics, diagnosing the cause of high risks	Unable to stop all kinds of threats, and processing time is high

III. CHALLENGES IN DESIGNING TRUST AND REPUTATION MODEL FOR E-COMMERCE

There are many challenges available while designing the model for DoS detection in the E-commerce transaction as the available model cannot fulfill all the requirements of secure environment for online business. The major challenges with the available models are listed below showing why those models are not that much appropriate for authentication and authorization in the E-commerce environment.

- Most existing works based on E-commerce transaction, which focuses on social networks and trusted certification, could not stop Sybil attack peers from completing transactions. [20].
- The limitations of CRAM framework are as follows: (i) the technique used the CSI–FBI (1997–2010) survey dataset. The small size of the dataset makes it a bit difficult to train and test our model, (ii) all the cyber-attacks are supposed to be independent, and (iii) correlated cyber-risk (CR) has not been considered [21].
- Deploying security equipment in a network without studying their usefulness and impact on the network's ability to stop attacks is unnecessary and may produce opposite effects. It is a loss of money and may cause a degradation of the network performance (processing time) [22].
- The traditional defence systems become less or even not applicable for application layer DDoS attacks, which make use of the asymmetric computation between client and server, as they are proper-looking requests from the protocol and traffic [11].
- The QADE trust model could not handle time-related issues. Namely, the current model does not differentiate between older and newer trust assessments [5]
- The FARM method could not applicable on real-world WS E-commerce applications, with tremendously scaled-up size datasets, to capture the normal and attack data for further optimum evaluation of the framework, besides detection and false alarm rates for effectiveness, and on 'time' performance for efficiency [19].

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Neal Koblitz and Victor Miller discovered the ECC in the year 1985. ECC system is type of public-key cryptographic scheme. The hardness of the elliptic curve discrete logarithm problem (ECDLP) decides the security of ECC. The advantage of using ECC is compared to other cryptographic schemes is, it provides the same level of security with smaller key size.

A. Elliptic Curve Groups

Let the elliptic curve E is considered over Fp, Where p is a prime number, and Fp indicates the field of integers modulo p. The equation (1) defines the elliptic curve E over Fp.

$$y2 = x3 + ax + b \quad (1)$$

where a, b ∈ Fp and fulfill the condition $4a3 + 27b2 \equiv 0 \pmod p$.

B. Elliptic Curve Discrete Logarithm Problem

If an elliptic curve E defined over Fq is given. Select two points P and Q from the curve E. Then the elliptic curve discrete logarithm problem is to find the value of integer x such that Q = xP. ECDLP is considered as more difficult to solve than the various factorization problems and general discrete logarithm problem that are used in other cryptosystems. In fact, nobody knows exactly how difficult ECDLP problem is to solve because no efficient algorithm is available to solve it [23]. The required key sizes of RSA cryptographic systems rise exponentially with increase in difficulty, while in elliptic curve systems the increase in required key size is relatively less. If ECC cryptosystems is implemented then it can be cracked only by solving ECDLP, so using this system Bob and Alice's can exchange their messages securely.

C. Elliptic Curve Encryption and Decryption Scheme

To understand encryption and decryption process consider E defined over a finite field Fp. Consider P be a random point on the curve and P has prime order n. The cyclic subgroup generated by point P for the curve E (Fp) is,

$$E(Fp) = \{\infty, P, 2P, 3P, \ldots (n-1)P\}$$

The elliptic curve E, the prime number p, the point P on the curve and its order n are the public key parameters. A private key d is selected randomly from the interval [1, n−1] (d ∈R [1, n−1]) and the corresponding public key is Q = dP. The problem of finding the value of d when domain parameters and Q is given is the ECDLP [24].

A plaintext m is embedded in the point on the curve that is M, and then encryption is performed by adding it to kQ, where k is a random integer, and Q is the Bob's public key. The Alice convey the points C1 = kP and C2 = M +kQ to the Bob who then calculates d*C1 = d*(kP) = k(dP) = kQ using her private key d, and then recovers M = C2 − kQ. Any unauthorised person wishes to recover M needs to calculate kQ. This task of computing kQ from the given domain parameters Q and C1 = kP is very difficult [24].

V.PERFORMANCE ANALYSIS OF ECC

Due to many advantages offered by ECC over other cryptographic algorithms, the ECC based authentication is proposed here. In this authentication model ECC based authentication is used in the environment where computation, storage and security are major constrained. So to analyze ECC performance, Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm is performed for specific elliptic curve which is shown in the equation (2). ECDH is actually a key-agreement protocol, which defines how keys are generated and exchanged between two parties. For this purpose, the elliptic curve over a finite field having a large prime number is considered, and calculations are taken in terms of computation time it needs to perform point multiplication on the curve and computation time it required for encryption and decryption of the secret message.

$$y2=x3+3x+5 \quad (2)$$

In this paper, ECDH algorithm as explained above is performed by considering various key sizes of the ECC such as 160 bit, 192 bit, 224 bit and 256 bit. In ECC 160 bit key size means the elliptic curve over finite field is considered having prime field size of 160 bit (The prime number p is having the length of 160 bits). The same ECDH algorithm is repeated for different prime field sizes using the elliptic curve as given in the equation (2). During analysis the computation time required by elliptic curve with various field sizes is noted down. The system having Intel core i3 processor with 4 GB of RAM was used during analysis.

Figure 1 provides the details of computation time required by ECC for different key sizes during encryption process that is the point multiplication process on elliptic curve and Figure 2 provides the details of computation time required by elliptic curve for decryption process of ECDH algorithm. The time required for computation is increasing with the increase in key size. Generally the need of security level decides the required key size of the elliptic curve

cryptographic algorithm. Today in practice 256 bit key size is preferred for strong security requirement.

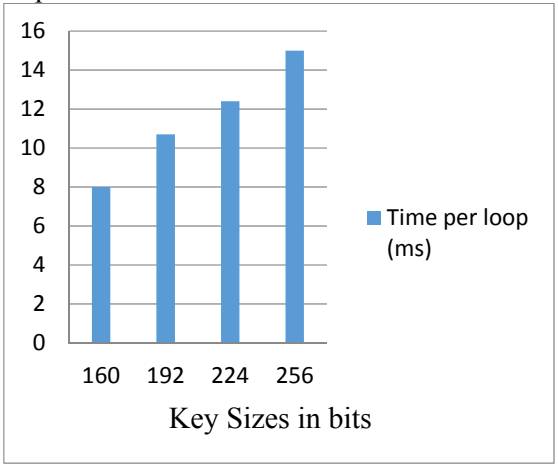

Fig. 1. Computation time taken for point multiplication during encryption.

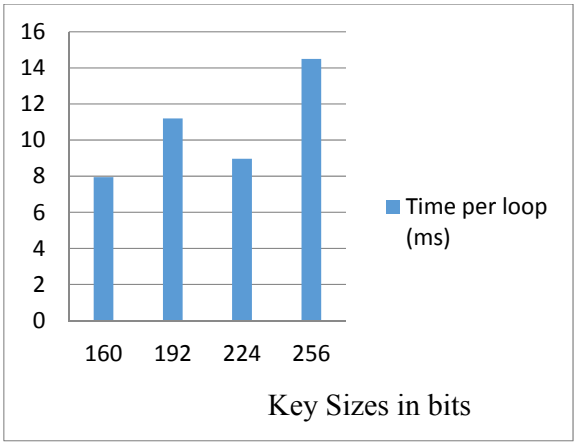

Fig. 2. Computation time taken for decryption.

The consumption of scarce resources decides the efficiency of any algorithm. As in [25] authors performed the implementation of ECC and Rivest–Shamir-Adleman (RSA) public key algorithm on hardware and found that as the word size of the processor decreases, the performance of ECC over RSA increases. Compared to RSA, ECC has advantage of smaller key sizes and faster computation, along with saving of memory, bandwidth and energy. According to [26] for 128-bit security levels, performance of RSA is generally 10-times slower than ECC for signature generation or key management operations. Typically for the comparison the measure used is time, but other measures such as space and number of processors are also considered. Table II shows the ECC and RSA key size requirement for various security levels.

TABLE II. KEY SIZES RSA, AND ECC FOR EQUIVALENT SECURITY LEVELS

	Security levels (bits)				
	80	**112**	**128**	**192**	**256**
ECC Key Size	160	224	256	384	512
RSA Key Size	1024	2048	3072	8192	15300

VI. GLOWWORM SWARM OPTIMIZATION

Glowworm Swarm Optimization (GSO) algorithm is used for the simultaneous capture of various optima of multimodal functions. [27]. Initially in GSO algorithm random distribution of swarm of agents in the search space is done. As agents are modeled after glowworms so henceforth agents will be called as glowworms. These glowworms are having some other behavioral mechanisms that are not present in their natural counterparts. Luminescent pigment called as luciferin is present in glowworms. The luciferin quantity encodes the fitness of glowworm locations and which allows them to glow at an intensity that is proportional to the function value being optimized. One assumption is made that the luciferin level of a glowworm does not decrease due to distance sensed by its neighbor [28].

In GSO algorithm a swarm is referred as the collection of N glowworms. To explain a glowworm state i at time t the set of variables are used in which $x^i(t)$ represents a position in the search space, $L^i (t)$ is a luciferin level and $r^i(t)$ represents a neighborhood range. GSO algorithm explains how these variables alter with change in time.

After the random distribution of agents in the search space, other parameters are initialized by predefined constants. Every next repetition consists of updation about glowworm movement, luciferin level and neighbourhood range. The fitness of the current position of a glowworm i in the luciferin level is encoded using the following equation (3),

$$L^i(t) = (1-\rho)\, L^i(t-1) + \gamma J(x^i(t)) \quad (3)$$

Where, ρ indicates the luciferin decay constant, γ indictes the luciferin enhancement constant and J is used to denotes an objective function.

In GSO every glowworm tries to find its neighbours. If a glowworm has several neighbours, the one neighbor will be selected randomly with probability proportional to the luciferin level of this neighbour. After this selection glowworm moves one step towards the selected neighbor with constant step size s. A glowworm j is said to be the neighbour of a glowworm i only if the distance between i and j is less than the neighbourhood range $r^i(t)$ and glowworm j has to shine brighter than than i ($L^i(t) > L^i(t)$).

During the last phase of algotithm, the neighbourhood range $r^i(t)$ is updated which is then used to bound the range of the communication in an group of agents by using equation (4).

$$r^i(t+1) = \min\{ r_s , \max [0 , r^i(t) + \beta (nd - | n^i(t) |)] \quad (4)$$

where, r_s is a sensor range, β is a model constant, nd is desired number of neighbours and $| ni(t) |$ is a number of neighbours of a glowworm i at time t.

VII. PROPOSED METHODOLOGY

The main objective of this paper is to design and develop a technique for DoS attack detection in the E-commerce applications based on two mechanisms, namely authentication and authorization. In the authentication phase, mutual authentication between user and server will be performed using several security parameters, such as session password, number of cache access and so on. Initially, the user and the server have to be registered under Authorization Centre (AC) for the authentication. Then, to authenticate the users various level of verification will be performed through different messages,

The security will be offered using the hashing function and ECC to prove the strength of the security protocol against DoS attacks. Once the authentication of user and the server is over, the authorization will be performed to mitigate the DoS attack during the E-commerce transactions. Here, the user behavior will be recorded based on several parameters, such as duration, service, flag, urgent, num_access_files, wrong_fragment, number of bytes sent from source to destination, number of bytes sent from destination to source, logged_in, number of connections to the same service as the current connection in the last two seconds and number of connections to the same host as the current connection in the last two seconds, in the web log file. Then, the important features will be selected from the web log file in the feature extraction process. Once the features are extracted, it will be fed as input to the proposed model of Glowworm Swarm Optimization (GSO) based Support Vector Neural Network (GSO-SVNN), to detect the DoS attack. The proposed GSO-SVNN will be designed by training the SVNN using GSO [28]. Figure 3 shows the block diagram of the proposed design for DoS attack detection. The implementation of proposed GSO-SVNN based DoS attack detection model will be done using the Matlab. The performance of the proposed design will be evaluated in terms of detection rate, accuracy, precision and recall, and will be compared with that of existing works [5], [17], and [20]. Moreover, an attack analysis will be performed to demonstrate the effectiveness of the proposed technique.

VIII. CONCLUSION

In this paper design of ECC based authentication and Glowworm Swarm Optimization based Support Vector Neural Network (GSO-SVNN) authorization for DoS attack detection is proposed. The design consists of the two mechanisms namely authentication and authorization. The proposed design will overcome all the drawbacks mentioned in the literature survey. 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. Key sizes for ECC and RSA along with their security levels are also shown in the paper where it is clear that ECC provides faster computation and better security with less key size.

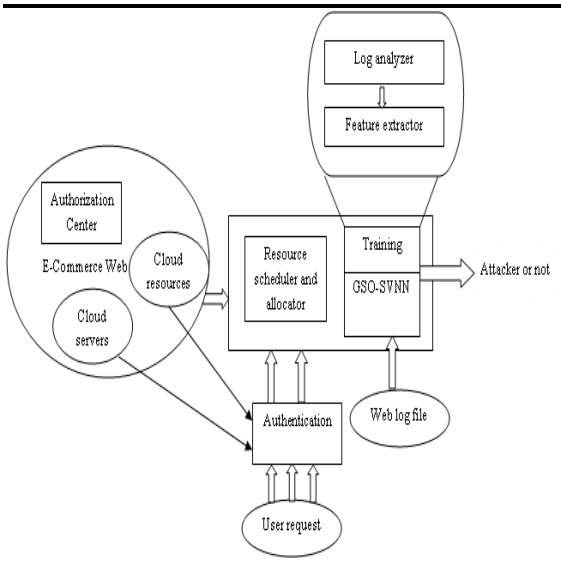

Fig. 3. Block diagram of proposed DoS detection technique.

The proposed DoS detection technique helps to detect DoS attack which hamperes the online business services.

Table I gives the overview of literature available for the trust and reputation models along with their limitations. Paper also highlights the challenges in designing the new trust and reputation model for E-commerce environment. The analysis of ECC is performed by considering the ECDH key exchange algorithm. The results shown in figure 1 and figure 2 show the computation time required by ECC for encryption and decryption process during ECDH algorithm. The proposed model for DoS detection will prevent the E-commerce transactions from DoS and DDoS attack and also it will be useful in the online business environment where less storage, faster computation and higher security level is required.

REFERENCES

[1] Yanpei Chen, Vern Paxson, and Randy H. Katz, "What's new about cloud computing security," University of California, Berkeley Report No. UCB/EECS-2010-5, no. 2010, pp. 2010-5, 2010.

[2] Jiuxin Cao, Bin Yu, Fang Dong, Xiangying Zhu, and Shuai Xu, "Entropy-based denial-of-service attack detection in cloud data center," Concurrency and Computation: Practice and Experience, vol. 27, no. 18, pp. 5623-5639, 2015.

[3] Estrella Gomez-Herrera, Bertin Martens, and Geomina Turlea, "The drivers and impediments for cross-border E-commerce in the EU," Information Economics and Policy, vol. 28, pp. 83-96, 2014.

[4] Lars Rasmusson, and Sverker Jansson, "Simulated social control for secure Internet commerce," in Proceedings of the 1996 ACM workshop on New security paradigms, pp. 18-25, 1996.

[5] Eva Zupancic, and Denis 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.

[6] TTW Group, "The notorious nine: Cloud computing top threats in 2013," Report, Cloud Security Alliance, 2013.

[7] Jose Brustoloni, "Protecting electronic commerce from distributed denial-of-service attacks," in Proceedings of the 11th ACM international conference on World Wide Web, pp. 553-561, 2002.

[8] J. Udhayan, and R. Anitha, "Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis," in proceedings of IEEE International Advance computing conference (IACC 2009), pp. 558-564, 2009.

[9] Xia Chun-Tao, Du Xue-Hui, Cao Li-Feng, and Chen Hua-Cheng, "An algorithm of detecting and defending CC attack in real time," in proceedings of 2012 IEEE International Conference on Industrial Control and Electronics Engineering (ICICEE), pp. 1804-1806, 2012.

[10] Stephen M. Specht, and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures," ISCA PDCS, pp. 543-550, 2004.

[11] K. Munivara Prasad, A. Rama Mohan Reddy, and K. Venugopal 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.

[12] Isaac Pinyol, and Jordi Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: a review," Artificial Intelligence Review, vol. 40, no. 1, pp. 1-25, 2013.

[13] Audun Josang, Roslan Ismail, and Colin Boyd, "A survey of trust and reputation systems

for online service provision," Decision support systems, vol. 43, no. 2, pp. 618-644, 2007.

[14] Paul Resnick, and Richard Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," in proceedings of the Economics of the Internet and E-commerce, Emerald Group Publishing Limited, pp. 127-157, 2002.

[15] David Lucking-Reiley, Doug Bryan, Naghi Prasad, and Daniel Reeves, "Pennies from eBay: The determinants of price in online auctions," The journal of industrial economics, vol. 55, no. 2, pp. 223-233, 2007.

[16] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru, "A Survey of attacks on Reputation Systems," pp. 1-17, 2007.

[17] Ya-Fei Yang, Qin-Yuan Feng, Yan Lindsay Sun, and Ya-Fei Dai, "Dishonest behaviors in online rating systems: cyber competition, attack models, and attack generator," Journal of Computer Science and Technology, vol. 24, no. 5, pp. 855-867, 2009.

[18] F. Al-Haidari, M. Sqalli, and K. Salah, "Evaluation of the impact of EDoS attacks against cloud computing services," Arabian Journal for Science and Engineering, vol. 40, no. 3, pp. 773-785, 2015.

[19] Gaik-Yee Chan, Chien-Sing Lee, and Swee-Huay Heng, "Defending against XML-related attacks in E-commerce applications with predictive fuzzy associative rules," Applied Soft Computing, vol. 24, pp. 142-157, 2014.

[20] Guojun Wang, Felix Musau, Song Guo, and Muhammad Bashir Abdullahi, "Neighbor similarity trust against sybil attack in P2P E-commerce," IEEE transactions on parallel and distributed systems, vol. 26, no. 3, pp. 824-833, 2015.

[21] Arunabha Mukhopadhyay, Samir Chatterjee, Kallol K. Bagchi, Peteer J. Kirs, and Girja K. Shukla, "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance," Information Systems Frontiers, pp. 1-22, 2017.

[22] Kamel Karoui, "Security novel risk assessment framework based on reversible metrics: a case study of DDoS attacks on an E-commerce web server," International Journal of Network Management, vol. 26, no. 6, pp. 553-578, 2016.

[23] Elaine Brow, "Elliptic Curve Cryptography" Math 189A: Algebraic Geometry, 2010.

[24] Darrel Hankerson,Alfred Menezes,Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, Inc, 2004.

[25] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, " Comparing Elliptic Curve Cryptography and RSA on 8- Bit CPUs", CHES 2004, LNCS 3156, pp. 119–132, 2004.

[26] Kerry Maletsky, "RSA vs. ECC Comparison for Embedded Systems" Atmel, White paper, 2015.

[27] Piotr Oramus, "Improveemnts to Glowworm Swarm Optimization: Algorithm", Computer Science, Jagiellonian University in Krakow,Poland Volume 11,2010

[28] Krishnanand N. Kaipa, and Debasish Ghose, "Glowworm Swarm Optimization: Algorithm Development," Glowworm Swarm Optimization, Springer International Publishing, pp. 21-56, 2017.