An Approach of Intrusion Detection Using Blockchain Security Prototype in IoT

R K Chandana Mani
Assistant Professor, Mother Theresa Institute of Engineering & Technology
(E-mail: rkchandana510@gmail.com)

***Abstract*— Internet of Things (IoT) is one of the most trending technologies that providing the services ranging from tactical military to health car. Although Internet of Things has few lack of advanced features, due to the lack of a physical line of defense, the security of such IoT networks is a big challenging task, especially for the applications where privacy have major importance. Therefore, in order to provide robust IoT networks in a privacy way, any kind of intrusions must be detected before attackers can hack the network. In this paper, a review of the state-of-the-art in Intrusion Detection using Blockchain technologies that are proposed for IoT networks is elaborated. At first, clear information is provided about Internet of Things, intrusion detection and Blockchain technologies. In next stage, presented a brief review of intrusion detection suggested for Internet of Things and reliability of those systems to IoT networks are presented. In next section, how blockchain technologies gives strength to intrusion detection system are presented. This is section is explains about comparison and analysis of each method. Finally, explained about intrusion detection systems that are reliably applicable to IoT networks are provided. This review is concluded by providing research challenges in the field of IoT for researchers**.

***Keywords*—** *Blockchain, Collaborative network, Internet of Things, Intrusion detection, Security and Trust management.*

I. INTRODUCTION

Due to their flexible and easy deployment applications, Internet of Things (IoT) are using in different kinds of fields like technology and science: To collecting the data from several devices and different fields, such as highway traffic, reconnaissance, military surveillance and health care; to observe the environmental and physical observations, like earthquake, ocean and wildlife, water quality, pollution, agriculture, wild fire; to observe industrial lands, like manufacturing machines status, building safety and so on [1]. On the other side, privacy and security in Internet of Things networks is a challenging issue, particularly networks have challenging tasks. For example, a confidential one country military records should not be passed to other countries in a military network application. Providing privacy and security for IoT networks is a challenging and important in cyber department applications where a privacy gap in the IoT network might cause several problems in a cyber-world. Researchers who are doing research on privacy and security in Internet of Things, has to focus on real-time problems for providing privacy and security networks.

Hacker attacks in IoT networks are classified into two main ways: Passive attacks and Active attacks. In passive attacks, attackers are hidden and hacks the information link to collect data and collapse the important elements of the IoT networks. Passive attacks can be classified into node malfunctioning, eavesdropping, traffic analysis types and node tampering/destruction. In active attacks, hacker affects the functions in the attacked IoT networks. This function may be the main goal of the attack and can be identified. For example, the IoT networking services may be terminated or collapsed due to the result of these kind of attacks. Active attacks can be classified into DoS attacks, hole attacks flooding, jamming, and Sybil types. Researchers who are doing research on privacy attacks and security attacks in Internet of Things, has to focus on this kind of attacks for understanding privacy attacks and security attacks in IoT networks.

Suggestions to active attacks and passive attacks against IoT networks has three ideas:

- Prevention: The main aim of this method is to prevent any hacker attack before it attacks. Any solution has to face against the opponent attack.
- Detection: If hacker handles the functioning taken by the above step, which means there is a failure to face against the hacker attack. In this situation, the second solution would search for the detection phase of the hacker attack in process and particularly identify the cluster nodes that are compromised.
- Mitigation: The last step is to mitigate any hacker attack after it happens by vanishing the routing tables which are affected the cluster nodes.

Intrusion is an unwanted behavior in an IoT network that is either achieved actively or passively. In a privacy and security system, the first priority is intrusion prevention, in case if we does not prevent intrusions, then the second priority is intrusion detection. It is the identification of any malware activity in an IoT network performed by the unauthorized network members. In the next step, intrusion detection systems provide the following functions to the IoT networks systems: first step is detecting of the intruder, location of the intruder, time of the intrusion. In the next step, identification of intrusion activity like whether it is a passive attack or active attack. In third step, identification of intrusion type like whole attack etc., next identification of network layer where the intrusion attacked like physical layer, data link layer etc. All

this information would be very useful for mitigation process. So, these are all steps very helpful for intrusion detection systems.

Internet of things has advanced features at the same time has few limited characteristics such as low transmission bandwidth, limited power supply, data storage and small memory size. Because of these limited features of IoT networks, many of the privacy and security methods for traditional IoT networks are not deployed to a IoT environment. Developing efficient and effective intrusion detection technique with the help of blockchain technologies that is most useful to IoT networks but this is a challenging task, this problem statement motivated us to work on this research field. Blockchain technologies are synchronized and shared across a network which can be used for distributed blocks of transaction records. Blockchain technology adds the more strength to the IoT networks to detecting the intruder. This survey is first step of our research is to build the state-of-the-art.

The rest of the paper is organized as follows: In Section II, a brief introduction of Internet of Things, Intrusions and Blockchain technologies. In Section III mentioned related work of security and privacy issues of IoT networks. Section IV presented about how blockchain technologies adds more strength to IoT networks. Finally, our survey paper is concluded by existing methods, focusing their weaknesses and providing a solutions for IoT networks that would be helpful for IoT environments.

II. BACKGROUND

A. Internet of Things (IoT)

The internet of things is functionally a multiple connected things like devices, as well as a feature of the next generation of wireless networks. As the development of internet of things have not yet be finished in abroad and developing countries, both industry and academia do not fully developed the advanced version of internet of things, and due to the lack of facilities, sources and information of the internet of things. The Internet of Thing is a new feature based on the connected network and ubiquitous network computing, it can be connected through a different kinds of wireless and wired networks and integration of internet, collection of several sensors, intelligent automation features, GPS, to receive the features of internet of things and people everywhere to receive the information from connected networks. Internet of Things will develops the technology and robustness to industries, it will be add the future economic development, social progress. Technological development is the key feature infrastructure. Internet of things technology is developing very fast, at the same time privacy and security of internet of things network is becoming more and more challenging. For example, Stuxnet virus is the one kind of malware, this is the one kind of intrusion attack in intrusion control of the malwares, the malwares in the form of worms in the IoT networks attacks. The hackers attacked Iran natanz uranium enrichment plant, causing about 20% of Iran's centrifuge control, scrap, lead to power delay. The security in internet of things is a primary challenge in the area of information technology. It is identified as the major problem of information technology industry. The basic characteristics of internet of things are comprehensive reliable transmission perception, and intelligent processing of collected data. The main concept of internet of things is the interaction among the objects and information among objects and human beings.

The IoT systems has been developed and several features in WSN (wireless networks) has to be changed in order to totally integration of devices in the IoT environments. Figure 1, represents a basic architecture of IoT as also tackled by the IoT European research project. In this model at each layer performs the services and functionalities to offer the services to users. At first layer, all multimedia devices are connected with each other under a network and share the data with other to take appropriate decision by each multimedia device. The next layer, IoT services and resource layer provides the search and discovery functionalities. By using this feature, each and every multimedia device provide data to a single specific device instead of restriction. At this layer, IoT services and resources shares with each device which are interconnected to network and on the other hand, devices maintains resource history storage details and service resolutions. In next layer, virtual entities are introduces with the main aim of counterpart of the physical devices. These virtual devices can be useful for efficient resource management in IoT network and virtual resources shares the storage memory with each device which are interconnected to network and on the other hand, virtual devices maintains resource history storage details and service monitoring. In the next layer, service will be executed and orchestration. All processing functionalities will be executed at this layer for processing multimedia device data. In the final layer, applications will provide the information to users. From bottom to top, collected data will be processed and sending to further layers. Finally, application user will receive the information at application layer which is works like user interface panels.

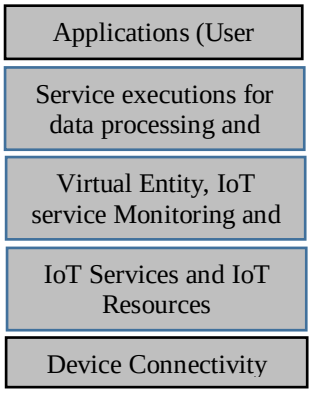


Fig 1: IoT architecture in the view of processing

Figure 2, presents the major advantages of Internet of Multimedia Things which is major applications of a middleware platform. This architecture involved with multimedia connected devices generation and the complexity. Smart intelligence systems makes the flexibility in real-time world and providing more benefits users daily life.

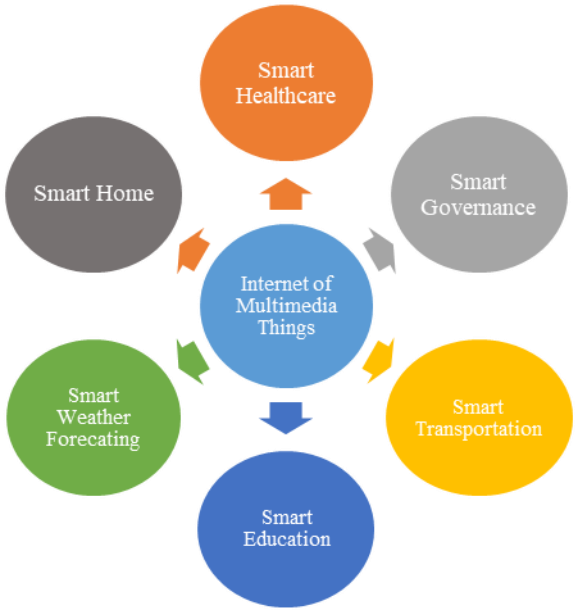


Fig 2: Applications for Internet of Things

B. Blockchain

With the enhancement of Internet and mobile technology and the development of analytics and big data computing technologies, the chain management has introduced in technology, and its enhancement would not be distracted from the information flow, capital flow. Bitcoin was introduced in Information Technology in 2008, bitcoin is a digital currency which is encrypted system introduced to the financial fields. This is the main cause of developing the blockchain technologies which was introduced in 2016, the features of block chain technology has adopted into many other research fields like automation technologies, intelligent manufacturing, internet of things, supply chain management etc. Block chaining technology is considered as the advance of the next generation cloud computing technologies.

Now a days, the block chain has not having static definition. Few industries mentioned that the chain of blocks is developed, managed and shared by each member of the network, and blockchain technology has the decentralized characteristics. Blockchain technology is a advanced technique of chain management system, it is adopted by bitcoin currency for providing the privacy, while promoting the blockchain researchers will often using the bitcoin currency, but fact is bitcoin is completely differs with blockchain technologies. The blockchain technology providing the privacy and security for crypto currency. Blockchain is working based on the cryptography and it's not taking any credit of bitcoin. In payment methods, with the help of blockchain technologies can make payments directly without interaction of third party payment services. Here bitcoin is a most successful feature of the block chain technologies and it is not equivalent to the blockchain technologies.

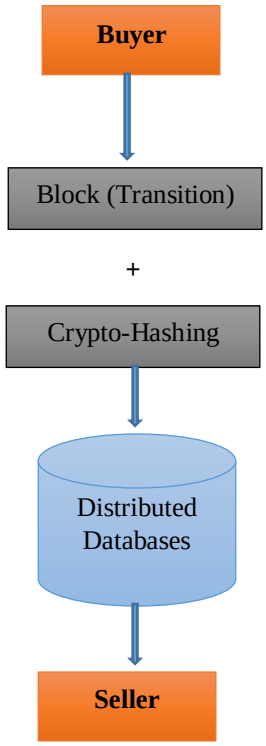


Fig 3: The Process of Blockchain

The blockchain technology is a trusted, secure, and decentralized distributed database. In other words, blockchain technology is a distributed management system which maintains the database to store the all transactions in the view of records. The most advanced privacy and security of the blockchain as an advanced security application technology, has become a most privacy of digital crypto currency. Blockchain technology is not a unique methods innovation and integration, it is a combination of several technologies like cryptography, mathematics, economic model technology and algorithms. This integration of several technologies with new architecture integrated together to develop a data record and store. The main concept of blockchain technology mainly has the following features. A blockchain is developed by exchanging the data records which consists of header portion and body portion. The main portion consists of current version number i.e. hashPrevBlock, hash value, consensus process, time stamp and node hash value. The blockchain technologies taking the advantages of distributed communication, distributed accounting, and distributed storage. These technologies helps for data-storage, verification of transactions and transmission of information in the blockchain management system. Advanced powerful computing technologies helps to the blockchain technologies like do not

tampered. Blockchain technology is classified into three approaches such as public blockchain approach, private blockchain approach, and finally union blockchain approach. In the public blockchain approach no official blockchain management mechanism, no organization and no centralized server. The group any individual or alone can be changed as the node based on the regulations of free network system. In this process, any group node can send the transaction details and which can appear the blockchain confirmation and anyone can participate in the process. The public blockchain approach is the first blockchain technology and is also the most useful blockchain approach at present situation. The digital crypto currency of the bitcoin system is developed based on the public blockchain approach. The private blockchain approach is developed by the private organization and this approach having separate rules are set based on the organization requirements. Write and read access is very limited for nodes, but only can use the blockchain ledger technology, like other distributed storage mechanisms. The union blockchain approach in between the private blockchain approach and the public blockchain approach. It's a selected nodes are designated as counting persons within a management group. The creation of each block is obtained by all the selected nodes. The selected nodes contributes in the consensus process and remaining nodes can contribute in the transactions.

C. Intrusion Detection System

The Intrusion detection system is a most key feature to provide the security and privacy of information systems. The intrusion detection system has become the important feature of the security and privacy research in recent time.

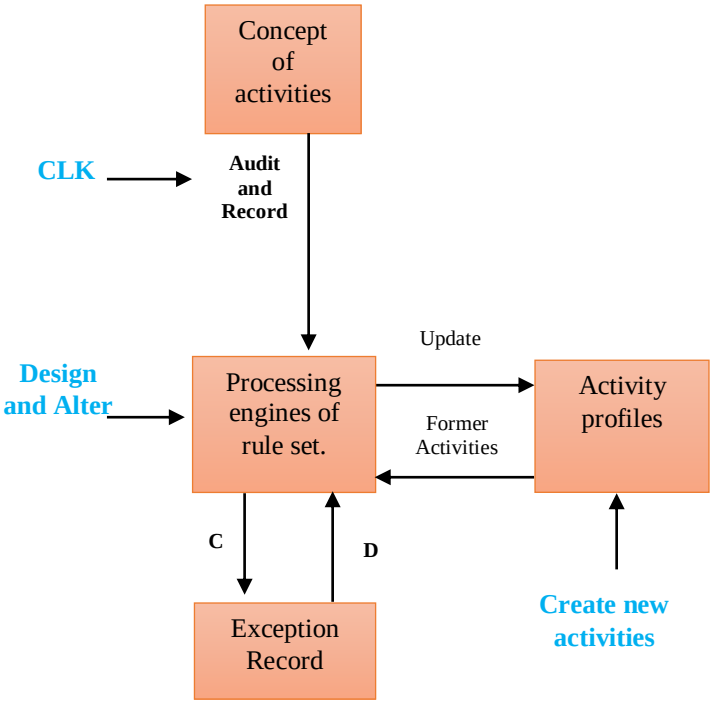


Fig 4: Intrusion Detection System

This section represents the brief information of intrusion detection system, explains the how intrusion detection system works in IoT networks and also represents of basic intrusion detection system, and discussed importance of intrusion detection system technology. With the advanced extension of IoT networks connections and communications, more chances are there to threaten by intrusion attacks. So, the privacy and security of the IoT network systems, the IoT communication system and the complete infrastructure has become a major challenging task. Also the traditional privacy and security technologies, another challenging research problem in privacy and security field. Data is the primary thing, and the privacy and security of collected data system is a major issue. Intrusion detection is the one of an advanced process of active and major topic of IoT networks security. In 1980s Aderson introduced the concept of intrusion detection system. At first the intrusion detection was used for security purpose of defense of computer system. Later this technology is adopted in networks to detect the malicious attacks and to identify the intrusion has become more challenging and diversified, but this intrusion detection systems helps to detect intrusions in the area of information security. The development of the intrusion detection system technology in information security system a lot. This intrusion detection system has several stages such as intrusion detection system of host and network based intrusion detection system, the distributed intrusion detection system and network intrusion detection system. Figure 4 [12] represents the intrusion detection system in information security systems. In this architecture, the processing power of rule set defines the rules for network management systems to provide the security and privacy systems. Here C and D denotes create and draw the records.

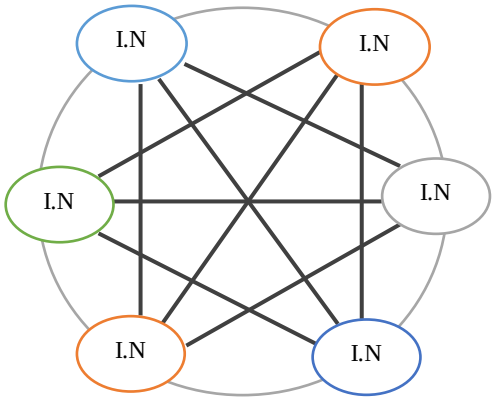
III. RELATED WORK

This survey on basically has done about how blockchain technologies improves the intrusion detection system in IoT networks and it is elaborated on different kind of technologies like internet of things and blockchain to enhancement the collaborative intrusion detection system. Many authors have presents the survey about IoT and blockchain technologies but the problem of integration of intrusion detection system is not given the proper solution. We have done some review work that related to three advanced technologies such IoT, blockchain and intrusion detection systems. Aazam et al. [8] represents a solution for integration of intrusion detection system known as "secured selecticast", which can be used for centralized distributed system. This system receives the records of malware IP addresses and gives the alerts for malware IP addresses to every user in the network. For privacy and secure information routing, to generate hashed alert creates the bloom filters. These all alerts can be maintained by central repository and main server repository for each user for bloom filters, at the same time master Bloom filter for working up the identification process. But in this system two main limitations are there such as, a centralized server repository was used in the proposed model, it can become a failure at a central point. Second issue is bloom filters generates wrong positives. In this work "secure selecticast" of its integration mechanism, focused on the suspicious evidence among users. L.N. Sun [10] presented network-to-network intrusion detection system to

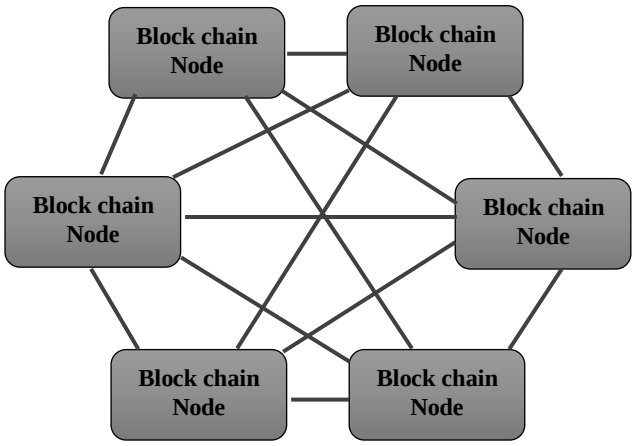
increase the privacy and security in a communicated networks, they used bloom filters for enhancing data privacy, and a advanced overlay network is mainly used for distributed systems. This kind of work mainly focused on effective data exchange policies, which are developed by a distributed correlation system scheduling algorithms. This method also creates the issues for false positives due to by using traditional security algorithms. Caron [12] is a proposed decentralized detection algorithm service which is deployed on PlanetLab. Geographically located applications uses centralized intrusion detection systems are obtained to identify malware attacks. Authors has done process by parallel by decentralizing the privacy keys over the entire networks dynamically constructed by traditional security algorithms. These two solutions are completely different but both authors had used traditional security algorithms. Caron [12] is developed the method for intrusion detection, while L.N. Sun [10] developed algorithm for identification of denial-of-service attacks. Here three constraints are there to identify malware attacks such as prevention, containment and vanish. Caron [12] mainly focused on detecting the malware nodes while L.N. Sun [10] focused on the prevention. Netbait is followed processing query system for intrusion detection in data using methods to detect worm. It explored the processing query over the networks. L.N. Sun [10] proposed content-based centralized system. Netbait presented decentralized method object by using location routing and used a distributed hash table. The Daming [13] proposed a solution for an integration intrusion detection system to provide a decentralized view of the intrusion detection systems. Weighi [14] is another solution of decentralized distributed application and centralized correlation. Chenfeng [15] is a peer-to-peer intrusion detection system which uses a neighborhood watch mechanism between trusted peers to share suspicious activity and gives the solution for decentralized method object by using location routing and used a distributed hash table.

IV. BLOCKCHAIN SOLUTIONS FOR IOT NETWORKS

By introducing the blockchain technology in a IoT networks which can improves the potential power IoT networks and blockchain technology is a distributed ledger and decentralized that improves the storing each record of transactions in a IoT networks.



(a)



(b)

Fig 5: Processing of IoT and Block chain

This block chain technology can be deployed in a network-to-network without another trusted third party. This block chain technology integration can be enhanced by advanced cryptography methods, making it more securable to communicate by any user in network. Because of the block chain technology, can improve the network communication such as advanced technology for providing the solutions for as mentioned above challenges in related work intrusion detection system.

A. Data Exchange among networks

The data exchange among network method is mainly focused on two constraints such as data privacy and mutual trust. Data privacy method presented that the exchanged information may having some data which is related of one organization, like network traffic which includes IP addresses of networks and packet payloads information which can be used to identify the security and privacy of an organization. Mutual trust means that when exchanging the information, integration organization has to trust others who are not owners of organization data. For example, two IT companies wants to make an agreement that they does not want to share the information with other organizations. Blockchain technology is one of the advanced solution that can be integrated to IoT networks to avoid this issue. Such as, data exchanging can be treated as a collection of transactions. At first stage integrated organizations should make a data exchanging agreement, which digitally agreed by each organization. After, this agreement will be recorded in a blockchain node, which is unalterable and public. In this situation, other organizations can receives the blockchain node, see the agreement then gives the confirmation of permission of the exchanged data. Such recorded displaying of the agreement confirms that one organization should not see without permission. Likewise feature of blockchain technology in the healthcare system, creates an open accounting system is creates to offer trust among different integrating organizations. For information security, another solution is to exchange transformed information instead of raw data. Likewise, if integrating first

party wants to validate the performance of their developed classifier based on the information from second organization. Based on the the data exchanging agreement, first party can record the classifier into the blockchain node, later second organization can access the classifier, execute it locally with the received information and sending the result to first organization. In this situation, second organization records the privacy information of the collected data. For data exchanging problem, blockchain technology can help develop mutual trust among organizations and this technology as a permanent ledger of among data owners.

B. Trust management

Integration of many networks can be categorized as distributed, centralized and hierarchical. In related work, centralized distributed architecture has been surveyed, while the other has to facing difficulties from privacy, security and scalability and these issue are due to one point of failure. For IoT communication networks, generating alert sharing is primary thing among different intrusion detection system nodes, these nodes can be used to help detect whether there is suspicious user or not. Additionally, alert sharing can be used to integrate the trust of a blockchain nodes within the IoT networks. For example, in IoT communication network the trustiness of a blockchain node could be integrated based on the permission of received alert data. This kind of architecture develops the robustness against few malware attacks like hole attack and betrayal attack. Blockchain technologies providing a potential power to IoT networks. For example, blockchain based IoT network, which used blockchain technology for improving privacy and security among intrusion detection system nodes. Particularly, blockchain nodes alerts the connected nodes generated by each intrusion detection system node as a records in a blockchain management. Later all integrating blockchain nodes takes the advantages of a consensus protocol to provide the validation of the stored records before saving them in a blockchain nodes.

V. FUTURE DIRECTIONS

As an advanced integration of technologies, blockchain and internet of things will increase the privacy and security in IoT networks, due to robust capabilities of domains. This integration of two technologies to validation itself with many advanced concept improvements. In the research area of intrusion detection system in IoT networks, blockchain technology can improve the privacy and security.

A. Data Exchange in IoT networks

Generally, blockchain nodes are works effectively to handle the recording of node information such as transaction processing and medical records. In bigdata environment data analysis is a major problem for a large centralized intrusion detection system or IoT network. So, blockchain technologies has a potential power to enhance the performance while increasing security and data privacy among integrating IoT networks.

B. Alert Share

Blockchain technology secures the malware alerts developed by different blockchain nodes and confirms only trusted alerts would be exchanged among IoT networks. But, due to the lack of real-time applications, it is an important step and an interesting and for future research improvements.

C. Trust Management

Few integrated intrusion detection systems using warning alerts to validate the trustiness of users. Blockchain technologies can gives the solution to improve the process of trust management. For example, developing blockchain technologies in IoT networks based on intrusion detection approaches to validate whether the received alert information is validated or not.

VI. CONCLUSION

Blockchain technology is a major improvement for decentralized transactions which are used in online transaction market and secure data management without the need of a trusted third party. Blockchain is an open source and distributed ledger which providing the records of online transactions among different networks in a valid way. So, integration of IoT and blockchain technologies provides secured network for crypto currency transactions and also it helps for supply chain management and healthcare systems, but still so much work have to be done to improve the potential of IoT application in the area of intrusion detection systems. To increase the growth of this research, this review work has discussed the potentiality of blockchain technology to solve the issues of data management and trust computing in integration of blockchain and IoT environment. We have discussed that blockchain technology have a potential power to improve the intrusion detection system.

REFERENCES

[1] Abadi DJ.Data management in the cloud: limitations and opportunities. IEEE Data Eng Bull2009; 32(1):3–12.

[2] Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R. Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. CoRR, vol. abs/ 1306.4956, 2013.

[3] Achanta V,Sureshbabu N,Thomas V,Sahitya M,RaoS. Cloudlet-based multi-lingualdictionaries. In: 2012 3rd international conference on services in emerging markets (ICSEM), December 2012.p.30–6.

[4] Kupferman, J., Silverman, J., Jara, P., Browne, J., 2009. Scaling into the cloud. CS270 - ADVANCED OPERATING SYSTEMS.

[5] Yang, Q., Peng, C., Zhao, H., Yu, Y., Zhou, Y., Wang, Z., Du, S., 2014b. A new method based on PSR and EA-GMDH for host load prediction in cloud computing system. J.Supercomput.68 (3), 14021417.

[6] Sheeraz A Alvi et al., Internet of multimedia things: Vision and challenges, *Ad Hoc Networks* (2015).

[7] Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Maasberg, M., Choo, K.-K.R., Multimedia big data computing and Internet of Things applications: A taxonomy and process model, *Journal of Network and Computer Applications* (2018).

[8] M. Aazam and E.-N. Huh, Fog Computing: The cloud-IoT/IoE middleware paradigm, IEEE Potentials, vol. 35, no. 3, pp. 40–44, May/Jun. 2016.

[9] Y. Sahni, J. Cao, S. Zhang, and L. Yang, Edge mesh: A new paradigm to enable distributed intelligence in Internet of Things, IEEE Access, vol. 5, pp. 16441–16458.

[10] L.N. Sun, Building intelligent parking lot based on RFID and cloud computing technology, in: Proceedings of International Conference on Mechatronics and Semiconductor Materials (ICMSCM 2013), Xian, Peoples R China, SEP 28-29, 2013, pp. 1550–1553.

[11] Internet-of-Things Architecture (IoT-A) Project Deliverable D1.2 – Initial Architectural Reference Model for IoT.

[12] Caron E, Forecasting for grid and cloud computing on-demand resources based on pattern matching. In: Proceedings of the IEEE second international conference on cloud computing technology and science. IEEE; Indianapolis, IN, 2010, .p.456–63.

[13] Daming Li et.al., Information security model of block chain based on intrusion sensing in the IoT environment, Cluster Computing, 2018.

[14] Weighi et.al., When Intrusion Detection Meets Blockchain Technology - A Review, Special Section on Research Challenges And Opportunities In Security And Privacy Of Blockchain Technologies, 2018.

[15] Chenfeng et.al., A Peer-to-Peer Collaborative Intrusion Detection System, IEEE, 2005.

[16] Zheng, X., Ge, B.: The evolution trend of information management of supply chain in China under the information environment. Inf. Sci. 10, 128–133 (2016).

[17] Ping et.al., Chinese Block Chain Technology and Application Development White Paper. Ministry of Industry and Information Technology, Beijing (2016).

[18] Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc, Sebastopol (2015).