INTRUSION DETECTION SYSTEM (IDS) FOR BLOCKCHAIN SECURITY

Feroz Ahmed[1*], Kriti Sharma[2], Meenakshi Gupta[3], Rinky Ahuja[4]

Article History: Received: 27.03.2023 **Revised:** 12.05.2023 **Accepted:** 28.06.2023

Abstract:

Block chain is basically an open, distributed, decentralized, publicly available digital ledger containing all the blocks in a chain having a hash-linked data structure where hashing is enabled by public – key cryptography. It is a concept based on which we are having the protocol of Bit coin; the widely known cryptocurrency. This work discusses the implementation of intrusion detection mechanism on Blockchain's model of information security. The job of the Intrusion detection software or systems typically called IDS is to monitor for the suspicious activity in a network and raise an alarm on discovery of either thus, acting like a firewall. Besides, exploring on implementation the work also shed light on existing details of Blockchain's principles, applications and security as well as on the existing mechanisms of Intrusion Detection Systems.

Index Terms: Blockchain, Intrusion Detection, Internet of Things, Information Security, Multivariate Model, Classification

[1*,2,3,4]School of Engineering and Technology, Sushant University, Gurugram, Haryana

Email: meenakshi78gupta@gmail.com

DOI: 10.31838/ecb/2023.12.s3.562

1. INTRODUCTION

Blockchain technology has spread into various areas at a rapid rate since its introduction especially with the advent of Artificial Intelligence technologies like Internet of Things (IoT), Big Data and so on. It's one of the most famous and core application is Bitcoin; a widely known cryptocurrency or digital currency. The applicability of Blockchain has also extended to other fields like Internet of Things (IoT), supply chain etc. As we go into the definition and explanation of Blockchain, we explored through them and compiled it in the most convenient form from our side i.e. it is a chain of blocks where each block contains the details or information like participating peers, time in a transaction and each block is distinguished from other block by a unique hash code generated by cryptography [1]. Its characteristics involved three important keywords i.e. open distributed & decentralized [2]. It means that blockchain is an open public distributed ledger that can record transactions between two parties for a permanent period. Also, this public ledger is placed on a decentralized network i.e. it eliminates the need of a central authority or server. It is worth to mention that this technology was invented by Satoshi Nakamoto in 2008 [3]. Now coming to the concept of Bitcoin, it is an application of Blockchain and the world's first decentralized cryptocurrency. The word 'crypto' is being used because this digital currency uses cryptography to verify transactions and regulate the generation of further units [1]. The formation of a block chain includes the following things: Bits, Nonce, hash Merkle Root, current version number, header and body of blocks. Talking about the Hash Merkle Root it is basically a numeric value which is used to check for the status of transaction. It is obtained after computation by hash values of all transactions in the block body. The transactional records maintained by block body are responsible for generating a distinguished merkle root through hashing process of merkle number. The concept of public key cryptography is also involved in transaction where a private key is used by sender to encrypt the transaction and then sender's public key is used by receiver to decrypt the transaction. Because of the distributed accounting in block chain each participating node stores all transactions recorded in the network. Therefore, accounts will remain secure until all nodes in the network are destroyed thereby keeping the data of accounts safe. Now coming to the concept of consensus, it is basically a protocol responsible for carrying out blockchain operations. The four mechanisms offered for consensus are: authorization share certificate mechanism, equity certificate, workload certification and authentication pool however all of them have different applicability under different conditions such as workload proof consensus is used in Bitcoin.

Blockchain are of three types: Public Blockchain, Private Blockchain and Hybrid Blockchain [3, 4, 5]. In case of Public Blockchain anyone can gain access to the Blockchain platform by just signing in. A single user does not have control over the entire network. The participating user can perform mining, verify transactions, access current or past records and also can perform the proof of consensus for an incoming block. Henceforth, a single person is not the central authority. It is open and transparent. Examples of public Blockchains are platforms like Bitcoin, Litecoin and Ethereum. Now coming to the private Blockchain (also known as Permission Blockchain) has a restrictive model that works in a closed network. Contrary to the Public Blockchain , it involves the role of a central authority who is responsible for deciding to whom the access is given for reading and writing operations in that blockchain. There are specific nodes in private blockchain that are enabled enough to authorize transactions, to give right to create and view. Examples of private Blockchain are Hyperledger and Corda.

Now there is a concept of Hybrid Blockchain where the approaches of private and public blockchains combined. It allows how much data we want to kept private and how much data we want to make public and transparent thereby incorporating both transparency and privacy effectively. Dragonchain is an example of that. The decentralized structure of Blockchain makes its more robust and simultaneously on the other hand, the concept of digital signatures in data exchanges between nodes immunes to its security mechanisms. The implementation of public-key cryptography maintains the authentication and trust mechanism along with the complex hash algorithms. The structure of a blockchain is more like a linked list where there are blocks available in adjacent directions can be traversed easily to check for the past transactions records.

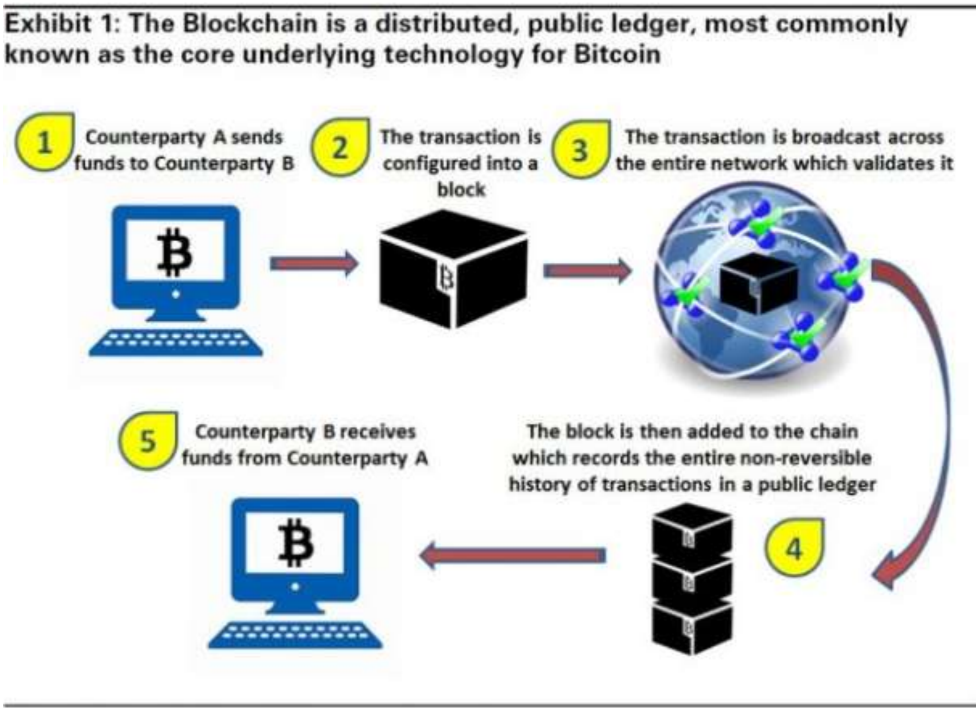
Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin
1 Counterparty A sends funds to Counterparty B
2 The transaction is configured into a block
3 The transaction is broadcast across the entire network which validates it
4 The block is then added to the chain which records the entire non-reversible history of transactions in a public ledger
5 Counterparty B receives funds from Counterparty A

Figure 1. Blockchain Work [1]

2. INTERNET OF THINGS (IOT)

2.1 Concept

“Internet of Things”—the widely used term has got a very simple understanding. As the name denotes it resembles of an infrastructure where all objects or things are connected with the internet. It includes both i.e. communication from one object to another object and communication between humans and objects. So in simple terms we can understand that it talks about an environment where all the components of that environment can interact among themselves as well as to human beings [6, 7]. Thus, the implicit requirement in the implementation of IoT is intelligent processing backed by Artificial Intelligence programming. Henceforth, the notion of Smart Homes, Smart cars and so on derive from this only.

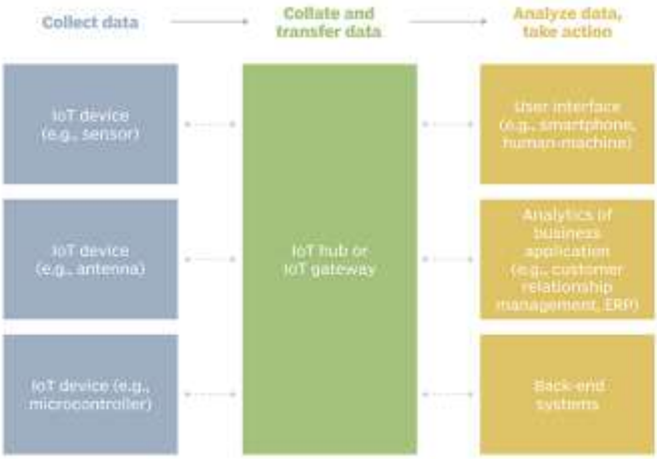
Collect data
Collate and transfer data
Analyze data, take action
IoT device (e.g., sensor)
IoT device (e.g., antenna)
IoT device (e.g., microcontroller)
IoT hub or IoT gateway
User interface (e.g., smartphone, human-machine)
Analytics of business application (e.g., customer relationship management, ERP)
Back-end systems

Figure 2. Sample how IoT works [8]

Now with all these things, some things automatically come along with them and i.e. security challenges and the vast explosion of data. Since IoT talks about everything is being connected with internet that means data will be generated in exponential form within a few seconds (popularly known as Big Data). Now with this, comes the biggest question of privacy and security. Anything available on the internet or part of it can be hacked. One of the major attacks which took place in 2016 in Mirai [8] was a very minute reflection among the security havocs that could generate via IoT platform. And not only the attacks but privacy issues is the biggest concern in this AI push. For instance, the issue of surveillance increases when every other product is connected to the internet.

2.2 Framework

The core framework of Internet of Things lies in the concept of interaction between virtual world and physical world. Now for this concept, we already have a system known as Cyber Physical System (CPS) which is also similar to the IoT, sharing the same basic architecture [9]. So, the whole notion lies in integration of physical world and virtual world maintaining the security and privacy concerns. Since with the expansion of IoT, this concern of security and privacy must be applied in every area like financial services, economics, legal issues, social welfare services thereby to maintain a decorum. The figure given below reflects the concept of integration of virtual and physical world.

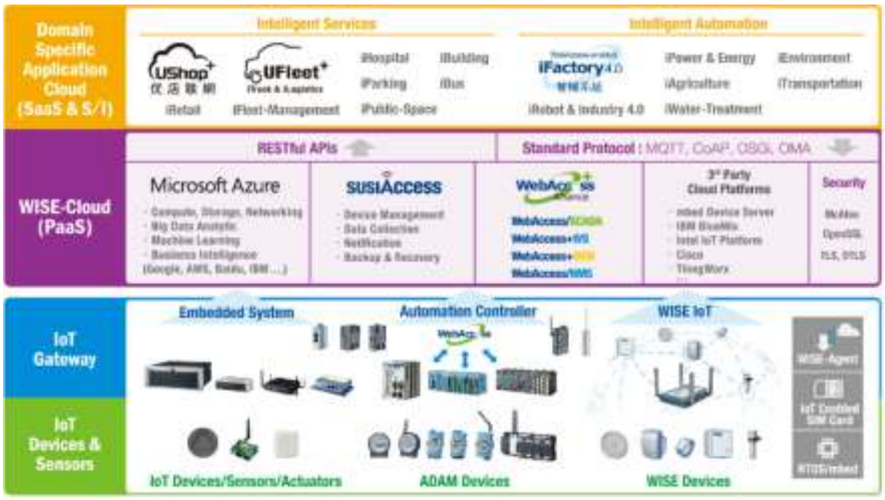

Figure 3. Framework for IoT [7]

Now there are further two categories in IoT namely public IoT and special IoT. Generally, when we discuss about an IoT infrastructure, majorly it is in the context of public IoT. A public IoT is based on the public network systems. The concepts of Smart cities are based on it only. But there is much privacy issues associated with public IoT since data of users can be exploited by third parties in an IoT infrastructure [10]. Special IoTs are much representing the concept of private infrastructure of Internet of Things which mainly includes private networking system. Although special IoTs can also be implemented on a large scale but it will face some interconnection and interoperability problem by some internet of things thus can't fulfill the total projects like smart grid or smart city. Therefore, only public IoTs can suffice the demand of IoT on a large or nationwide level.

2.3 Conceptual Model of Iot

The core conceptual model of IoT focuses on the integration of virtual and physical world as much as possible, thereby promoting internet or information technology environment. Now the challenge lies in implementing this model is the mass delivery of mobile computing services [13]. The answer to this challenge is "sensors – implanted" devices. A 'sensor' is basically any hardware that captures data from the real world. Examples of these sensors include RFID tag readers, bar code reader on PDAs and so on. The devices like our smart phones are just tools which serve as a platform to combine these sensors with the applications and services thereby integrating the physical world and virtual world. Now taking this concept further on next level, we reached to a level of "Informatization and Industrialization" [14] which change the course of civil engineering significantly.

Thus, the model talks about an information technology environment all around us. Actually when we say Internet of Things it is viewed in the context a complete takeover by virtual platforms or complete assimilation of virtual world with the physical world. So from that perspective, at present level it can be said that the present Information Technology infrastructures is partially covered by IoT concept. One thing to mention here is that this ultimate aim or underlying aim of IoT i.e. integration of physical and virtual world requires a range of unique technologies like Cyber Physical System (CPS) technology, Information Technology (IT) and so on. Fig. 5 describes about it.

2.4 Architecture

The architecture of Internet of Things broadly categorized in three layers [7] [15] [16]. First, a layer comprises of sensors and actuators which basically serves as a good for carrying information from the real world. Because it is the prime medium of gathering data from the real world, it is also considered as perception layer. This is at the bottom level in IoT architecture. Second, the layer talks about networking mechanism. This layer is responsible for transmission of data from perception layer to the intelligent applications and that's why it is an important layer since it is acting like a gateway for transferring information. Hence, it also acted as a blended platform because the devices and communication technologies like (RFID, Bluetooth, Wi-Fi) meet at this stage. Also, the network of IoT is not like any other general network rather it is an advanced form of network which is self-configuring, self-optimizing and self-protecting. Third, the layer resembles the cloud services which basically act as a service layer. This is the topmost or we can say is the front-end of IoT. The layer is supported with intelligent applications along with the facility of storage of data. The applications existed on this layer receives information from the network and then perform operations on it accordingly.

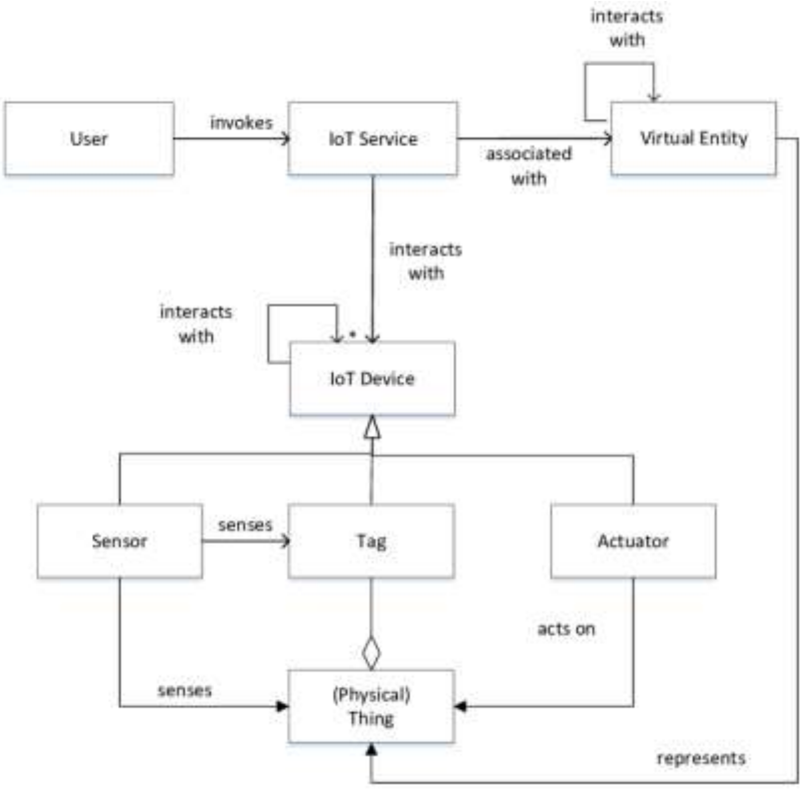

Figure 4. Conceptual Model for IoT [11] [12]

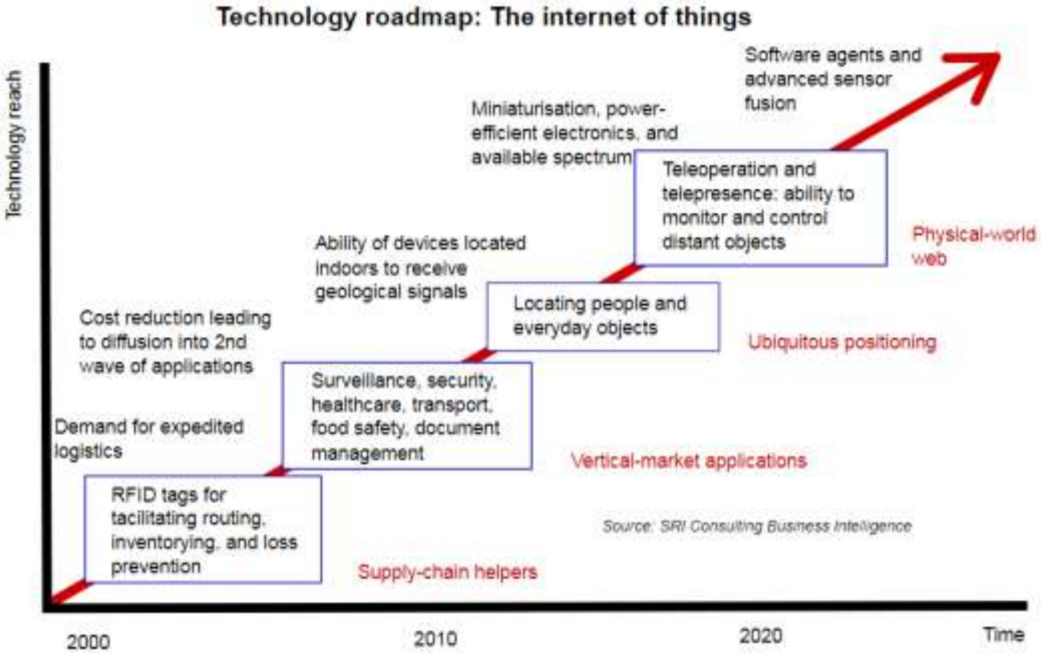

Figure 5. Technology Road Map of Internet of Things [9]

3. INTRUSION DETECTION SYSTEM (IDS)

3.1 Introduction

Intrusion Detection is basically a computer system security mechanism which is used to detect intruders and attacks in any communication system [17]. The objective is to protect the information confidentiality, integrity and availability. As with the evolvement of more and more diversified threats and attacks, the focus on the advancement of intrusion detection mechanism started increasing thereby leading to the development of Intrusion Detection Systems which works at various levels like HIDS (host-based Intrusion Detection Systems) where the focus is on a particular host to detect for any kind of suspicious activity occurring within that host. Similarly, we have NIDS (Network Intrusion Detection Systems) to detect vulnerabilities at network level by observing for unprecedented flow in network traffic, PIDS (Protocol-based Intrusion Detection Systems) to secure the web server by monitoring HTTPS protocol [18] and so on [19]. The IDS checks for intrusion broadly at categories like masquerade, malicious injection, DoS or DDoS.

3.2 From IoT point of view

Now with the proliferation of Internet of Things, the concern of privacy and security goes deeper in computer networks. For example, if the device uses a constant Wi-Fi or Bluetooth Low Energy (BLE) MAC address, it will expose the user identity and location [10]. Furthermore problems which could be addressed are that the information leak in cases like purchasing or shopping on online stores may give an attacker a chance to promote false advertisements to confuse the customers. Currently, the security mechanisms in IoT are maintained by traditional asymmetric key cryptographic techniques (TLS, SSL, and HTTPS). All these security solutions make use of a known MAC address in all communications in a single public IoT space, which leads to the exposure of users' identity. As we discussed above that IoT is an integration point of virtual and physical world, we here add one more point that the devices of real world like car, bulbs have their own significant flaws [20] and this intersection of mature and immature technology results in security problems. The problems like DoS (Denial of Service) attacks in embedded systems are mainly due the incapability of such systems to hold on to the recursive requests by invaders. Also in case of MITM (Man in the Middle) attack the third parties took advantage of weak encryption algorithms of embedded systems. To solve such problems in IoT, work has been done in this regard; the development of a FOCUS [21] platform is being done to send alert messages for the possibility of DDoS attacks. To tackle the insecurity problems in wireless sensor networks, the work in [21] suggest about a real-time intrusion detection mechanism particularly anomaly-based intrusion detection. The anomaly intrusion detection considers all intrusion activities as abnormal. It defines a set of guidelines system for detecting any violation of the described rules or guidelines and considers that particular violation as intrusion. Actually, its implementation involves the concept of a statistical model where a threshold value is being set and whatever events or activities crosses that threshold limit will be considered as an intrusion. The selection of threshold limit must be an optimal value; it should be neither too high nor too low, thus creating problem for security administrator.

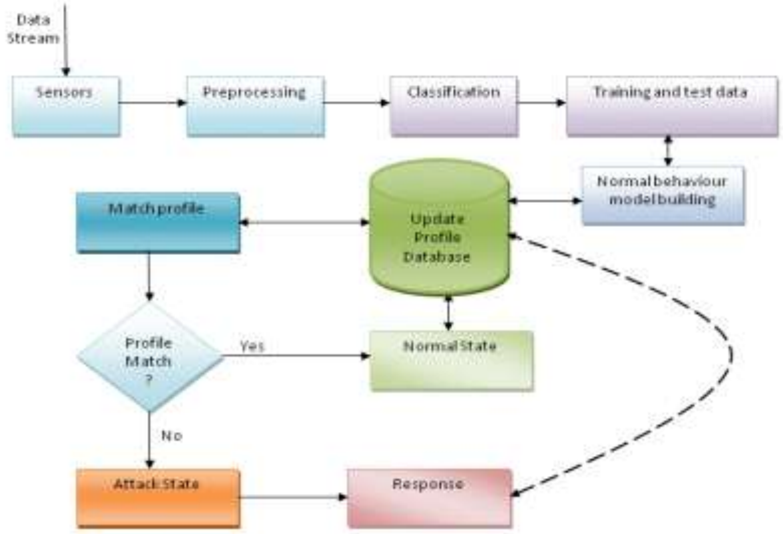

Figure 6. Anomaly Detection technique for Intrusion Detection [22]

3.3 IDS based on mean and standard deviation model

To find a threshold value we can resort to the method of finding mean of the events. Suppose let's say there are 'n' number of events where 'y' is representing a particular event as depicted in equation 1.

$$y = \{y_1, y_2, \dots ., y_n\} \tag{1}$$

Henceforth, now the standard deviation (std) and mean (m) value can be estimated as shown below:

$$m = \frac{y_1 + y_2 + \cdots + y_n}{n} \tag{2}$$

$$std = sqrt(\frac{y_1^2 + \cdots + y_n^2}{n+1} - m^2) \tag{3}$$

Now for any value which will be **Y_{n+1}**, if it lies beyond the threshold limits **(m ± t.std)**, it will be considered as an abnormal activity where't' stands for standard deviation.

3.4 IDS on the basis of Multivariate Model

This model is based on the correlation between two or more than two parameters unlike of a mean and standard deviation model which is based on a single parameter. The Markov model detects for any kind abnormal behavior and counted that as a state variable if found. The concept of state transition matrix is being utilized to denote the rate of occurrence of migration among distinct states. If the result corresponding for a given prior state and matrix is found to be low then the behavior is considered to be as abnormal. Now coming to clustering, as the name denotes is based on the grouping of users' activities as normal and abnormal categories. There is no need of training dataset in case of unsupervised clustering approach and also it does not require any strict filtering mechanism which also reflects a good outcome in detecting intrusion. Now coming to the concept of neural networks we have a network of nodes in it which interacts with each other by adjoining weights. Their processing can be explained in two stages: First, this network of nodes is being trained on a normal system behavior after having done with adjustment of weights among distinct nodes. Second, now this network monitors for the events in the network and accordingly classifies them as normal or abnormal. The advantage in this approach is the elimination of statistical data for decision making but the limitation is in the allocation of weights in network requires a large number of attempts and failures.

3.5 IDS on the Basis of Network

The source of data in a network based IDS is packet of data. The module which is responsible for recognizing the signal of an attack basically consist of four kinds of methods and they are mode, byte frequency, threshold, correlation between low-level events, detection of abnormal behavior based on statistics and once that has been detected , the IDS provides ample opportunities to tackle with an attack. Normally the HIDS (Host Based Intrusion Detection System) is capable enough in detecting any intrusion at application level. It can be combined with the operating system to monitor for any abnormal behavior. Its functioning is mostly similar to the NIDS (IDS on the basis of network).

3.6 Misuses in IDS

One of the deficiency which lies in the IDS is its exposing of the pattern by which it detects intrusion. Once their approach or mechanism got leaked then the IDS got compromised. Any adversary can utilize this opportunity to launch an attack on the system. Because of this limitation only those intrusions could be detected whose behavior found in the database or already stored. To avoid it there are some mechanisms like the use of expert systems where any upcoming intrusion event is being translated or being mapped with expert system rules. These rules then possibly resemble any kind of audit event or intrusion behavior or a series of events. If those events do not satisfy the description rules then the behavior of that particular event is being declared as abnormal. One of the limitations with this technique that it requires timely updating in expert rules.

3.7 Future Scope in IDS

Although IoT has changed the traditional ways of networking at a major level but still the IDS needs a lot of improvement. Till now we have understood that the selection of data plays a vital role in determining any type of upcoming behavior as intrusion hence this concept of selection of data can be integrated with the operating system in a computer to increase its effectiveness. The main challenge which still needs to be resolved is the masquerade attack carried out by adversary in IDS. Also, there should be an evaluation mechanism for the strength of IDS.

BLOCKCHAIN CHALLENGES

There are some advantages and disadvantages that are associated with the blockchain. Its major strength lies in the fact that data stored on it can’t be manipulated but the problem lies in the fact that its size is increasing day by day (for example Bitcoin) along with its applicability giving rise to storage and synchronization problem. The links between various blocks in a blockchain must hold these aspects: (1) as we have observed that the current technologies of blockchain are specific to their domain rather than having general approach of blockchain. Thus, it can be concluded that the blockchain technology is an integration of the existing technology with the general concept of blockchain [23, 25]. (2) It must make use of P2P protocol and the use of asymmetric cryptography simultaneously in order to maintain the availability of data with all nodes and the authenticity of the participants. (3) it must satisfy with the basic building structure of blockchain [26-27]. Problems of synchronization and transaction efficiency need to be resolved. One more major weakness in the structure of Blockchain is lack of privacy. Its openness can give the transactional details of any address. This needs to be addressed.

COMBINATION OF IoT AND BLOCKCHAIN

Now as we are witnessing that BlockChain has been used in various fields like in medical, banking to maintain records because of their non-temper able security perspective and somewhere in this approach an applicability of IoT exist. IoT is nothing but a connection of things via Internet and we can found it in the applications of BlockChain. IoT is having a wide and complex scenario and its applicability varies with the domain and area. The final outcome or conclusion which can be derived from the objective of IoT and BlockChain combination is to build a secure and trustful environment for maintaining records along with the sensitive issue of privacy.

BUILDING OF MODEL

The basis for evaluation of the security of information depends upon various factors like existing domestic and international standards related to it and also upon the associated threat, vulnerabilities of information.

Table 1. Analysis of Risk

Critical points	Damage Degree		
	High(100)	Medium (50)	Low (10)
High (1.0)	100	50	10
Medium (0.5)	50	25	5
Low (0.1)	10	5	1

Risk can be defined as a threat to the information which could be turn into an attack on exposure of vulnerabilities associated. The formulation of the term ‘risk’ accumulates the following parameters: source, medium, approach, receptors and outcomes. Basically, there are two aspects to determine the risk associated with information systems and i.e. degree of damage and vulnerabilities which could be exploited by sources of threat. The table above (table 1) is a depiction of risk analysis where the risk associated with an information system is multiplied by the likelihood of the occurrence and the hazard level. Now it is a 3×3 structure but the size can be increased depending upon the complexity of organization. The estimated risk level resembles the degree of risk.

Table 2. Combination of threat origins, motivational levels and threat behavior capabilities

Threat Level		1(Low)	2(Medium)	3(High)
Threat behavior capability	1(Low)	1	2	3
	2(Medium)	2	3	4
	3(High)	3	4	5

The procedure of risk analysis is described as follows: A blended version of threat origins, motivational levels and capabilities of threat behavior produced a threat level which tells us about the potential of threat as shown in Table 2. Table 3 reflects the chances to exploit vulnerabilities.

Table 3 Combination of Threat level and Vulnerability Utilization level

Threat/vulnerability level	Threat Level					
		1	2	3	4	5
	1	1	2	3	4	5

The level in which vulnerability is exploited	2	2	3	4	5	6
	3	3	4	5	6	7

Table 4 is showing the importance of asset

Asset/impact level	Asset value level		
	1(Low)	2(Medium)	3(Low)
Impact Level	1	2	3
Impact Level	2	3	4
	3	4	5

Now in classification of any kind of intrusive behavior where we classify audit record, the incorporation of more features in classification may lead to more accuracy, but simultaneously we need to deal with entropy.

4. CONCLUSIONS

Authors have discussed the concept of Blockchain along with its structure and characteristics. Authors came acoss over the concept of Internet of Things (IoT) and discussed its complexity along with its features. Also, for the development of a security model for Blockchain suggest the use of intrusion sensing mechanism of IoT in Blockchain to make a secure model for Blockchain's information. Authors also discussed about IDS on the basis of different models. To support discussions authors give the suggestion of a possible model for this approach. However, Blockchain is still in the age of evolution and formation and need much complex issues need to be addressed. The concern of this work was to just highlight the mechanism of Intrusion Detection System in context of Blockchain technology.

5. REFERENCES

1. R. Shaw, "BlockChain Key Terms, Explained", kdnuggets, Nov. 2017. [Online]. Available : https://www.kdnuggets.com/2017/11/blockchain-key-terms-explained.html [Accessed: May. 03, 2020]
2. "BlockChain Explained", investopedia , Feb. 01 2020. [Online].Available : https://www.investopedia.com/terms/b/blockchain.asp [Accessed: May. 03, 2020]
3. W. Contributors, "BlockChain" , Wikipedia, The Free Encyclopedia, Apr 24 2020. [Online]. Available : https://en.wikipedia.org/wiki/Blockchain. [Accessed: May. 03, 2020]
4. T.K. Sharma, "Types of Blockchain in the market: Which one is Better?" , BlockChain Council , Nov. 26, 2019. [Online]. Available: https://www.blockchain-council.org/blockchain/types-of-blockchain-in-the-market-which-one-is-better/. [Accessed: May. 05, 2020]
5. O.S. Hiremath, "Different Types of Blockchain And Why We Need Them" , Edureka , May 22, 2019. [Online]. Available: https://www.edureka.co/blog/types-of-blockchain/ . [Accessed: May 05,2020]
6. M. Burgess, "What is the Internet of Things? Wired explains", Wired, Feb. 16,2018. [Online]. Available: https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.[Accessed: May. 06, 2020]
7. Li, D., Cai, Z., Deng, L. et al., "Information security model of block chain based on intrusion sensing in the IoT environment" , Cluster Comput 22, pg. 451–468 ,2019.

8. M. Rouse, “Internet of Things (IoT)” , TechTarget IoT Agenda, Feb. 2020. [Online]. Available : https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed: May. 06, 2020].
9. W. Contributors, “Internet Of Things” , Wikipedia, The Free Encyclopedia, May 02 2020. [Online]. Available : https://en.wikipedia.org/wiki/Blockchain. [Accessed: May. 06, 2020]
10. A. F. Harris, H. Sundaram and R. Kravets, "Security and Privacy in Public IoT Spaces," 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, 2016, pp. 1-8.
11. Data Distribution Service-Based Architecture Design for the Internet of Things Systems - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Conceptual-model-for-IoT_fig1_322271635 [accessed 7 May, 2020]
12. Tekinerdogan, Bedir & Koksal, Omer & Çelik, Turgay. (2017). Data Distribution Service-Based Architecture Design for the Internet of Things Systems. 10.1007/978-3-319-70102-8_13.
13. Barton, John & Kindberg, Tim. (2001). The Challenges and Opportunities of Integrating the Physical World and Networked Systems.
14. Yao, Fuyi & Ji, Yingbo & Li, Hong Xian & Liu, Guiwen & Tong, Wenjing & Liu, Yan & Wang, Xiaowei. (2020). Evaluation of Informatization Performance of Construction Industrialization EPC Enterprises in China. Advances in Civil Engineering. 2020. 1-18. 10.1155/2020/1314586.
15. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.
16. Bahrani , “What is IoT(Internet of Things)? IoT Architecture Explained”, Edureka , May. 22, 2019. [Online]. Available : https://www.edureka.co/blog/what-is-iot/. [Accessed: May. 09, 2020]
17. Aloqaily, Moayad & Otoum, Safa & Al Ridhawi, Ismaeel & Jararweh, Yaser. (2019). An Intrusion Detection System for Connected Vehicles in Smart Cities. Ad Hoc Networks. 10.1016/j.adhoc.2019.02.001.
18. Pp. pankaj, “Intrusion Detection Systems”, GeeksforGeeks . [Online]. Available : https://www.geeksforgeeks.org/intrusion-detection-system-ids/. [Accessed: May. 10, 2020].
19. D. Rom, “Five Major Types of Intrusion Detection Systems (IDS)” , SlideShare, May 12, 2016. [Online]. Available : https://www.slideshare.net/davidromm/five-major-types-of-intrusion-detection-system-ids [Accessed: May 10, 2020]
20. O. Mavropoulos, H. Mouratidis et. al , “A Conceptual Model to Support Security Analysis in the Internet of Things”, Computer Science and Information Systems,14(2), pg. 557-578
21. Costa, Kelton & Papa, João & Lisboa, Celso & Munoz, Roberto & Albuquerque, Victor. (2019). Internet of Things: A Survey on Machine Learning-based Intrusion Detection Approaches. Computer Networks. 151. 10.1016/j.comnet.2019.01.023.
22. A Hybrid Mitigation Technique for Malicious Network Traffic based on Active Response - Scientific Figure on ResearchGate. Available from:https://www.researchgate.net/fi

gure/Anomaly-Detection-Technique-for-Intrusion-Detection-Figure-2-depicts-the-anomaly_fig2_282273622 [accessed 12 May, 2020]

23. Zhang, Y., Wang, H., Xie, Y.: An intelligent hybrid model for power flow optimization in the cloud-IOT electrical distribution network. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1270-0
24. Anwar, S., Mohamad Zain, J., Zolkipli, M.F., Inayat, Z., Khan, S., Anthony, B., Chang, V.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms 10(2), 39 (2017)
25. Haider, W., Hu, J., Slay, J., Turnbull, B.P., Xie, Y.: Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. J. Netw. Comput. Appl. 87, 185–192 (2017)
26. Sedjelmaci, H., Senouci, S.M., Ansari, N.: Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology. IEEE Trans. Intell. Transp. Syst. 18(5), 1143–1153 (2017)
27. Cai, Z., Deng, L., Li, D., et al.: A FCM cluster: cloud networking model for intelligent transportation in the city of Macau. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1216-6