IOT BASED BLOCKCHAIN SOLUTION: COVID-19 AND DEFENSE

Vaishali Garg, Komal Sukhija, Seema Verma
E-Mail Id: vaishaligarg1999@gmail.com, komalsukhija222@gmail.com, seemaknl@gmail.com
Manav Rachna International Institute of Research and Studies, Faridabad, India

Abstract-Development is an indispensable part in the information technology field. The Internet of Things (IoT) basically opens door for all devices, appliances, and software to share and communicate information over the Internet. The shared data contains a large amount of secretive information, thus preserving information security on the shared data is an important issue that cannot be neglected. To secure data linked with IOT, blockchain is combined with IOT. IOT when implemented with blockchain is of great advantage to us. Here, the various characteristics, challenges and applications related to IOT are studied. Also, the Blockchain architecture and challenges are discussed in brief. In this work, the two IOT cases are considered; one for COVID-19 and another for Defense System. In both the cases the security and privacy issues are discussed and the solution is proposed in context of the blockchain.

Keywords: Internet of things (IoT), blockchain, privacy.

1. INTRODUCTION

IOT first came into existence in 1999 by Ashton [1]. It is a technology which is hard to be replaced. IOT is used almost everywhere and in all fields. IoT has gained great success in the past few years. It is used in cars, intra-body sensors, smartphones etc. The IOT connects various devices to the network thereby leading to increase in security threats. To ensure security many techniques are used and blockchain [7] is one of them. Blockchain which is used nowadays is an effective countermeasure to ensure security whereas the IOT is used to apply encryption to sensor devices used all over the world. There are many security requirements we need to check for every devices like authenticate to multiple networks securely, providing strong authentication, check that data will be available to multiple persons, maintaining the availability of the data, managing the contention between that data access and privacy concerns between multiple consumers. Our world consists of various devices out of which many are linked to internet so there security is a major concern. All devices are not made with keeping in view their security so they are very much vulnerable to outside attacks. To be secured from such attacks, blockchain and IOT are linked together. Blockchain is a simple technology used to protect data from manipulation. It is a data structure where blocks of data is stored in sequential manner. Blockchain when linked with IOT is used to secure devices and information linked with each other.

In this work, the two case studies are considered that are related to Covid-19 and Defense system. Their security and privacy are discussed and a secured solution is provided with Blockchain. The structure of the work follows as: in the next section IOT architecture is discussed with various challenges and applications. In section 3, various characteristics of Blockchain are studied with its challenges and applications. In section 4, two IOT related case studies are given and the secure solution with blockchain is proposed. Finally the work is summarized and concluded in section 5.

2. INTERNET OF THINGS (IoT)

The Internet of Things [1] is a network of physical devices that can deliver the best value and service by exchanging data with manufacturers and connected devices. This is the ability to transfer data over a network without human interaction. The idea is to connect a physical device that is not Internet-enabled to the entire world of everyday objects so that they can connect to the Internet and communicate through them. These can be monitored with a simple remote control.

Fundamentally, IOT is a way of connecting ours to the internet, and our daily routines are simpler, smarter and faster. Connected devices equipped with sensors or actuators are aware of the environment, understand what is happening and act accordingly. This is accomplished by processing the data found on the node, device hub, or cloud. In addition, the device is independently decision-enabled or can communicate information to the user, allowing the user to make the best decision. The idea of connecting devices via the Internet[14]. Born in the 1970s. At the time, it was known as the embedded internet. This technology was first used on the Coca-Cola machine because the programmer could connect it to the refrigerator to check for drinks and see if it was cold [4]. In 1999, Kevin Ashton coined the term Internet of Things [1]. In 2010, IOT gradually became popular

2.1 Architecture of IOT

Below is an architectural diagram of a gateway that does not have sensors on the gateway itself. Gateway software installed on the device responsible for collecting data from the sensor, preprocessing the data, and sending the final result to the data center.

As shown in the figure (Fig. 2.1), there are variations on the sensor architecture, with some sensors located on the gateway device.
The embedded sensors built into the gateway can also include options such as GPS units and temperature sensors connected to the gateway. One can find the detailed architecture in [14].

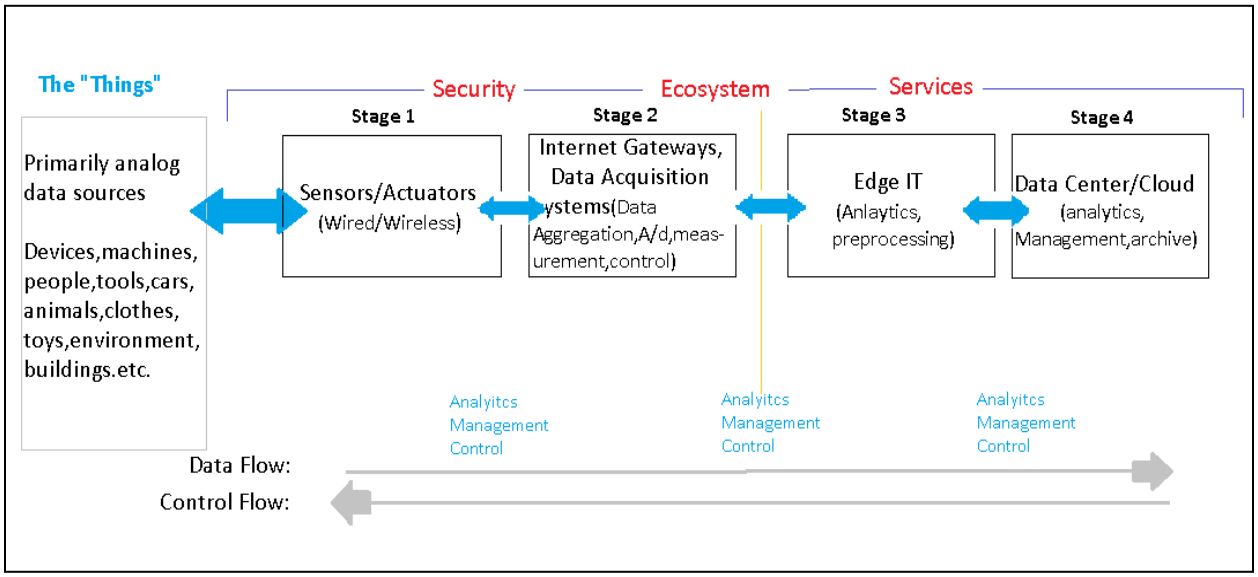

Fig. 2.1 Architecture of IoT

The IoT ecosystem consists of web-enabled smart devices with sensors and communication hardware to collect, send, and manipulate data retrieved from the environment (Fig. 2.2).

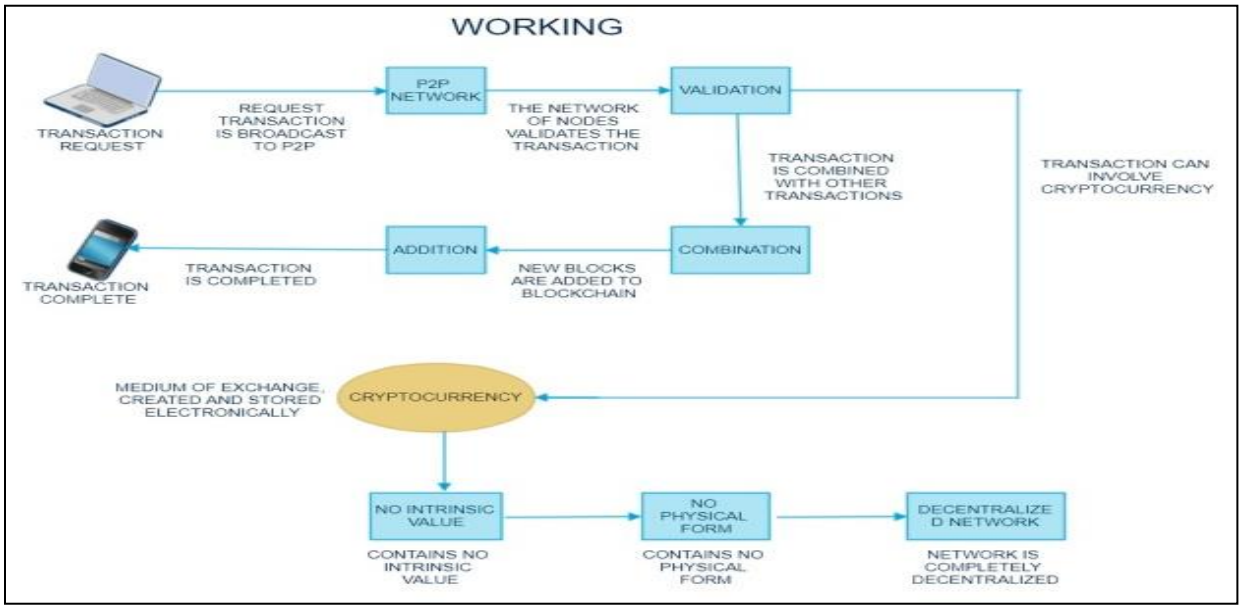

Fig. 2.2 Working of IoT

IoT devices share the data they collect by sending it to the cloud for analysis or by connecting to an IOT gateway that is analyzed locally.

2.2 Characteristics & Features of IoT

Few characteristics of IOT devices are presented here [4]:

2.2.1 Easy to Monitor

The smart appliances in the smart homes can be easily operated and monitored via mobile phones.

2.2.2 Easy to Operate

The smart appliances are easy to operate after analyzing the data which is conveyed to our smart devices. Further evaluation and operations can be done by using this data.

2.2.3 Reduction in Energy Cost

Sensors can be used to detect the need of energy. Like in a conference hall if there is nobody then there is no use of air conditioning, so sensors can be helpful in analyzing this data and adjust the temperature according to it.

2.2.4 Security

The extent of transparency and privacy issues is quite high for devices connected to IOT and hence they are very much prone to security threats. So to overcome this, the endpoints, the networks and the data that is being transferred must be secured properly.

2.2.5 Intelligence

Intelligence in IOT is mainly due to the interaction between various devices in a network. Its intelligence gives rise to handling situations well and performing various tasks.

2.2.6 Connectivity

Connectivity is another important factor in IOT. It provides ease of working and compatibility between devices.

2.3 Challenges of IoT

For the IoT system to function smoothly as a standalone system, we need to take into consideration various factors [1],[2], some of them are:

2.3.1 Security

IoT has become a severe security concern and has therefore seek the attention of various government organizations and firms working for security of data. In the future, security will not be just restricted to sensitive information and assets but also to our own lives and health.

2.3.2 Connectivity

IoT connects many devices, hence it has also become one of the most important challenge for IOT. Managing so many devices and handling their data is a real time challenge.

2.3.2 Compatibility and Longevity

IoT is gaining importance in every sector where many technologies are competing to become a standard, therefore this causes problems in connecting devices due to deployment of additional hardware and software devices. Once a standard is chosen it needs to be updated as to ensure long term support and manage IoT devices.

2.3.3 Standards/Interoperability

Interoperability means the ability to choose the devices having the best features and at best prices and make them work as a single unit.

2.3.4 Intelligent Analysis and Actions

For implementing IOT, data analysis is done which can sometimes lead to false analysis. Intelligent actions are also a great challenge as the adoption process of new technologies is slow, interoperability of machine and their action in unpredictable situations.

2.3.5 Intelligent Analysis and Action

For implementing IOT, data analysis is done which can sometimes lead to false analysis. Intelligent actions are also a great challenge as the adoption process of new technologies is slow, interoperability of machine and their action in unpredictable situations.

2.3.6 Insecure Communications

Encryption is must while sending messages to the network [6]. There are many private network that is use to send messages. There are many attacks to decrypt the encrypted messages. It is one of the challenge in the IOT.

2.3.7 Hijacking

There are many ways of hijacking of IOT devices:
By sending spam Emails: There are many smart appliances that have same power and functionality of the tablets so they can be hijacked and can be turned into email servers [16].
By using botnets: IOT devices can be hijack by using the malicious botnets. The purpose of botnet is to perform distributed denial of service attack. The main purpose is to hijack domain name system servers.
IOT malware and Ransomware: Ransomware is a type of malicious software that encrypt the whole device and ask for some money from the user to get decrypt the system. It also aim to steal the user data.

2.4 Applications of IoT

There are many IOT applications described in literature [9]. Some of these are presented here:

2.4.1 Smart Homes

Smart homes consist of our daily use devices which are more smart and sense the presence of human [19] like smart doors which got open when they detect the presence of the house members and smart electricity system which shut the lights off when there is no use.

2.4.2 Smart Cities

Smart city includes smart surveillance, automated transportation, smart energy and water distribution system by installing the sensors [18] and using web applications the problem faced by the people can be resolved.

2.4.3 Agriculture

Here IOT can be used to monitor humidity, temperature, amount of sunlight so that measures can be taken to grow the qualitative crop [16].

2.4.4 Wearables

There is a high demand for having work in this field. The main aim is to add sensors and software that able to collect data about the user. It cover the health and fitness information of the user. It is designed to be small in size highly energy efficient.

2.4.5 Retailing

IoT helps the retailer to connect to their customer with the help of smart devices such as smart phones. Retailers can also track the customer location and adjust their store layout according to their convenience to maximize their profits.

3. BLOCKCHAIN

A block chain [12] is a technique that protect the data from modification. It works with block and every block contains the data or information about the specific thing. It works like a spreadsheet or MS excel in windows as spreadsheet works with rows and columns whereas block chain works with blocks. The information is added to the block in block chain then it will connect with others blocks in the block chain.
It is also known as distributed ledger as a ledger is over network among all the peers and every peer have the copy of complete ledger.
Blockchain can be categorized into public, private and hybrid blockchain.
The concept of blockchain was first described in 1991 [17]. It was created so that the already created documents could not be backdated or altered. It was then adopted and reinvented by Satoshi Nakamoto in 2008 [3]. It was them improved by him by reducing the speed by which blocks of data are added to the blockchain. It was then finally implemented in 2009 where it serves as a ledger for all the transactions that take place on the network [4].

3.1 Architecture of Blockchain

The architecture is described in figure (Fig. 3.1). There are a number of nodes in a blockchain system each of which has a local copy of the ledger. Nodes may be present in different organizations. The nodes do not need a central authority to coordinate and validate the transactions but instead they communicate with each other to gain access on the ledger [13]. The process of gaining access is called as consensus. A transaction request is sent to the blockchain by the users to carry out the task (Fig 4). After completion of a transaction a record of that transaction is stored on one or more ledgers which cannot be altered later, that is called immutability.

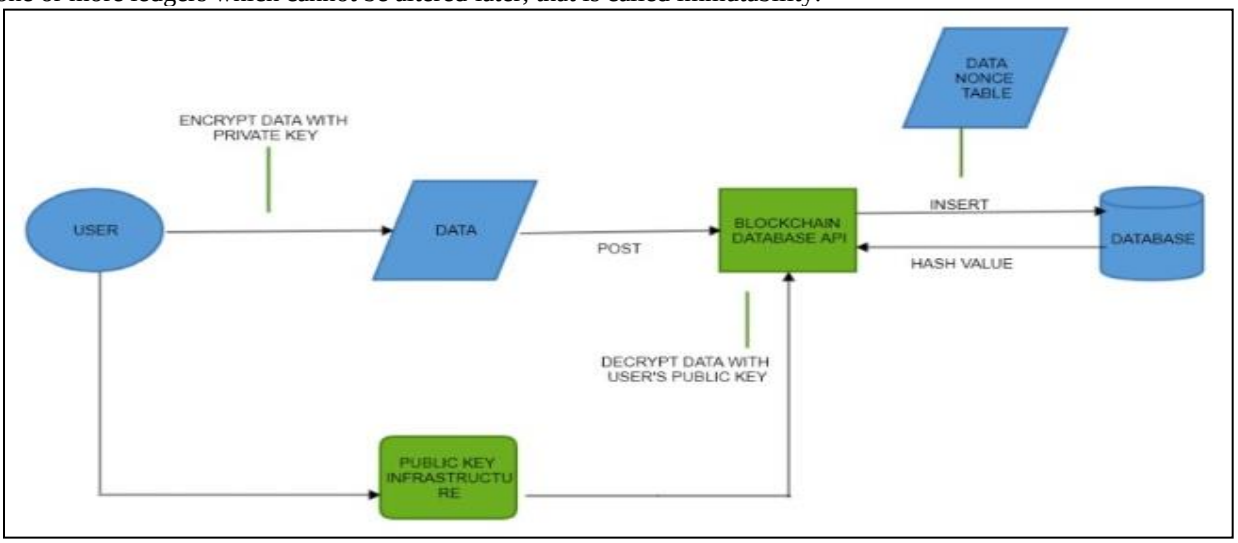

Fig. 3.1 Architecture of Blockchain

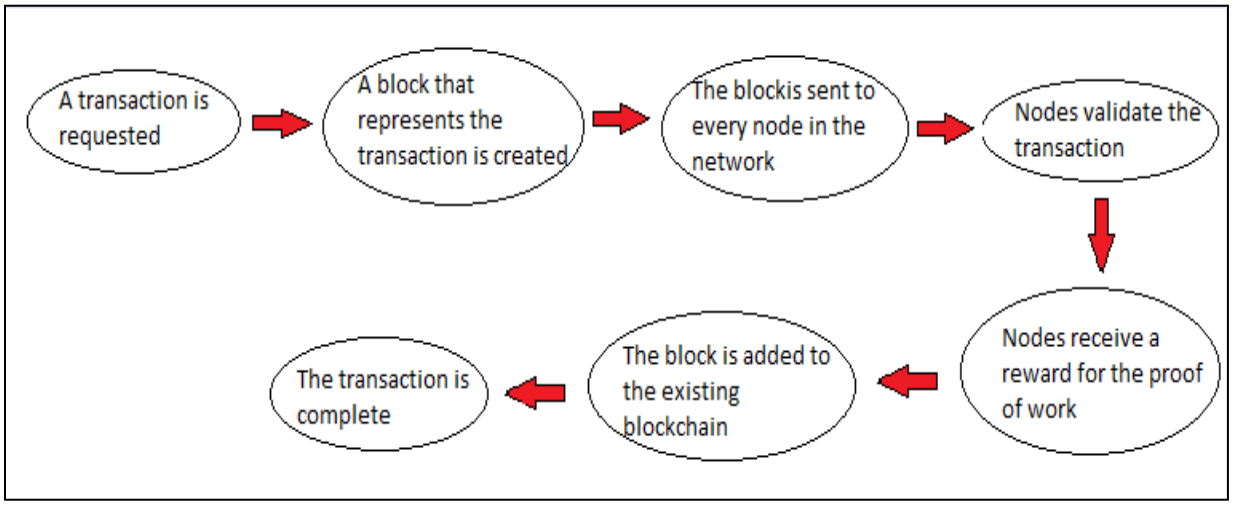

Fig. 3.2 Working of Blockchain

In (Fig. 3.2), the transaction is requested first, the transaction is created instantly and divides into block, each and every block are send to the network and attached to the existing/previous block when they are validated. Then, the transaction is completed.

3.2 Challenges of Blockchain

3.2.1 Complexity

The study of block chain is very complex as it added a new vocabulary to the cryptography.

3.2.2 Scalability

For less number of user the block chain will be efficient but what if the number of user will increase that will lead to the decreasing in the speed of the transaction that has been made. For large number of users, the restriction will be also applied like 10 persons in 1 second.

3.2.3 Transaction Costs, Network Speed

Bitcoin can be an perfect example for transferring money will no longer be cost effective for money transfer due to rapidly growing network which in turn increases the transaction costs in network [15].

3.2.4 Starting Cost

To build/purchase the software for the block chain is highly expensive once the installation will be done it is very beneficial for various tasks i.e. productivity.

3.2.5 Security of Data

The data secured by block chain is publicly visible so, that is the major concern for the government to restrict the action of access.

3.2.6 Human Error and Inadequate Skills

To maintain and review the data, once need a qualified person to get over this challenge. The error in one transaction can make a bigger difference.

3.3 Integration of IoT With Blockchain

The block chain and internet of things are interlinked together [10],[11] as for providing the security in the IOT things. IOT devices need to be secured as they have chances to be breached as IoT devices also contain moving parts. blockchain will add to this process will eliminate the unauthorized access also. The ways in which block chain is useful in IoT:

3.3.1 Smart Homes

There are many smart devices, appliances used in day to day life [8]. They are interconnected to each other so to centralized it, we need block chain. With the help of block chain integrity and security of the centralized data is maintained.

3.3.2 Smart Work in Industries

As, industries are also using IOT devices to maintain the record of their supply [5], in this process they need a block chain to provide security for the data that is transmitted over the network. The data that is collected can contain manufacturer detail, location, etc.

4. PROPOSED METHOD TO SOLVE SOME IOT PROBLEMS

IoT and Blockchain when combined together is of great value to almost every sector including medical facilities, home facilities, in the field of airlines, defense and many more. Here two scenarios are discussed: healthcare (Covid-19) and Defense. In both the cases the secure solution with blockchain technology is provided.

4.1 IoT with Blockchain in Healthcare (COVID_19)

In healthcare industry, one can monitor health of the patient that is far from the hospital. IOT can help in healthcare industry in many ways:

4.1.1 Remote Health Monitoring

In some cases, patient do not need to come to the hospital for checkup, they can monitor from their homes by using IOT devices.

4.1.2 Security of Staff and Patient

Security is the major concern in every industry, IOT can make it easy by maintain the data about tracking of the patient and staffs. IOT and real time location system can be used for keep on tracking of staffs and patient.

4.1.3 Monitoring of Medical Hardware

Let's suppose if a person needs to take to operation theatre in emergency and the device fails, it will lead to a serious concern. IOT device can maintain the information about the hardware of the device and inform staff earlier when some issue arises in the device.

4.1.4 Proposed Solution (Covid-19)

If a patient is having a heart problem since a long time and a hospital cannot admit a patient without any issue at a particular time, and there is a need of monitoring the health status of the patient so, it can be done from his home. A patient can be monitor by their phone and if there an irregularity in his health then it will immediately inform the doctor or the staff of the hospital that has the record history of the patient so that, the hospital staff can immediately sent the ambulance to him. There are many proposals for IOT devices that can be used in healthcare industry i.e. a wrist band can be used to monitor the health of the patient.
In the fig. 4.1, there is patient who is at high post and many persons want to harm the patient. If we are using the IOT devices for monitoring the patient then it needs to ensure that the data that is transmitted from the patient to the doctor must not be tampered. Here, the block chain is used for providing the security of the data that is transmitting over the network. It is very difficult to tamper data while sending block by block using block chain methodology. And it automatically includes in the process.

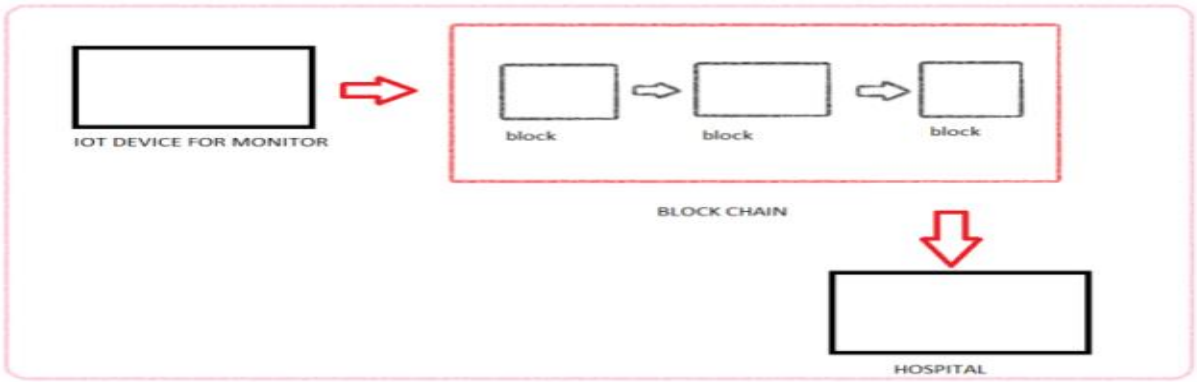

Fig. 4.1 Implementation of IOT and Blockchain in Healthcare (COVID-19)

Following are some steps that needs to follow:

- All the data needs to collect that you want to transfer over the network.
- By using blockchain technology, convert the data into blocks to provide unbreakable security.
- While sending over the network, use the secure network also (i.e. https).
- While receiving the data, cross check with any algorithm (i.e. by generating hash and check it with hash of original data)

If we talk about today's scenario, there is a spread of corona virus all over the world. An application named Aarogya Setu was developed to detect the health of each and every person. What if, someone steals the data while transmission and manipulate it while sending it will create the huge problem to the government. In this case, we need a high security during transmission. With the help of above-mentioned method, we can secure the data while

transmitting it over the network. So that the government will get the exact data without manipulation as it is very difficult to break the security done by block chain.

4.2 IOT with Blockchain in Defense System

As we all are well aware of inter-country wars and the equipments used at that times. One equipment among them is the army tank that is a fighting vehicle used by our army men to fight the opponents on the frontline combat. So to increase it's advantage the new idea being proposed here is that we can use some IOT enabled chip (which can be accomplished using Mobile IOT and Bluetooth low Energy) in all the weaponry like fighter jets, tanks, ships, submarines so that all the connected weaponry data can be collected together and instructions can also be fed together using the IOT protocol.

We can make our weaponry more efficient by fixing a detector in our weaponry so that they can detect all neighboring weaponry and then using the information collected and stored of our weaponry, instruct them to attack nearby opposition army weapons.

Here we even want Blockchain as using Blockchain we will be able to protect the confidential data stored on our systems which contains information about the weaponry of our own country so that it cannot be modified by the opposing party.

Another interesting feature that can be included is that only some authorized army officials who fight through weaponry can only run weaponry. It would thus lead to greater efficiency of our weaponry in terms of confidentiality, authenticity and integrity as a small change in that information can cause great harm or damage to us.

Hence, by using IOT enabled devices which are secured through Blockchain in defense (fig. 4.2) we can actually prevent our boundary from some major attacks and even contribute towards a more protected nation.

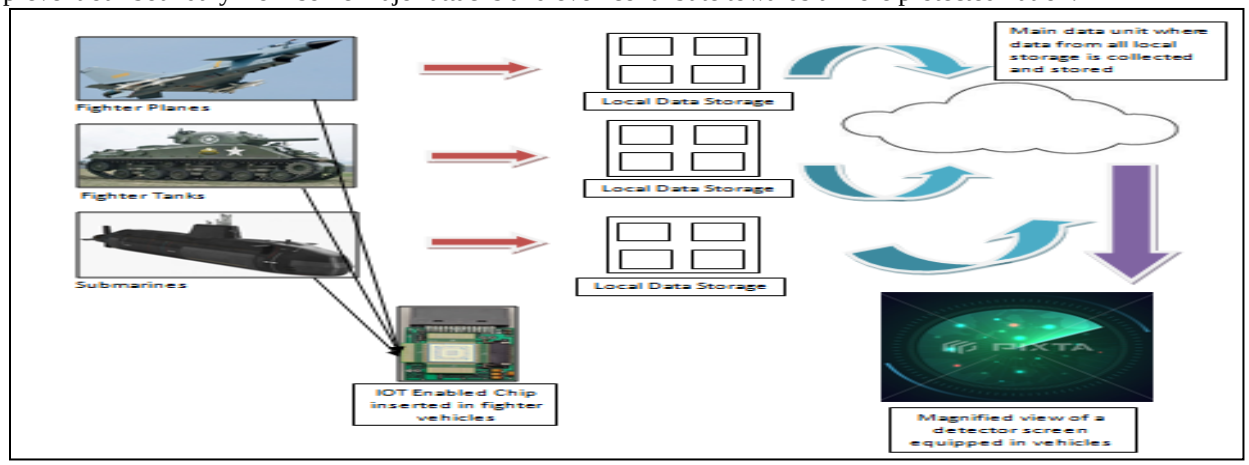

Fig. 4.2 Implementation of IOT and Blockchain in Defense

CONCLUSION

In this work, the architecture of IOT and Blockchain is discussed with their challenges and various applications. We have provided an overview of existing literature of blockchain for IoT, and presented a roadmap application based on integration of blockchain and IOT that will lead to great changes and prove to be advantageous to the world. Here, the two case studies are discussed in detail and solution is provided and worked upon them on how to implement them. The solution of the problems are proved to be a secure for various scenario.

REFERENCES

[1] AshishA.Magduma, AshwiniB.Patilb, A Review paper on security in Internet of Things (IoT), Islampur, India, Volume 3, 415-421, 2018

[2] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, IOT Security: Ongoing challenges and research opportunities, Matsue, Japan, 2163-2871, 2014

[3] Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things – A survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

[4] Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.

[5] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233– 2243, 2014.

[6] O. Bello and S. Zeadally, "Communication issues in the internet of things (IoT)," in Next-Generation Wireless Technologies. Springer, pp. 189–219, 2013.

[7] Rishabh Jain and Aniket Dogra, Solar Energy Distribution Using Blockchain and IoT Integration, IECC ' 19, Okinawa, Japan, July 7–9, 2019

[8] Jawad Ali, Togeer Ali & Yazed Alsaawy and Ahmad Shahrafidz Khalid & Shahrulniza Musa Blockchain-based Smart IoT Trust Zone Measurement Architecture, COINS crete, Greece May 5–7, 2019

[9] Laphou Lao, Zecheng Li, Songlin Hou & Bin Xiao, Songato Guo and Yuanyuan Yang, A survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modelling ACM Computing surveys Vol. 53, No. 1, Article 18, February 2020

[10] Reuben Jackson, Why IoT needs the blockchain and blockchain needs IoT, Retrieved March 12,2019 from https://hackernoon.com/why-IoT-needs-the-blockchain-and-blockchain-needs-IoT-896725b349c4

[11] Steve Huckle, Ritupurna Bhattacharya, Martin White, and Natalia Beloff 2016. Internet of things,blockchain, and shared economy applications. Procedia Copmuter Sci 98, 461-466,2016

[12] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ''A survey on the security of blockchain systems,'' Future Gener. Comput. Syst., vol. 2017, pp. 1–13, August 2017

[13] Shao, Q.-F & Jin, C.-Q & Zhang, Z. & Qian, W.-N & Zhou, Aoying. (2018). Blockchain: Architecture and Research Progress. Jisuanji Xuebao/Chinese Journal of Computers. 41. 969-988. 10.11897/SP.J.1016.2018.00969.

[14] Huansheng Ning, Hong Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things", Advances in Internet of Things, Vol.2, No.1, January 14, 2012.

[15] Archana Prashanth Joshi, Meng Han_ and Yan Wang, "A survey on security and privacy issues of blockchain technology", Mathematical Foundations of Computing, Vol. 1, No. 2, pp. 121-147, 2018

[16] Abdmeziem, R. and Tandjaoui, D. (2014) 'internet of things: concept, building blocks, applications and challenges', Computers and Society, arXiv preprint arXiv:1401.6877

[17] Sabah, Sana & Mahdi, Nada & Majeed, Israa. (2019). The road to the blockchain technology: Concept and types. 7. 1821-1832.

[18] Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., Oliveira, A.: Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. In: The Future Internet Assembly. Springer (2011)

[19] Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., Loge, C.: The Smart Home Concept: our immediate future. In: 1st IEEE international conference on e-learning in industrial electronics. IEEE (2006) 31.