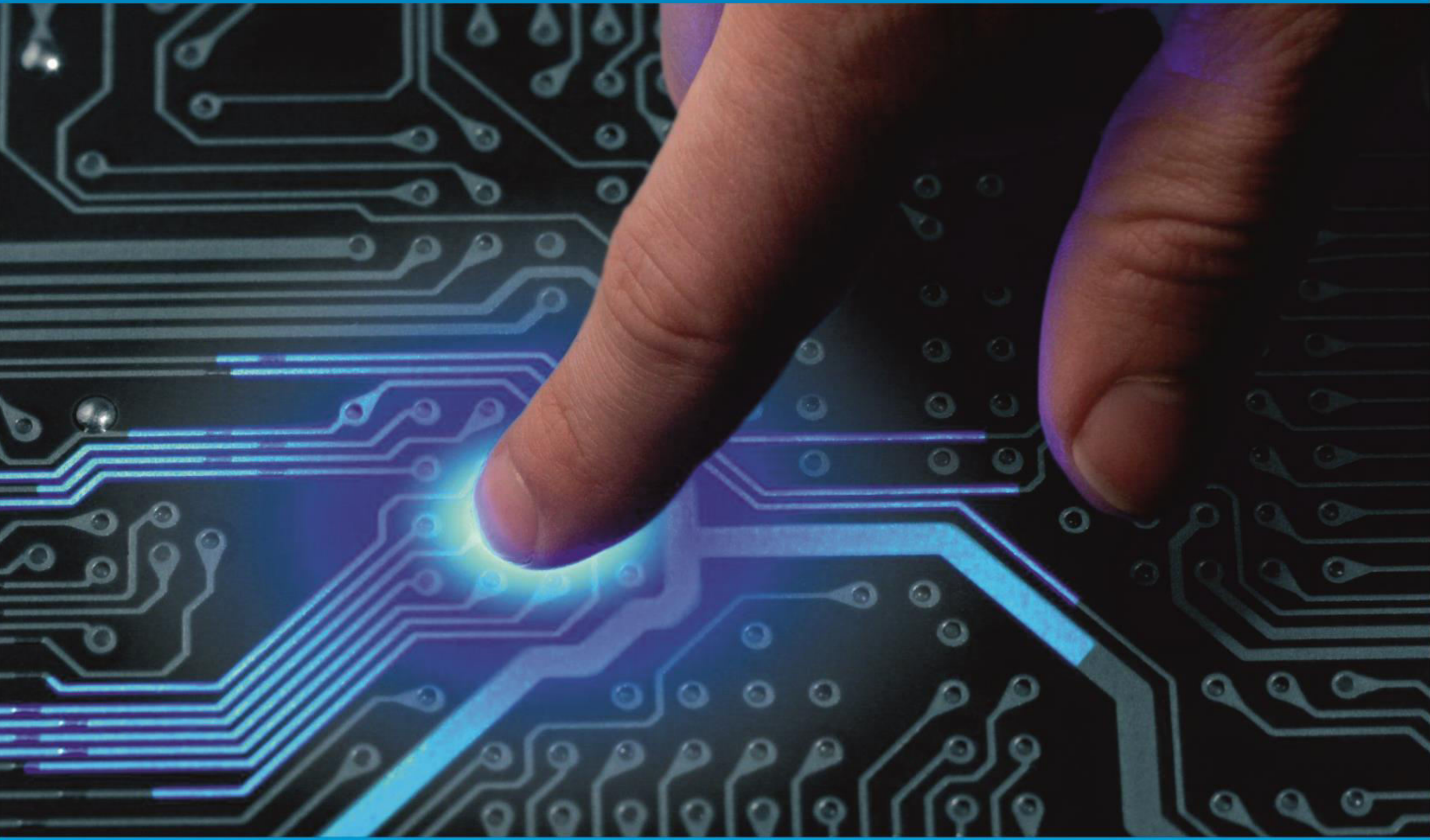
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903145|

DDOS Attack Detection Scheme Using Cryptography in Blockchain Technology

[1]Mrs.A.M. Sermakani B.E., M.E., (PH. D), [2]Shivani Sree.K B

[1]Associate Professor, Department of Information Technology, S. A. Engineering College, Chennai, India

[2]UG Scholar, Department of Information Technology, S. A. Engineering College, Chennai, India

ABSTRACT: With development of block chain technology, and its security theory research and practical application have become crucial. Now a new DDoS attack has arisen, and it is the DDoS attack in blockchain. The attack is unsafe for blockchain and many other scenarios. However, the traditional and existing DDoS attack detection and defense means mainly come from the solution. Aiming at the above problem, the paper proposes the anti- DDoS chain design philosophy and detection framework. AdaBoost and Random Forest are used as our machine learning strategy, and some different lightweight classifiers are used, such as CART and ID3. Experimental results confirm that our DDoS sensing method has better performance.

KEYWORDS: DDoS attack, Cryptography, Blockchain Technology

I. INTRODUCTION

Currently, the Internet inter connects billions of computers and smart device, and provides a global communication, storage and computation resources. Internet security is facing great challenges in many fields that include politics, economics, military, and social life. Security problem has been regarded as the dominated bottleneck of the development of Internet of Thing, Big Data, Cloud Computing, Artificial Intelligence, and Software Defined Networking (SDN) yet. Confidentiality, integrity, and availability are three important security issues of networks [1]. For availability of Internet service, the Distributed Denial of Service (DDoS) attack is one of the most significant threats. In spite of some forceful safeguards, the attack is still the most frequent and the most devastating one. With the rapid development of blockchain technology, the attack is bound to endanger blockchain network and many business applications.

II. EXISTING SYSTEM

The recent research work for DDoS attack detection years mainly includes the followings. In 2016, Jia et al. [9] focused on how to distinguish the attack traffic from normal data flows in Big Data and brought forward a novel real-time DDoS attack detection mechanism based on Multivariate Dimensionality Reduction Analysis (MDRA) algorithm. In this mechanism, the dimensionalities of multiple characteristic variables recorded by Component Analysis (PCA) first are reduced. In 2017, Somani et al. raised a new "Scale Inside-out" approach which reduces the "Resource Utilization Factor" to a minimal value for quick absorption of the attack. The novel approach sacrifices victim service resources and provides those resources to mitigation service in addition to other co- located services to ensure resource availability during the attack.

III. PROPOSED SYSTEM

Learning method and uses Virtual Reality (VR) parallel tactics.

i. In the first blockchain, the different lightweight classifiers are alternately deployed in different blocks of the same chain, such as CART and ID3. They coordinate complementary to detect and resist DDoS attack by combining strategy and thought of AdaBoost.use the other ensemble learning algorithms.

ii. The artificial blockchain based on VR parallel tactics is structured in an experimenter and it is connected with the actual blockchain by virtual and realistic interaction means. The interaction includes two aspects. Firstly, the fast and precise intelligent detection for DDoS attack traffic in artificial blockchain can effectively guide the DDoS.

IV. SYSTEM REQUIREMENT

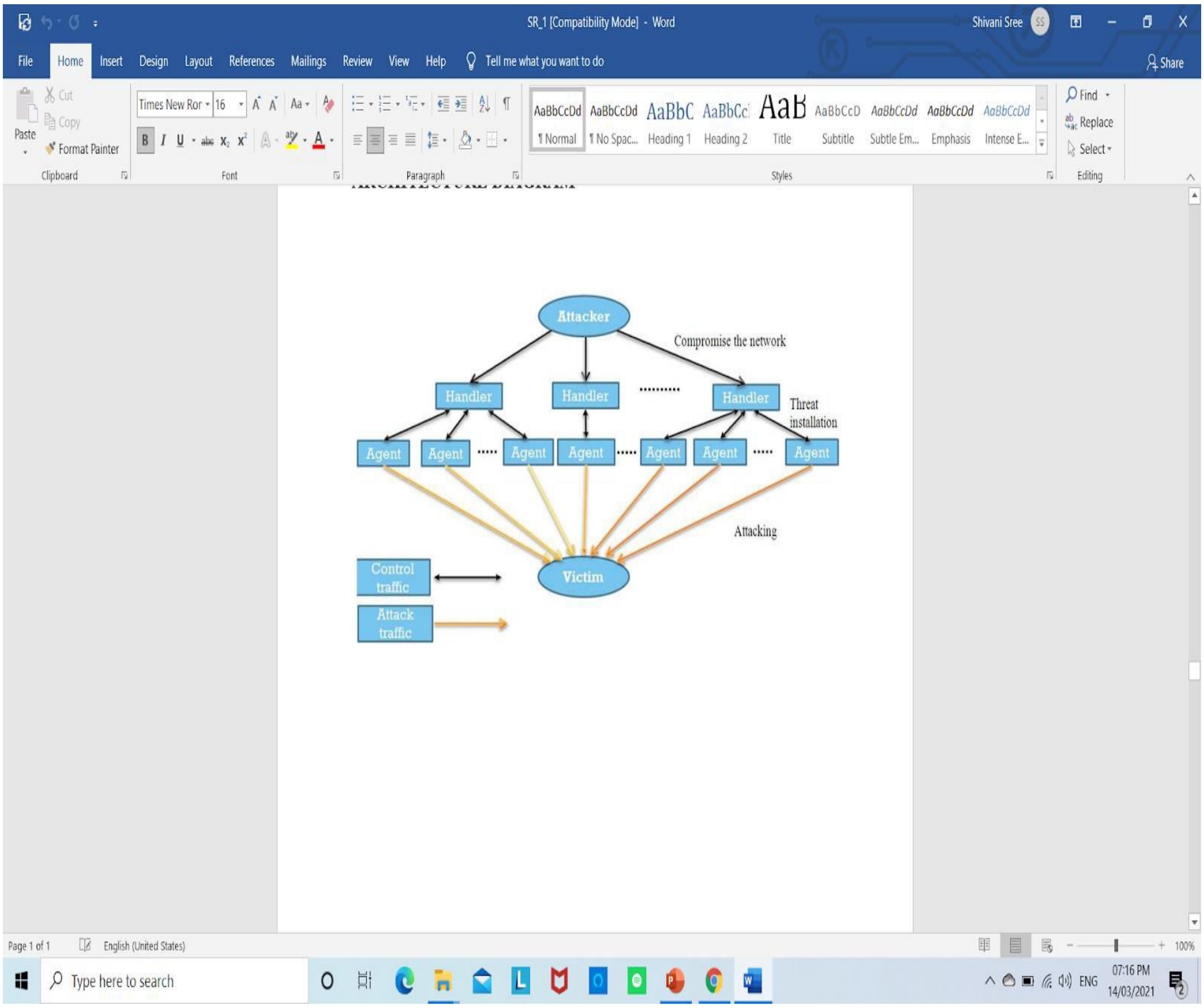
SOFTWARE REQUIREMENTS

Operating System	:	Windows 7-64 bit
JAVA IDE	:	Eclipse
Programming Language	:	Java
Database	:	MySQL

HARDWARE REQUIREMENTS

PROCESSOR	:	Dual Core 2 Duos.
RAM	:	4 GB DDR RAM
HARD DISK	:	250 GB

V. SYSTEM ARCHITECTURE



VI. MODULES

- Data collection & pre-processing
- Implementing the AdaBoost algorithm
- Implementation of the training model for the detection of the DDOS attacks & classification of the DDOS attacks
- Evaluating input training models for the better accuracy.

DATA COLLECTION & PREPROCESSING

Data collection which means collecting the data from the different sources. after collecting the data dataset will prepare. The main objective of the data pre-processing step is to remove the noise and outliers which are less suitable to find the sentiment of texts or tweets. This noise could be punctuation, numbers, special character, and some terms which do not hold much weight in the context of the text. Like removing twitter handles, removing punctuation, numbers, short words, and special characters. After this we tokenize

IMPLEMENTING THE ADABOOST ALGORITHM

AdaBoost algorithm, the sample weights of misclassification in learner will be enhanced in previous iteration, the sample weights of correct classification will be lowered. The distribution of sample is changed in every iteration; the sampling cannot be repeated.
The algorithm uses weighted majority voting strategy. The weights show performance of
every weak learner. The core of this strategy is to increase the weights of weak learner whose classification error rate is smaller, and to decrease the weights of weak learner whose classification error rate is higher. It has the lower generalization error, the higher classification accuracy, and the smaller probability to overfit. AdaBoost is sensitive to noise and outlier.

IMPLEMENTATION OF THE TRAINING MODEL FOR THE DETECTION OF THE DDOS ATTACKS & CLASSIFICATION OF THE DDOS ATTACKS

Different algorithms are randomly deployed in parallel block chains respectively. They coordinate complementarily to detect and resist DDoS attack in the chains. The ensemble learning algorithm that uses different lightweight classifiers is able to improve immensely the generalization performance, universality and complementarily to accurately identify the onslaught features to launch an attack. The parallel anti-DDoS chain design philosophy
uses virtual and realistic interaction strategy. The strategy is that the artificial block chain and actual block chain interact by computing, experimenting, and evaluating. The artificial block chain can constantly optimize the actual block chain. Otherwise, the actual blockchain can continually guide the artificial blockchain as well.

EVALUATING INPUT TRAINING MODELS FOR THE BETTER ACCURACY

Here β is used to balance the weights between Precision and Recall in F-Score computation. When,
(I) β=1, it shows that Precision is as important as Recall.
(ii) β<1, it expresses that Precision is more important than Recall.
(iii) β>1, it denotes that Recall is more important than Precision.
Here, we set β=1, therefore,
F1-Score= $2\times Precision * Recall / Precision * Recall$
F1-Score = $2\times TP / 2*TP+ FP + FN$
So F1-Score takes comprehensively into account the two results (i.e., Precision and Recall).
TPR=Recall=$TP / TP+ FN$
TP (True Positive): It is the number that positive samples are correctly classified as positive samples;
FP (False Positive): It is the number that negative samples are incorrectly classified as positive samples;
TN (True Negative): It is the number that negative samples are correctly classified as
negative samples;

VII. CONCLUSION

In this work, I've worked to detect the DDoS attack using parallel blockchain technology and parallel DDoS detection philosophy. In addition, a heuristic judgment based on experience is used as our weight selection approach. This project also rectifies the server downtime error due to DDoS attack.

REFERENCES

1. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation computer systems, vol. 28, no. 3, pp. 583-592, 2012.
2. N. Hoque, D.K. Bhattacharyya, and J.K. Kalita, "Botnet in DDoS attacks "Botnet trends and challenges," IEEE communication surveys & tutorials, vol. 17, no. 4, pp. 2242-2270, 2015.
3. Q. Wei, Z. Wu, K. Ren, and Q. Wang, "An open flow user-switch remapping approach for DDoS defense," KSII Transactions on Internet and information systems, vol. 10, no. 9, pp. 4529-4548, 2016.
4. S. Behalf and K. Kumar, "Detection of DDoS at tacks and flash events using information theory metrics-An empirical investigation," Computer Communications, vol. 103, pp. 18-28, 2017.
5. R.Y. Chen, "A traceability chain algorithm for artificial neural networks using T–S fuzzy cog native maps in blockchain," Future Generation Computer Systems, vol. 80, pp. 198- 210, 2018.
6. Y. Yuan, and F.Y. Wang, "Parallel blockchain: concept, methods and issues," Acta Automatic Sinica, vol. 43, no. 10, pp. 1703-1712, 2019
7. B. Jia, Y. Ma, X. Huang, Z. Lin, and Y. Sun, "A novel real-Time DDoS attack detection mechanism based on MDRA algorithm in big data," Mathematical Problems in Engineering, pp. 1-10, Sep. 2016.
8. Y. Yong, X. Ni, S. Zeng, and F.Y. Wang, "Block chain Consensus Algorithms: The State of the Art and Future Trends," Acta Automatic Sinica, vol. 44, no. 11, pp. 2011-2022, 2016.
9. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016.
10. Bin JiaShandong and Yongquan Liang: Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain in 2020.