International Conference on Intelligent Sustainable Systems (ICISS 2019)
IEEE Xplore Part Number: CFP19M19-ART; ISBN: 978-1-5386-7799-5

A Review on Blockchain Urgency in the Internet of Things in Healthcare

Rakhi Soni
Department of Computer Science
Rajasthan Technical University
Kota, India 324010
Rakhi.Soni.gsr@gmail.com

Gaurav Kumar
Department of Computer Science
Rajasthan Technical University
Kota, India 324010
Gaurav.kumar.npiu.cse@rtu.ac.in

***Abstract*—With the growing use of the internet, new technology came into the existence and it is on the same edge now, where decades ago the internet was. Internet of things (IoT) is facing many security issues. Due to the lack of the security standards, industries are afraid to take a risk with IoT. In the Healthcare industry where data is vast and valuable, it is risky to use IoT with it. It can compromise the patient's security. In this paper, various methods are discussed for Healthcare issues in IoT, by several researchers. Mainly the research work is focused on the different solutions proposed in the healthcare for IoT. At the end, a theoretical analysis of proposed solution is done.**

Keywords—Internet of Things(IoT), Security, Privacy, Security attacks, E-Healthcare, Blockchain.

I. Introduction

Internet of things and Blockchain are two great technologies having a great identity in their selves but the merger of both also helping in many industries. The Healthcare industry is in the list of insecure industries while it is carrying valuable data of its patients. We know that IoT is providing great automation to the industries, but it is also providing the insecurity which is a problem for the industries that require an improvement in the existing system. Healthcare industry is one of the industries, which are facing this problem. The data transaction is a very big concern in the healthcare industry. IoT will provide the ease on the other hand security concerns can be eliminated by using the Block-chain technology.

Data transaction occurs between different healthcare institutions, service providers; the data gets passed through different parties. In a Blockchain network, these transactions will be transparent in nature. A peer-to-peer transaction is the biggest advantage of Blockchain. The communication between multiple endpoints in the healthcare industry, which is in IoT architecture, can be secured using this Blockchain technology [1].

The Blockchain technology can be a cure for IoT. Because of its security concerns, only 30% of the healthcare industry is using IoT [2]. There are histories of IoT problems faced by other industries.

The total population on the earth is about 7.6 billion. Out of which 3.7 billion are using the Internet, almost 50% of this population, which is using the internet, lives in Asia, 24% of this population lives in India. Investment in digitization and urbanization and friendly regulatory policies grip the key to ensuring that India continues to advance on its path of socioeconomic progress. IoT in India alone is predicted to be $9 billion by 2020 [3].

In 2016, October 21 an attack happened at Dyn. This Distributed Denial-of-Service (DDoS) attack was accomplished through a large number of DNS lookup requests from 1,00,000 IP addresses. In the DDoS attack, all the bots were the internet-connected devices like Printer, IP Camera, and Residential Gateway. The Mirai infected these devices. This attack proved that how insecure is IoT. All IoT devices were the part of the attacker's union without even knowing a thing. All devices were working as a bot and participating in the DDoS attack by creating a botnet. This attack is called as Mirai attack [4].

Fig. 1 shows the rank of the healthcare industry in security. Healthcare industry is at 15th rank among all the other industries in security perspective. That means the healthcare industry needs to be secured and need solutions for security breaches. Healthcare industry has lower endpoint security [17].

In this paper existing solution and their demerits are presented to show the need of Blockchain in the Healthcare. This paper is organized in various sections. In section II, background study of some of the existing solutions for Healthcare in IoT are discussed. In section III, all the possible challenges in an IoT environment are discussed to explain the possible attacks in the IoT infrastructure. In section IV, a solution is proposed to implement Blockchain in E-healthcare. In section V, a theoretical analysis is given and in the last, the conclusion with the future scope is discussed.

II. Background Study

When every industry is upgrading to the digital world then why not the healthcare industry? It is because this industry is keeping highly valuable data in its pocket and the industry knows the breaches. The healthcare company, which is in the digital world, they are on the top list of the insecurity. Using IoT in healthcare giving a rise of stealing the valuable data they have of a patient. The P.I.I. (Personal Identifiable Information) is at a risk if they use IoT. This P.I.I. keeps the information about the patient like Name, Social Security No., Health Insurance No., Medical History, Medical Id (a US Medical Id to provide medical benefits to poor). What is the motive of these cyber attacks on Healthcare data? Because Hospitals, Pharmacies, Urgent health care clinics, and health insurance companies keep valuable data of a patient. In the black market Social Security No. is worth 10 cents and a credit card no. of 25 cents. This health data may worth 100 or even 1000 dollars. Definitely, you get all the important data at a single place and even that worth more, so a steal would come to this straight [5]. The transfer of this data is also important because to provide the best facilities to a patient, a healthcare organization needs to transfer the data. They transfer the data so that the consultant could be taken from a good physician or from other healthcare organization. Maximum data transfer is done through and to the laboratories. The transfer of data when using IoT architecture gives the rise of transferring data through these multiple endpoints.

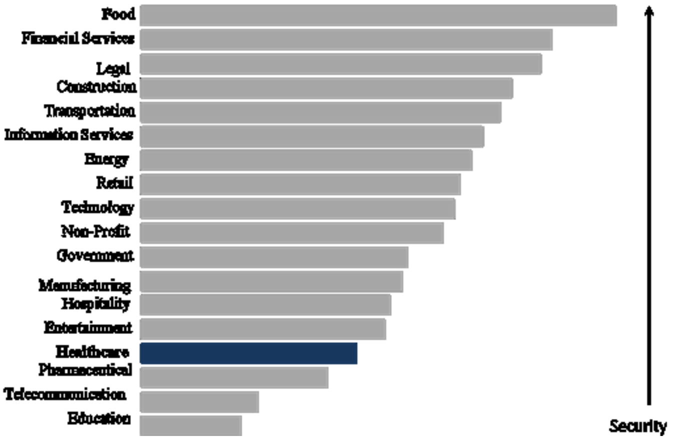

Figure 1 [17] Rank of Healthcare industry in security perspective

Many of the researchers have proposed solutions for IoT in healthcare. In [6], an Automation Healthcare System (AHS) is proposed. The main objective of this system is to provide advanced home healthcare services. The system collects the health information of the patient and creates an alert to the service provider i.e. caretaker or doctors to take immediate action. This method uses the Body Sensor Network (BSN).

In [7], a Narrowband IoT is proposed to provide co-ordinate services. The motive of this solution is that it needs fewer amounts of resources. The main attraction of the system is low power wide area (LPWA) coverage.

In [8], a Context-Sensitive Role-based Access Control scheme is proposed. In the proposed scheme, in which two types of access control is defined. The Open Access is associated with the authenticated clients and the medical devices and the Closed Access is for unauthenticated and non-medical devices. In the proposed method, a Supervisory System (SS) is culpable for authenticating and registering the things. The new client or device admission will be handled by the Intelligent Trusted Administrator.

In [9], a Real-time Multilayer Smart Healthcare Monitoring Framework using IoT and its several computing components is proposed. This method intensifies the health supervision and control by expanding the computational capabilities of sensors. In data processing, the concepts of Body Area Network (BAN) are used and data compression techniques are applied to sensor's data.

In [10], a Healthcare IoT System Model using Raspberry Pi 3 is proposed. In the proposed system, the sensor senses the information from the human body. The system checks the patient's condition by sending the real-time information to cloud and cloud stores the information. The goal of the system is to provide convenient information to the respective member and to get the location of the near healthcare. The distance calculated by the Euclidean distance equation and the information can be displayed to the patient.

III. CHALLANGES

It is observed that many of the industries have already adopted the IoT environment where on the other hand the remaining industries are afraid of the security breaches which other industries have already faced. It can be compared that today IoT is similar to the early internet when consumers faced many threats over the internet regarding the security.

The five necessary questions about the connected devices in the healthcare industry

- Is data being stored and transmitted securely between the IoT devices?
- Is there a new path for unauthorized access of data?
- Can Software security updates be adopted or not to address new risks?
- The APIs between these software and devices are secure or not?
- Is there any new way to steal the data?

Whenever a device or software is developed all the possible threats are also counted that can degrade the security. The biggest challenge in using IOT in healthcare is the security, which can keep the patients PII secure.

According to the study of many researchers [11] [12], The IoT architecture is poised of four layers, Perception Layer, Network Layer, Middleware Layer and Application Layer. The description is given below [13]

A. Perception Layer

The tasks of this layer are identification, node networking and data sensing such as service provider identification information in healthcare, patient medical information, information about equipment and waste [13]. All the information that can be sensed in an IoT infrastructure is the part of this layer.

B. *Network Layer*

This layer is the backbone of the Hospital infrastructure and IoT. This enables transmission and admission of medical data and permits the use of health-specific communication. [13] [14]

C. *Middleware Layer*

Middleware is software that makes different, complex and already existed IoT components as allies that are primitively not meant to connect. This is a cloud computing based layer, because of the services it provides such as computing resources consignment, as a service to end user, resilience and scalability. It increases the processing for the large amount of collected information at the perception layer. [15][12]

D. *Application Layer*

This layer deploys a set of an application dedicated to software and hardware system of the healthcare organization and concerns with the management of medical technology.

Fig. 2 shows different attacks in IoT infrastructure which are classified as physical attacks, network attacks, software attacks and encryption attacks [16].

These are the various attacks on an IoT infrastructure, that is a challenge to create a 'no-privacy concerns' IoT architecture.

Multiple endpoints communication is a challenge and also a security concern. IoT solutions, involving thousands of endpoints that sense and process the data over multiple networks. Challenges included with the multiple endpoints in an IoT solution-

Time and efforts required to communicate reliably with the cloud is a challenge.

Rigid framework locking of IoT systems, that system cannot respond fast to the changes.

The biggest question for IoT is why not a bottled insecurity. Why wrapping up this technology with other security technology. There are many reasons for that. The limitations of the computing devices in IoT play an important role in this. Lack of the standards and the protocol for security in IoT is an issue and a reason of why security is not bottled in but wrapped around. The connected device in IOT infrastructure has limitations like storage capacity and power. The devices are not capable to handle such big protocols in such small storage and power.

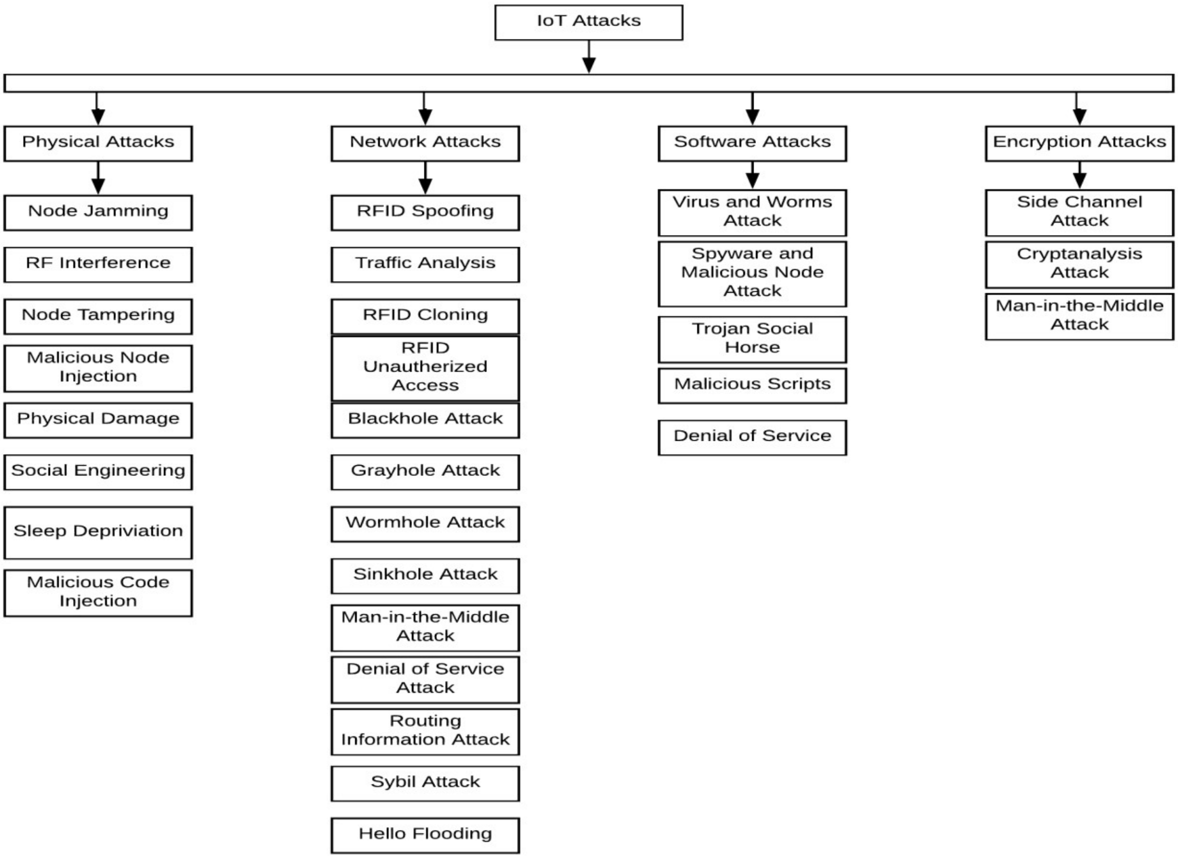

Figure 2 Four types of attacks in Internet of Things. The four attacks are Physical Attack, Network Attacks, Software Attack and Encryption Attack

Table 1 IOT ATTACKS AND AFFECTED LAYER

S.No.	IoT Attacks	Layer	Dangerous Attack (Comparatively)
1	Physical Attack	Perception Layer	Malicious Node Injection
2	Network Attack	Network Layer, Middleware Layer	Sink Hole Attack
3	Software Attack	Middleware Layer, Application Layer	Worms Attack
4	Encryption Attack	Application Layer, Perception layer	Side Channel Attack

In Table I, affected layer are shown with respect to various attacks. In physical attacks, malicious node injection attack is more dangerous because it stops the services and also modifies the data. In network attacks, sinkhole attack is the riskiest attack because it attracts all the traffic towards the base station and selective forwarding, packet dropping and altering is also a threat by the adversary. In software attack, the worm attack is the most unsafe. Worms are the self-replicating programs which harm the system by using the security breaches. This attack can alter the file system and the information without any notice. In encryption attacks, side channel attack is very difficult to detect because the attacker uses the side channel information to intrude. [16]

IV. PROPOSED SOLUTION

In This section we have given an idea about the implementation of Blockchain technology in I-Healthcare sector (IoT Healthcare). IoT has several issues like, the lack of security standards, protocols, inability to update the device firmware, the secured data transmission and secure web interfaces. The solution of the above said IoT problems can be Blockchain. Communication among the multiple endpoints in I –Healthcare can be secured with Blockchain. Every piece of data would be transmitted using Blockchain. Therefore, intruder/attacker cannot alter modify and delete the in transit data. At the network and the middleware layer Blockchain can provide a higher level of security. Figure 3 shows architecture for Blockchain integrated I-Healthcare. The architecture gives the idea of sharing the P.I.I. of patients or important information through the Blockchain technology in a IoT Healthcare.

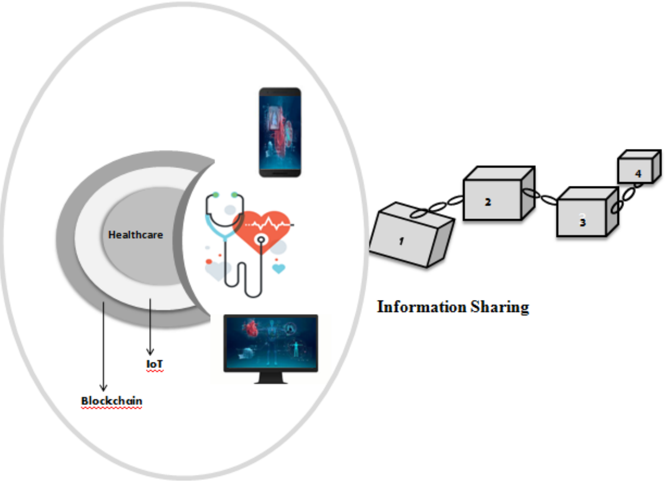

Figure 3 Blockchain IOT Healthcare

V. THEORITICAL ANALYSIS OF EXISTING SOLUTION

In the theoretical analysis, we have analysed the existing solutions and presented the important facts. In Table II, each of the models is associated with certain properties like, objective, possible attacks, complexity (Implementation + Maintenance), and compromised layer of the model and intensity of the attack.

Complexity is measured in two parts, implementation and maintenance, and categorized in three categories, easy, medium and hard. The parameter, compromised layer, contains the details about various IoT layers with respect to each model. The last column displayed the intensity of possible attacks with respect to each model. Intensity levels are categorised in three ways that are, high, moderate and low.

The main issue in the Automation Healthcare system (AHS) is that no security mechanism is provided in the solution. So that, this model is vulnerable to all above listed attacks.

The main problem found in Narrowband IoT system is that the no secure communication is available among endpoints. Therefore, DDoS attack, RFID attack and network attack may be possible in that system. For the attack intensity, moderate is assigned because this model invokes MAC layer functioning. Complexity is rated as easy because low band sensors are required to process for even wide area. This solution is not compatible with real-time application because of the delay it incorporates. High bandwidth requirements cannot be fulfilled by this model in healthcare.

The healthcare IOT system model is vulnerable to physical attack, which can lead to other software or network attacks. Default settings in identity and password can be a concern. The system does not give any security solution which makes it high vulnerable to attacks. Affected IOT layers are network and application layer. The middleware layer may be affected in endpoints communication. Complexity is easy because of the less components (comparatively) are required.

In Real-time Multilayer Smart Healthcare Monitoring Framework, no mechanism is available for secure communication. Therefore, DDoS attack can harm the in transit communication from patient to healthcare and vice-versa. Network and software attacks may be possible due to no security mechanism and it may affect network, middleware and application layer. The complexity is hard due to the processing and the computation at sensor level and data compression techniques.

Context-Sensitive Role-based Access Control scheme suggests a solution for secured access control. Passive attacks may be possible in this model like man-in-the-middle attack and also software attacks are possible in context to the system. The complexity is rated as high because of the context definition is complex. The intensity level is rated as moderate because the model claims the security but few attacks are possible. Because of fewer security and interoperability standards it does not fulfill the purpose.

According to the study, the discussed solutions lack in the security mechanism for communication among multiple endpoints. The physical attacks may be possible in all discussed solutions. The middleware layer is also compromised in many of the solutions when it comes to the multiple endpoints communication. The healthcare will have vast structure of endpoints and security is a critical issue for information transaction.

VI. Conclusion

We have discussed the several IOT threats for various proposed solutions. Healthcare industry keeps the important PII and concerns are increased while the endpoints are more. Further, we have studied the the emergence of Blockchain into the healthcare industry to overcome the security concerns between the multiple endpoints communication. In theoretical analysis, various proposed solutions have been compared on the basis of several parameters and a review has been suggested. The storage can be an issue for such vast data. For the future work, storage concerns can be taken into account to solve.

TABLE II. THE MAIN PURPOSE AND ISSUES OF THE EXISTING SOLUTIONS

S.No.	Model	Year	Objective	Attack/s	Complexity	Compromised Layer	Intensity of the attack

1	Automation Healthcare System (AHS)	2016	Advanced Home Healthcare Service	May be all	Medium - easy	A(Less)
						B
						C
						D(Less)
							High

2	Narrowband IoT	2017	Co-ordination Services Or Monitor Service	RFID Attacks 2	Medium	B C	Moderate
3	Healthcare IoT System using Raspberry Pi 3	2018	Get the nearest healthcare organization by calculating the location with Euclidean Distance Calculation	1 2 3	easy	B D	High
4	Real-time Multilayer Smart Healthcare Monitoring Framework using IoT	2018	Expand the computational capabilities of the sensing devices	2 3	Medium	B C(Possible) D	High
5	Context-Sensitive Role-based Access Control scheme	2018	Access control	1 3 Man-in-the-middle Attack	Hard	A B C (Less Compromised)	Moderate

1-for physical attacks, **2**-for network attacks, **3**-for software attacks, **4**-for encryption attacks.

A-for the perception layer, **B**-for the network layer, **C**-for the middleware layer, **D**-for the application layer

REFERANCE

[1] A. Dorri, Salil S. Kanhere , R. Jurdaky and P. Gauravaramz, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home”, *2ND IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things* 2017

[2] "How IoT is transforming the healthcare industry", *PathPartnerTech*, 2018. https://www.pathpartnertech.com/how-iot-is-transforming-the-healthcare-industry/

[3] TaTa Communications, "INDIA IoT REPORT - EMERGENCE OF A NEW CIVIC OS", 2018.

[4] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack", *Oracle.DynCompany News*, 2016. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[5] M. Yao, "Your Electronic Medical Records Could Be Worth $1000 to Hackers", *Forbes*, 2016.

https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/1

[6] K. S. Velrani and G. Geetha, "Sensor based healthcare information system," *2016 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR)*, Chennai, 2016, pp. 86-92.doi: 10.1109/TIAR.2016.7801219

[7] S. K. Routray and S. Anand, "Narrowband IoT for healthcare," *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, 2017, pp. 1-4. doi: 10.1109/ICICES.2017.8070747

[8] V. Alagar, A. Alsaig, O. Ormandjiva and K. Wan, "Context-Based Security and Privacy for Healthcare IoT," *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Xi'an, 2018, pp. 122-128.doi:10.1109/SmartIoT.2018.00-14

[9] P. Jangra and M. Gupta, "A Design of Real-Time Multilayered Smart Healthcare Monitoring Framework Using IoT," *2018 International Conference on Intelligent and Advanced System (ICIAS)*, Kuala Lumpur, 2018, pp.1-5. doi:10.1109/ICIAS.2018.8540606

[10] S. Yattinahalli and R. M. Savithramma, "A Personal Healthcare IoT System model using Raspberry Pi 3," *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, 2018, pp. 569-573. doi: 10.1109/ICICCT.2018.8473184

[11] D. Lake, R. Milito, M. Morrow and R. Vargheese, “Internet of Things: Architectural Framework for eHealth Security” Journal of ICT, 2013

[12] I. Cvitic, M. Vujic and S. Husnjak, “Classification of Security Risks in the IoT Environment”, *Proceedings of the 26th DAAAM International Symposium*, pp.0731-0740, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-07-5, ISSN 1726-9679, Vienna, Austria DOI:10.2507/26th.daaam.proceedings.102

[13] A. Djenna and D. Eddine Saïdouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," *2018 2nd Cyber Security in Networking Conference (CSNet)*, Paris, France, 2018, pp. 1-4. doi:10.1109/CSNET.2018.8602974

[14] Lei Yu, Yang Lu, XiaoJuan Zhu, “Smart Hospital based on Internet of Things,” Journal of Networks 2012

[15] "IoT middleware (Internet of Things middleware)", *IoT Agenda*, 2015

[16] J.Deogirikar and A.Vidhate, "Security attacks in IoT: A survey," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp.32 37. doi:10.1109/I-SMAC.2017.8058363

[17] P. Nohe, "The Healthcare Industry is lagging behind on Cybersecurity https://www.thesslstore.com/blog/healthcare-industry-cybersecurity-2018/", *Hashed Out by the SSL Store*, 2018. .