Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019)
IEEE Xplore Part Number:CFP19OSV-ART; ISBN:978-1-7281-4365-1

Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy

Shashvi Mishra,
School of Computing Science and Engineering,
Vellore Institute of Technology, Chennai Campus,
Chennai, 600127, Tamilnadu, India,
shashvimishra@gmail.com

Amit Kumar Tyagi
School of Computing Science and Engineering,
Vellore Institute of Technology, Chennai Campus,
Chennai, 600127, Tamilnadu, India
amitkrtyagi025@gmail.com

Abstract: Data security plays an important role in the healthcare monitoring systems, where critical patient data is transacted over the internet especially through wireless devices, wireless routes such as optical radio channels, or optical fiber-related transport networks. In one way or the other every device is connected to internet and we address such things as internet connected things. As the network is moving towards wireless applications, the threat to attack is also becoming a crucial issue. These attacks can be identified through various intrusion detection techniques and some of which were discussed in the previous decades. The intrusion detection technique is used to identify the privacy breach in the network. Its main purpose is to detect the unauthorized access. Some of the systems or networks that need protection are part of wireless networks (Things connected to internet). Wireless network applications comprises of WLANs (Wireless Local Area Networks), WPANs (Wireless Personal Area Networks), ad hoc networks etc. Since digitization is taking place in each and every sector and so the threat to data also exist. In this article, we protect IoT based E-healthcare systems by using a novel concept called "Blockchain Technology".

Keywords: **Wireless sensor networks, Intrusion detection System, Internet of things (IoT), Security in e-healthcare systems, Blockchain technology.**

I. INTRODUCTION

The Internet Connected Things (ICT) is one of the largest evolutions in the field of computing. The occasional accessibility of lots of these devices in this huge heterogeneous community (network) will make it difficult to holistically (means that devices are connected in such a way to each other that they cannot set apart, it can only happen when a device as a whole gets disseminated) screen information go with the flow. Nonetheless, to shield networks, unauthorized intruders should be detected within the constraints of each sort of tool or subnetwork earlier than any gadget data may be intruded. Intrusion detection is an important research topic for providing authentication to various smart devices [1]. Along with intrusion prevention, reaction and tolerance, intrusion detection is one method which could defend towards the real cyber-attacks threatening important systems.

IDS (Intrusion Detection System): Intrusion detection is the technique which helps to notify or signal if some intruder has breached privacy somewhere and in reaction to that either that intruder is blocked or the sever at which the attack took place gets blocked. Currently, Intrusion Detection System (IDS) is classified further into two categories:

- Network Intrusion Detection System (NIDS): The term network means for the whole network and all the devices come under that network. These NID systems are set up at a fixed point in a network for monitoring traffic from all devices.
- Host Intrusion Detection System (HIDS): The term host means that the detection process runs for only a single host (computer, laptops etc.). These systems work on independent devices in a network. It examines incoming and outgoing packets and sends a warning through alarm if any malicious activity is encountered (refer figure 1).

A small comparison is made on the analysis techniques:

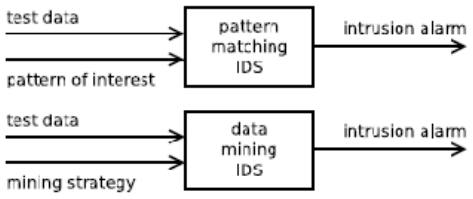

Figure 1: Comparison on the basis of Analysis Techniques

Wireless Sensor Networks (WSNs): Wireless sensor networks are low cost and easy established networks [2]. They are built upon small sized, self-operable nodes known as sensor nodes. These nodes can be used in any many applications/ sectors like military, healthcare,

topology detection etc. These nodes maintain a topology by sensing the networks and then work on the scenario further by using any routing protocol. Security is a major concern (issue) for all type of networks, mobile networks, wired and wireless networks or ad-hoc networks. As WSN is widely being used today so there is requirement to secure transmission of reliable packets. Using IDS-based mechanisms in the sensor networks can be very effective. These detection systems can detect the abnormal behaviour of the sensor nodes such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In IDS, the unit that analyses the network and detects the abnormal behaviour of node(s) is called an IDS agent. Though in the field of sensor networks IDS is still new area and further research is going on. Various researchers have provided their surveys for the detection of the anomalies on the same.

Internet Connected Things or Internet Enabled Things: The Internet of Things (IoT devices) is a gadget of interrelated computing object, mechanical and virtual machines, objects, animals or human beings which can be furnished with specific identifiers and the potential to transfer statistics (data) without requiring human-to-human or human-to-computer interaction [15, 16]. In the same way, taking healthcare into context, medical internet of things is the collection of devices connected to the internet to perform processes supporting the healthcare application. Medical Internet of Things (MIoT) [3] has emerged as a brand new era in e-healthcare sector that gathers crucial body parameters of patients and monitors their physical or mental information with the aid of small wearable gadgets or implantable sensors. MIoT has shown extremely good potential in imparting a higher assure for human's health and supports an extensive variety of applications from implantable clinical devices to Wireless Body Area Network(WBAN). Figure 2 shows the current structure of healthcare application enabling IoTs devices.

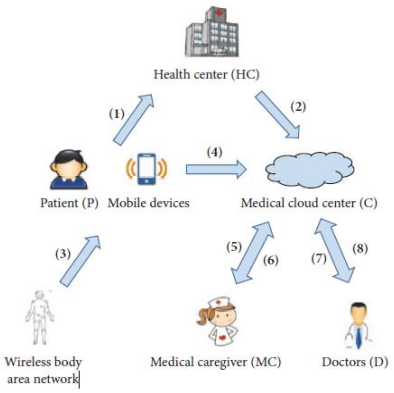

Figure 2: Connection of Wireless Sensor Network with Patients [3]

This is the small description of how patient is operated with the help of wireless sensor networks and the connection is established between the patient and the doctor (refer figure 2). As we know, the cost of our basic needs are gradually increasing day by day and our healthcare amenities are at great hike and as it is the basic need for each and every human being so people have to get access to that at every cost. Otherwise, a large section of the society will become unproductive. Though the technology cannot stop the people from getting sick or gain ageing, what technology can do is to make availability of healthcare handier. It can happen by making the medical facilities easily accessible. Some of the benefits are listed below as:

- Simultaneous reporting and monitoring: Through real-time monitoring of the condition in place through a smart medical device linked to a smart phone app, connected devices can collect clinical and other health data needed and use the smart phone's data connection to pass the information collected to a doctor.
- End-to-end connectivity and affordability [4]: With the support of healthcare automation platform and other new technologies, and next-gen healthcare facilities, IoT will simplify the workflow of patient care. Healthcare IoT enables interoperability, machine-to-machine interaction, exchange of information and movement of data which makes delivery of healthcare services efficient.
- Data assortment and analysis: When cloud storage is inaccessible, it is difficult to store and handle large amounts of data that a healthcare system sends in a very short time due to its real-time use. Also collecting data from multiple tools and sources for healthcare providers and processing it manually is a difficult bet. IoT apps are able to collect, monitor and analyze data in real time and reduce the need for raw data to be processed.
- Tracking and alerts: In case of life-threatening situations, on-time alert is critical. Medical IoT devices collect vital data and transfer data to physicians for real-time tracking while dropping alerts about critical parts through mobile apps and other connected devices to people. Reports and alerts give a firm opinion on the condition of a patient, regardless of location and time. It also helps to make well-versed choices and to execute them on time.
- Remote medical assistance: In case of an emergency, patients can use a smart mobile app to contact a doctor who is many kilometres away. With mobility solutions in healthcare, the physicians can check the patients immediately and identify the on - the-go problems. In addition, various healthcare delivery companies are planning to build computers that can administer medications based on patient prescription and pain-related data accessible via connected apps. IoT will improve hospital care for the patient. It, in effect, would slash the distribution of medical care to people.

Moreover this, in [15] author has discussed about internet of things and its possibility (IoTs in future) with other applications in near future, where as in [16], authors have discussed security and privacy concerns in internet of things based infrastructure (or environment) in detail. These issues are more useful for further research in the next decade. Hence, the rest of this paper is organized in the following manner. Section 2 describes about the related work done in the field of intrusion detection in internet connected things. Section 3 provides the motivation behind choosing this area of research. Section 4 discusses about problem definition in simple terms. Further, section 5 discusses about our proposed solution for intrusion detection this smart era. Section 6 describes the open issues and challenges faced in the respective field in the surveys done in last few years. In last, section 7 concludes this work in brief with mentioning future research areas which can be taken into consideration (in next decade).

II. RELATED WORK

Today's our goal is to make the human life easier and more efficient and for this IoT has various emerging technologies which are making the environment better. IoT integrates with internet and physical objects such as human health, industries and many more [15]. As we know the more we get involved into IoT devices the more problem arises against the security and privacy and thus the need of intrusion detection system arises. An IDS provides a solution which is lightweight but provides the highest degree of protection and this makes it better to use. An Intrusion Detection System (IDS) is a type of security system which is performed on network layer. From previous many decades, it has been an important tool for the overall protection of the information. The intrusion detection system is broadly categorized into two categories:

- Network Intrusion Detection System
- Host Intrusion Detection System

Now, related work related to intrusion detection systems is discussed as: Gaudreau and Moorman [4] in their paper stated about various current trends in IoT. Further, with low cost and effortlessly built programmable embedded gadgets, DIYs and a spirit of young marketers paradigm is being promoted outside of the company and industrial geographical regions. These different adjustments are definitive of the IoT computing generation. With a huge sort of architectures starting from undocumented ad hoc embedded devices to very established ones adhering to the standards, the IoT is confused with additional safety troubles. For this purpose, present IDS joined at time of community get admission to, interacting with each provider layer. Sun and Li [3] have emphasized wholly on the security of Medical Internet of Things (MIoT). A sort of scientific devices and software packages are carried out to enhance the high-quality of medical offerings and also generate huge quantities of data. Recently, the significance of records is evident enough. How to effectively guard records protection and privacy at all tiers of data float will hold a critical function in future related research. Starting from the safety and privacy requirements of MIoTs (Medical Internet of Things), this paper discusses the safety and privacy troubles from five technical aspects and offers the demanding situations of future research.

Robert Mitchell [2] in his survey states that Intrusion detection is an important research topic with many important applications. Along with intrusion prevention, reaction and tolerance, intrusion detection is one of the methods which could defend towards the real cyber-attacks that are threatening important systems. They have provided the tools and the detection technique which can be used. Further, Mohammed Faisal Elrawy [5] discusses here about smart environments and purpose behind developing smart environments is defined as to make human life much easier by solving their problems and fulfilling their needs with the help of sensors. They defined the different problems arising in different layers while transmission. Any intrusion detected in the system without permission threatens information privacy of IoT users. The security of IoT environment is considered as a serious issue as various attacks effect the services and applications offered in IoT based smart environments. Future work will talk about the design of high performance hybrid IDS specifically designed for various platforms. Al-Janabi and Al-Shorbaji [6] discusses that wearable computing sensor gadgets become a critical part in our everyday lifestyles and sports. Today, people have often implanted sensor systems in their bodies to give a first-class enhanced and advanced life. This research explored the use of WBANs in security and privacy phrases. In addition to attacks on WBANs, it also addressed the WBAN communication structure, security and privacy in WBAN, and the challenges to the integration of sensors and actuators.The implications done here require the public and health care personnel to be aware of the challenges that come with WBAN usage to make sure that the application used in delivering patient's healthcare information is secured and protected at all levels. Alampalayam Kumar and Vealey [7] had cited that Internet of Things (IoT) has become centrally important in modern world's sector as hospitals, cities, organizations etc. In this paper, they have articled that as greater IoT based gadgets get linked to the internet, it outcomes in the extension of the surface region for external attacks. They categorized the attacks based on the layers that make up IoT and discussed numerous such attacks with examples. We also reviewed the literature on the current methods of protecting the IoT network and summarized certain protection techniques on how to deal with the security issues within the IoT. So, this section discussed about the related work done in this field and now the next section will discuss about the motivation provided behind selection of this research field.

III. MOTIVATION

Today every application/ industry is shifting towards using internet connected things (smart things) to reduce workforce and also increasing productivity. But, using these devices in many sectors/areas raises several serious issues like vulnerabilities in software, intrusion (malware, virus, worms) attacks etc. To identify such serious concerns in various internet of things applications (especially in e-healthcare), we need to provide complete detail of various type of attacks occurred (mitigated), including existing solutions (techniques) and also suggesting counter measures for future work. Also, we need to provide some detail with respect to IoT enabled application like automation (i.e., transportation), i.e., some better solutions for protecting privacy during parking of vehicles or sharing of vehicles [13, 14]. Basically, IoTs are used in automated vehicle, may cause of leaking privacy of vehicle's user during travelling over the road.

Hence, this section described about the interest towards writing this article and now the next section will describe the open issues and challenges towards intrusion detection system.

IV. PROBLEM DEFINITION

The main problem arising in the field of cyber security [8] is stealing of data and using it in any malicious way. Attacking an organization or anyone's personal data may result in loss of wealth, time, properties and much more. It is necessary to keep our systems updated and secured if we belong to any of the IT sectors and especially when we belong to the medical field as losing of medical information has become a crucial issue these days. The reason behind this much of the medical information is getting stolen and then being sold for money and personal purposes. There are basically two types of attacks:

- Internal Attack: The internal attack comprises of mainly three kind of problems:
  - Leaking of information, which can only be possible when any insider is involved as intruder.
  - Security of system and privacy of information is one of the most important things for any organization which can easily be at stake if intrusion is taking place from inside.
  - The last one which is also equally important is trust. In the medical field trust is very important as trust issues can be raised keeping the point that the patient's data can be sold by the doctor to any third party which may use it in a malicious way.
- External Attack: The externals attacks comprises of attacks by ethical hackers, botnet etc., or by the attack of viruses, Trojan horse etc. These can enter into the system by accessing of any internet site or by attaching any external storage device in the system. Here, attackers are not directly involved with the system. Either they usually track the user's behavior for days or find any vulnerability in the network and then attack whenever they get the appropriate time.

Both internal and external attacks are equally harmful to the system and may result into a greater loss if not detected on time. Sometimes it might be a possibility that user did not have intentionally attacked the system and wrong data just accidentally get breached, but this can happen in internal attack usually. For example, when an employee is copying any data of his use and mailing it to someone and by mistake any other confidential data get copied and being sent to any unauthorized person.
Hence, this section defines problem in clear manner, including several type of attackers. Now, next section will discuss proposed work (using blockchain technology) in detail.

V. PROPOSED WORK

As we discussed in the problem definition, we have to protect our system from both internal and external attacks and not many systems so far are there which can detect both external and internal attacks. In this work, we propose an idea for the system for both types of attack through a single system. As in every system nowadays, there is a need of either password or any security measure (finger print, ID card etc.) which will provide access to the system. In the organizations or hospitals database is maintained which includes details of doctors, nurses etc., and provide them the authorization to access the system. Another database is maintained for keeping the records of the patients which is usually not accessible by each and every person related to the hospital as we need some accessibility parameters to access those databases and the information present. So, what we are proposing here is whenever a person will sign in into the patient's database, a token will be generated at that time. This token will be active only for a particular amount of time, after this time a new token need to issues/ generated for further accessing of records. This token provides anonymity among existing users on a public/ private network. Also, this token will work as a dummy number which consist personal information of user's and this information is encrypted by hash keys (or hash function) and stored in block using Blockchain technology. Blockchain technology concept provides anonymity and security to user's personal information in this proposed work.

Note that next time when next user will login into the system, new token will be generated (again a new dummy number) and this will happen each time whenever any user will login into the system. Each time when a token is generated, that token number along with the information of the login person (user) and the

information which they have accessed will get stored in the admin's database (with using proper encryption schemes). Hence, the key points of the proposed system are:

- Token is being generated for a limited period of time after verifying authenticity of user using his/ her contact number. For example, issuing of One Time Password (OTP)
- Securing of the system is taking place using blockchain technology which will encrypt the information present in the token, the user's information and also user's action of every moment he performs until his session continues.

Hence, through Blockchain technology, we can find internal attackers available in a network. Identifying of internal attack/ attackers was a critical issue till now, but we solve this problem using Blockchain technology easily. Now taking in context of external attack, how we will detect intrusion is firstly when a user will try to login and change the password. For that our proposed system will generate (raised) an alarm which will indicate the admin that some intrusion has took place (attack has taken place) but when someone will try to change the password for the second time the admin will block the user and will keep their information saved. Hence, this section discusses our proposed method for identifying internal attacker and external attackers in detail. Now, next section will discuss several open issues and challenges in detection intrusion in this smart era or near future

VI. OPEN ISSUES AND CHALLENGES

Different mechanisms and parameters must be considered for a secure IoT deployment as described below [9]:

- Data Privacy, Data Confidentiality and integrity: Since IoT information moves over several hops in a network, the privacy of the data requires a proper encoding mechanism. The data stored on a device is vulnerable to a violation of privacy by compromising nodes in a network of the IoT due to a diverse integration of services, devices and networks. The attack-prone IoT devices can affect the data integrity by an attacker by altering the stored data for malicious purposes.
- Authentication, Authorization and Accounting: Authentication between two communication networks is necessary to ensure communication in IoT. The devices must be authenticated for secure access to services. The diversity of IoT authentication mechanisms exists mainly because of the diverse underlying heterogenous architectures and environments supporting IoT devices. Such environments present a challenge to identify the global standard IoT authentication protocol. In the same way, the processes of authorization ensure that licensed people have access to systems or data. Authorization and authentication are properly implemented in a reliable environment that guarantees a secure communication environment. The resource usage details like accounting and auditing and monitoring provide a reliable network management system.
- Availability of services: The attacks on IoT devices that prevent services from being delivered via traditional denial-of-service attacks. Different strategies such as sinkhole attacks, jamming adversaries and replay attacks use IoT components at various levels to exacerbate service quality (QoS) for IoT users.
- Single point of failure: The increasing number of single -point failures can reveal continuous development of heterogeneous networks for IoT-based infrastructure that could harm services provided by IoT. This includes the creation of a scalable ecosystem for many IoT devices as well as alternative methods to implement a fault-tolerant network.

While blockchain technology can bring many benefits, there is still an innovation that can suffer from various internal and external challenges [10].

- Storage facility constraint: In the IoT environment, the required storage capacity is very less than the ledger-based blockchain technology for sensors and actuators. IoT facilitates the processing of a single central database where, as in Blockchain, each ledger must be saved at the node.it requires more space with time when compared to traditional IoT devices.
- Absence of facilities in the sector: Even though the technology is recent, several problems must be tackled in order to facilitate it.
- Lack of manpower (qualified): This technology has very little skilled resources, and when combined with the idea of IoT this number is very small. Which means that trained workers who understand the integrated IoT-blockchain concept are very few.
- Legal issues: There are no legal codes to obey in this technology. This is one of the most important issues to address.
- Processing time: If these computing capacities differ, the time to carry out the authentication varies and the processing time changes.
- Scalability: concerning the scale of the ledger blockchain, which could lead to centralization as it expands over time and required some record management that shadowed the future of blockchain technology.

Hence, this section discusses several open issues and challenges faced today and in near future. Now, next section will conclude this work with including some future research directions in brief.

VII. CONCLUSION AND FUTURE ENHANCEMENT

Internet connected things have very higher growth in near future, i.e., it will be easily adopted by many applications. Together this, vulnerabilities or attacks also be more on IoTs. So, we need to secure IoTs with efficient and smart solution. Blockchain as decentralized concept, is recognized as a better solution for providing security to data in motion and rest. In this article, we proposed a security mechanism to IoTs based applications/ systems. In our next work, we will implement this proposed idea in a useful environment.

Future research will explore how blockchain can be used to protect other IoTs and related network as a shared security framework (for example: cyber-physical systems). A recent white paper from microsoft shows that public blockchain network processing power and related cost of energy is prohibitive to enterprise scenarios. Thus, an open source cocoa framework [11] has been recently proposed to research the optimization of blockchain and blockchain based Platforms to reduce energy consumption while providing more effective and secure services. Some of the future enhancements for blockchain and IoT are listed here [12]: a). How can IoT systems and anti-forensic technologies exploit attackers from the security features to avoid inquiries and forensic investigations? b). Attackers have taken advantage of security features of IoT devices and ant forensic techniques, how investigators and incident respondents can gain access to safe, IoT-saved communications. c). In areas where an IoT device is physically controlled and accessible to the public, how can blockchain ensure the security and privacy of the data that is stored on the IoT device.

ACKNOWLEDGEMENT

This research work is funded by the Anumit Academy's Research and Innovation Network (AARIN), India. The authors would like to thank AARIN, India, a research network for supporting the project through its financial assistance.

REFERENCES

[1] Isra's Ahmed Zriqat and Ahmed Mousa Altamimi, "Security and Privacy Issues in E-healthcare Systems: Towards Trusted Issues", *International Journal of Advanced Computer Science and Applications*, Vol. 7, No.9, 2016.

[2] Robert Mitchell and Ing-Ray Chen, "A Survey Detection in Wireless Network Applications", 2014.

[3] Wencheng Sun, Zhiping Cai, "Security and Privacy in the Medical Internet of Things: A Review", *Hindawi Security and Communication Networks,* Volume 2018.

[4] Audrey A. Gendreau and Michael Moorman, "Survey of Intrusion Detection Systems towards an end to end secure internet of things", *IEEE 4th International Conference on Future Internet of Things and Cloud*, 2016.

[5] Mohammed Faisal Elrawy, Ali Ismail Awad and Hesham F. A. Hamed, "Intrusion Detection Systems for IoT based smart environments: A Survey", *Journal of Computing: Advance Systems and Applications,* 2018.

[6] Samaher Al-Janabi et al., "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications", *Egyptian Informatics Journal,* 2017.

[7] Sathish Alampalayam Kumar and Tyler Vealey, "Security in Internet of Things: Challenges, Solutions and Future Directions", *49th Hawaii International Conference on System Sciences,* 2016.

[8] Daryabar, Farid, et al., "A survey about impacts of cloud computing on digital forensics", *International Journal of Cyber-Security and Digital Forensics* 2.2, 77-94, 2013.

[9] Mohammed Amine Ferrag et al., "Blockchain technologies for the internet of things: Research Issues and Challenges", 2018.

[10] Ahmed Banafa , "IoT and Blockchain Convergence: Benefits and Challenges",2017, https://iot.ieee.org/newsletter/january-2017/iot-andblockchain-convergence-benefits-and-challenges.html

[11] Microsoft 2017, The Coco Framework Technical Overview. https://raw.github usercontent.com Azure/coco.framework/ master/docs/Coco%20Framework%20whitepaper.pdf

[12] Atlam, Hany F., et al., "Blockchain with internet of things: Benefits, challenges, and future directions", *International Journal of Intelligent Systems and Applications* 10.6, 40-48, 2018.

[13] Tyagi, Amit & Niladhuri, Sreenath. (2017). ISPAS: An Intelligent, Smart Parking Allotment System for Travelling Vehicles in Urban Areas. *International Journal of Security and Its Applications*. 11. 45-64. 10.14257/ijsia.2017.11.12.05.

[14] A.K. Tyagi and N. Sreenath (2016), "Vehicular Ad Hoc Networks: New Challenges in Carpooling and Parking Services", *in proceeding of International Conference on Computational Intelligence and Communication (CIC), Pondicherry, India 2016*, vol. 14, (2016).

[15] Tyagi, Amit Kumar, Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), *Amity University Rajasthan, Jaipur - India, February 26-28, 2019*. Available at SSRN: https://ssrn.com/abstract=3356500 or http://dx.doi.org/10.2139/ssrn.3356500.

[16] Tyagi A.K., Rekha G., Sreenath N. (2020) Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. *Learning and Analytics in Intelligent Systems, vol 3. Springer, Cham*.