International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 15, 2019 (Special Issue)

Can Blockchain Technology be the future of Network Intrusion Detection System: A review

Shreevyas H M
Research Scholar, dept. of CSE,
DIAT-DRDO, Pune, IN.
shreevyas@gmail.com

C R Suthikshan Kumar
Professor, Dept. of CSE,
DIAT-DRDO, Pune, IN.
suthikshnkumar@diat.ac.in

Ruhin A Shaikh
Dept. of CSE,
ACU, BG Nagar, KA, IN.
ruhinshaikh02@gmail.com

Abstract— The advent of internet and development of latest hardwares has made billions of personal devices and electronic gadgets to communicate like never before using the high-speed network but at the cost of being vulnerable to numerous kinds of cyber-attacks. Network Intrusion detection systems are the preferred choice by most of the organizations to protect their devices and network resources. However, only IDS is not a viable solution to the rapidly changing technologies and increasing attack rate as IDS is a trust-based approach. In this paper we have discussed the possibility of using one of the emerging technologies such as Blockchain to build next generation network intrusion detection systems. The paper discusses about the IDS, blockchain technology, integrating blockchain for IDS and also research issues and open challenges.

Keywords— Blockchain, IDS, Collaborative Network Intrusion Detection system, Cyber Security

I. INTRODUCTION

In recent days, the cyber-attacks have become even more intricate and the intruders that are spread across the network have major impact on the society. It is highly difficult to completely avoid such threats but detecting such threats at the early stages may help protect the systems from being afflicted. Therefore, Intrusion detection systems (IDS) are used to reduce peril to the network. wireless networks are more vulnerable to malicious attacks than wired networks.

IDS are basically intended to monitor, analyze the network traffic and to detect variety of attacks inflicted in the network.

According to the literature, the emerging technology blockchain has proven its ability to achieve literally unbreakable security for cryptocurrencies such as bitcoin. That has motivated us to investigate the capabilities of Blockchain to build next generation collaborative network intrusion detection systems [1]. In recent years the blockchain technology has shown its adaptability in many fields including banking, managing supply chain and also in the healthcare sectors [2, 3]. As this technology has the ability to protect the integrity of the data storage and transparency in the process. We have reviewed the idea of using blockchain in building the next generation IDS.

This paper is organized as follows. Section II gives an overview about Intrusion Detection System and CIDS, section III describes about the Blockchain technology and its applications. Section IV discuss the possibility of integrating the blockchain to build an effective next generation network intrusion detection system. The last section gives a list of research issues and open challenges in this domain.

II. BACKGROUND ON IDS

Intrusion detection systems are the advanced security systems designed to monitor, analyze the network traffic and to detect variety of attacks inflicted in the network [4]. IDS are classified into two categories such as Host based intrusion detection system and Network based intrusion detection system.

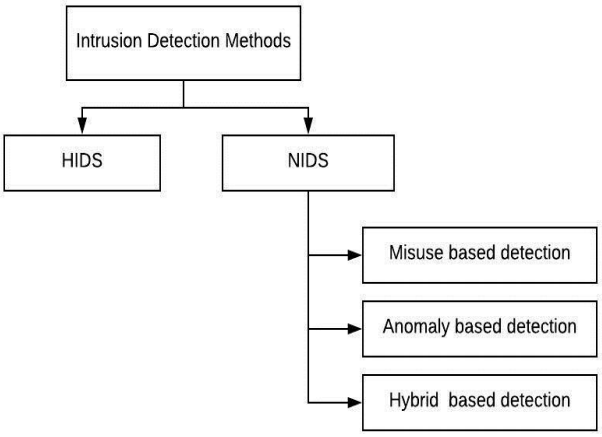

Fig. 1. IDS classification methods

A. *Host based Intrusion Detection System (HIDS)*

HIDS screens and dissects process and record exercises identified with the product condition, for example, programming calls, nearby security approach, neighborhood log reviews and so forth with a particular host and furthermore the occasions happening inside that have for suspicious exercises. HIDS are ordinarily conveyed on hosts, for example, openly available servers and servers containing delicate data.

B. *Network based Intrusion Detection System (NIDS)*

NIDS examines traffic between host looking for patterns or signatures of nefarious behavior. Active IDS generates alarms as well as blocks the detected malicious traffic whereas Passive IDS informs the system administrator about the attack by generating alarms. NIDS are further classified into three types such as Misuse based, Anomaly based and Hybrid based detection methods.

Misuse or signature-based detection: An IDS designed to detect known attacks using the signatures generated for those attacks. This type of detection is fast and easy to configure but its limitation is that the attacker can slightly modify the attack so that it cannot be detected.

Anomaly based detection [5]: This method is useful for detecting unwanted traffic, that is specifically unknown. It models the normal network and system behavior based on deviation from normal i.e., anomalies are detected. The advantage is that the profiles of normal activity are customized for every system., hence making it difficult for the attacker. The limitation is that it has high false alarm rate. Anomaly based methods can be further categorized in three ways namely Point anomaly, Contextual anomaly and collective anomaly.

Hybrid detection method: This is a combination of misuse and anomaly-based detection in order to prevent attacks. Hybrid based approach is used to increase detection rates of known attacks and also to decrease false positive rates for unknown attacks.

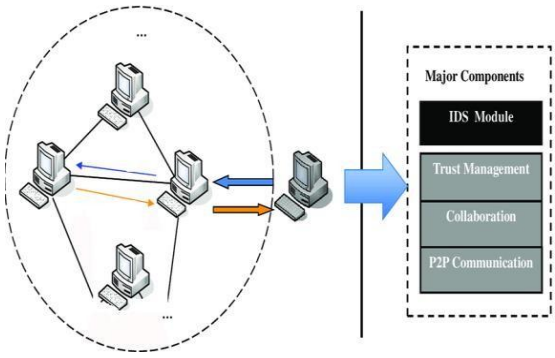

Fig.2 CIDS architecture

CIDS framework [6,7] allows various nodes in the network to exchange information. Hence data will be stored in all the collaborating nodes [8] in the network.
Each node comprises of IDS module, trust management [9], collaboration and p2p communication [10]. IDS module manages intrusion detection functions.

III. BACKGROUND ON BLOCKCHAIN

The blockchain in its fundamental form can be viewed as the distributed, decentralized, transparent and ordered database of exchanges [11]. The data in the blockchain is partitioned into blocks. Each block comprises of data, past hash and present hash. Hash resembles a fingerprint of the data in the block. The initial block is called Genesis block. Each block is depending upon the past one. These blocks are cryptographically connected to one another by the hash function thus the name is given as blockchain. The framework in which a blockchain serves as the database involves nodes [12]. These nodes are responsible for appending new blocks to the blockchain. Another block can only be appended after all nodes in the framework achieve a consensus. The blockchain innovation brings new idea which grasps new innovations in technology and shifts the power from one to many, or from central idea to a distributed one.

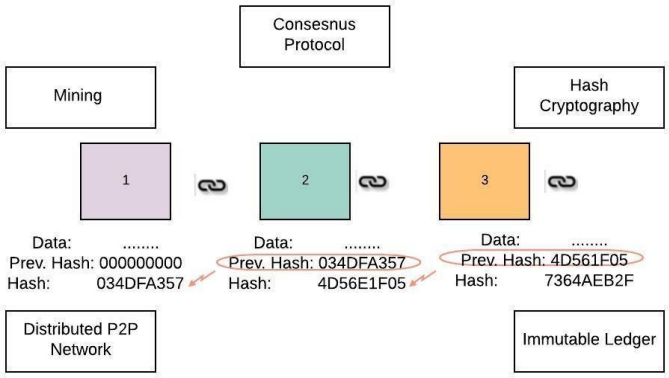

Fig. 1. Overview of Blockchain technology

A. *HASH CRYPTOGRAPHY:*

Secure Hash Algorithm (SHA): It is one of the cryptographic hash functions. A cryptographic hash [13] is resembles a signature for any computerized record. Hash is a one-way function, it cannot be decoded back. There are different SHA algorithms like SHA 256, SHA 512, SHA 3 etc. where 256,512 and 3 represents the bits it takes up in the memory. If we modify the data in the block then the hash generated will change completely. Hence exhibiting Avalanche effect. The five requirements for hash algorithm are one-way, deterministic, fast computation, avalanche effect, must withstand collision [14].

B. *Immutable Ledger*

Ledger is used to keep records. Immutable ledger [9] refers to a ledger that cannot be corrected, it remains permanent. Because of any change in one block the succeeding blocks have to be changed that leads to breaking of the chain. Hence it becomes difficult for anyone who wants to manipulate the data.

C. *Distributed Peer-to-Peer Network*

Distributed p2p network [15] consists of n-number of computers so the entire blockchain will be stored across the network in many systems. If any block is hacked then the other computers in the network communicate with each other regarding modification in the blockchain. Once the

modification is detected in the network then the correct values will be copied and hence data will be restored. Therefore, the hacker has to attack more than 50% of the blockchain at a time only then they can hack successfully. Hence additional security comes into picture where technology brings trust in trustless network.

D. MINING

A block stores multiple transaction. Mining is all about nonce. Nonce gives extra control and flexibility. we can change the hash by changing nonce. The miners solve the cryptographic puzzle to find the correct hash. The miners work to calculate the correct nonce by changing different nonce values. For the block to be added in the blockchain the hash generated should be less than target and the hash should start with leading zeroes.

When two miners perform mining at the same time for same block then byzantine problem occurs. The blocks which are not majority are called orphaned blocks. In this case the transaction doesn't take place in the network.

E. CONSENSUS PROTOCOL

The protocol regulates the computation of new blocks [16]. The block is shared among all nodes in the system, the protocol is responsible to keep the blockchain valid. The protocol regulates how the blockchain is used for specific purpose. Consensus protocol [17] provide defense against attackers. Different types of consensus protocols include proof of work, proof of stake, proof of elapsed time etc.

F. Applications of Blockchain Technology

Due to the nature of blockchain, this emerging technology can be widely implemented in various fields like finance [18], healthcare, defense applications [19] and in various other applications. Blockchain technology has been widely used in financial transactions like Cryptocurrencies. bitcoin is one of its kind. In order to ensure security and integrity of the medical information Blockchain technology plays a vital role in providing solutions in the distributed environment explores the potential application of blockchain technology in healthcare, its various requirements, challenges and obstacles encountered for using blockchain technology. It also introduces the smart contracts [20] for blockchain based healthcare systems for pre-defined agreement among various stakeholders. Other implementations of blockchain include blockchain for IOT [21], blockchain for big data
[22] blockchain for data security [23] in cloud computing.

IV. HOW CAN WE USE BLOCKCHAIN AS AN IDS

As the number of internet enabled devices are growing in a rapid phase, the complexity of the network also increased with time. The single IDS may not be sufficient for the effective detection of various attacks. Therefore, to overcome the above-mentioned issue, the concept of collaborative intrusion detection framework [1] is used because of its enhanced detection accuracy. The collaborative Intrusion Detection System (CIDS) allows the IDS nodes to exchange data with each other, however there are two important issues such as data sharing and trust management which may affect the detection accuracy.

Because of the inalienable idea of blockchain innovation, it very well may be demonstrated for comprehending the difficulties with the CIDS. The problem of data sharing in blockchain can be addressed by building strong correlation between collaborating parties and can protect privacy in the data by working as an irreversible contract ledger between the owner of the data and the rest of the communicating parties. Since blockchain allows to resolve the trust computation issue, the resulting collaborative IDS will be the robust IDS.

V. FUTURE WORK AND RESEARCH CHALLENGES

Even though use of blockchain in CIDS shows promising approach in achieving high detection accuracy and least misclassification rate, addressing data sharing with all the communicating parties is still a major concern, since trusting each other is a big challenge for the all the communicating parties to achieve data privacy. By the design philosophy, blockchains are suitable for managing the records of events, medical records, and transactions. Therefore, ensuring proper data sharing is very essential to fight against the problem with the centralized IDS method. As Blockchains were initially developed for the purpose of cryptocurrencies, It cannot be used in the same way as it exists today, so proper research in customizing and developing the consensus protocols for the network intrusion detection is not addressed by many researchers.

SUMMARY.

In this paper, we have discussed the issues with the existing Intrusion detection system and the architecture of collaborative IDS is also discussed. This study presents a new research direction of using emerging technology of blockchain as an IDS in a collaborative environment. The literature shows that there are multiple techniques have been used to improve the performance the IDS in the last two decades but the innovative method of using blockchain as an IDS can really make the IDS more robust, highly secured and that leads to the reduced misclassification rate. However, we have also discussed the open challenges and about the future work, which is very essential to make it a reality.

ACKNOWLEDGMENT

The authors would like to Thank the DIAT-DRDO, Pune and ACU, BG Nagar for their valuable support and constant encouragement.

References

[1] Weizhi meng, Elmar wolfgang tischhauser, qingju wang, yu wang and jinguang han,"When intrusion detection meets blockchain technology: A review", Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies, IEEE access, Vol:6, 1, 2018

[2] Matthias mettler,"Blockchain technology in healthcare,the revolution starts here", IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Sept -2016

[3] Tomaso Aste,Paolo Tasca and Tiziana Di Matteo "Blockchain Technologies : The foreseeable impact on society and industry", Published in Computer (Volume: 50) Issue:9, 2017.

[4] Shadi aljawarneh, Monther aldwairi and muner bani yassein," Anomaly based intrusion detection system through feature selectin analysis and building hybrid efficient model", Journal of computer science, Vol 25, March 2018.

[5] P. T. pham and S.Lee. (2017),"Anomaly detection in the bitcoin system-Anetwork perspective".[online].Available:https://arxiv.org/abs/1611.03942

[6] N.Alexopolous,E.Vasilomanolakis,N.R.Ivanko,M.muhlhauser,"Towards blockchain-based collaborative intrusion detection system",in proc.Int. Infracture.secur.,2017,pp. 1-12.

[7] Y.-S. Wu,B.Foo,Y.Mei, and S. Bagchi."Collaborative intrusion detection systems(CIDS):A framework for accurate and efficient IDS", in proc. Annu. Comput. Secur.Appl.Conf. (acsac),Dec. 2003,pp.234-244.

[8] Vasilomanolakis, E., Habib, S.M., Malik, R.S., Milaszewicz, P., M• uhlh• auser, M.: Towards trust -aware collaborative intrusion detection: challenges and solutions. In: International Conference on Trust Management (IFIPTM). Springer (2017)

[9] Vasilomanolakis, E., Karuppayah, S., M• uhlh• auser, M., Fischer, M.: Taxonomy and Survey of Collaborative Intrusion Detection. ACM Computing Surveys 47(4), 33 (2015)

[10] C. Duma ,M.Karresand,N.Shahmehri, and G.Caronni,"A trust-aware,P2P-based overlay for intrusion detection",in proc.DEXA Workshop,2006,pp.692-697

[11] S.nakamoto (October-2008).Bitcoin:A peer to peer electronic cash system.[online].Available :http://bitcoin.org/bitcoin.pdf

[12] Bayu Adhi Tama,Bruno Joachim Kweka,Youngho Park and Kyung-Hyune Rhee, "A critical review of blockchain and its current applications", International conference on Electrical engineering and computer science (ICECOS) -2017

[13] Karl wust and Arthur Gervais,"Do you need a blockchain?", Crypto Valley conference on Blockchain (CVCBT) June 2018

[14] R. Goyal and V.Goyal,"overcoming cryptographic impossibility results using blockchains", in proc. 15th Int. Conf. TCC, Baltimore,MD,USA,2017,pp.529-561.

[15] Walport, M.: Distributed ledger technology: Beyond blockchain. UK Government office for Science (2016)

[16] N. Szabo. Smart Contracts: Building Blocks Digital Markets.Accessed:Oct.15,2017.[online].Available: http://www.fon.hum.uva.nl/rob/courses/informationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[17] Baliga, A.: Understanding Blockchain Consensus Models. Tech. rep., Persistent Systems Ltd. (2017)

[18] Antonopoulos, A.M.: Mastering Bitcoin: unlocking digital cryptocurrencies.O'Reilly Media, Inc. (2014)

[19] Amool sudhan and Manisha j nene,"employability of blockchain technology in defense applications",proceedings of the international conference on intelligent sustainable system(ICISS 2017)

[20] Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292{2303 (2016)

[21] bing mo,kuiren su,songjie wei,cai liu,jianping guo,"A solution for internet of things based on blockchain technology". 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), July 2018

[22] elena karafiloski and anastas mishev,"blockchain solutions for big data challenge", IEEE EUROCON 2017 -17th International Conference on Smart Technologies, July 2017

[23] S.prianga,R.sagana and E.sharon,"evolutionary survey on data security in cloud computing using blockchain. IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) July 2018