SECURITY & PRIVACY CONCERNS, MEDJACKING AND ATTACKS IN IOT HEALTHCARE SYSTEM

Mukesh Choubisa and Prof. S O Khanna

ABSTRACT

The Internet of Technology (IoT) is an emerging technology in computer science society. IoT Internet based information architecture facilitate the exchange of information from one place/system to another place/system. The Internet of technology has the principle of providing an IT-infrastructure to exchanges of things in a reliable and secure manner in network. The Internet of Things (IoT) refers to a basic concept of linked/connected devices of all types over the Internet wireless or wired. The popularity of IoT has improved rapidly, as these technologies are use by many organizations for various purposes, including medical devices, network communication, education, business development and transportation.

Index Terms *IoT Security, IoT Privacy, IoT in Healthcare, Medjacking in IoT, IoT Healthcare Security and privacy challenges, IoT healthcare systems, security of IoT, privacy, information security.*

Reference *to this paper should be made as follows: Mukesh Choubisa and Prof. S O Khanna, (2022), "Security & Privacy Concerns, Medjacking and Attacks in IoT Healthcare System" Int. J. Electronics Engineering and Applications, Vol. 10, No. 2, pp. 51-62.*

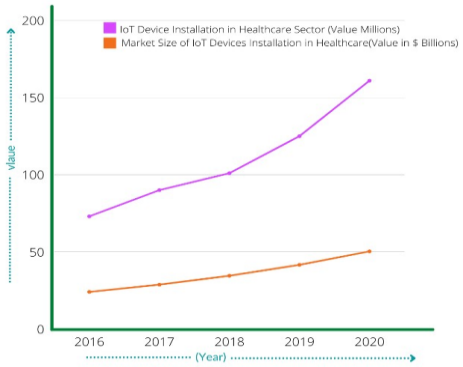
Biographical notes:

Mukesh Choubisa , *Mukesh24sa@gmail.com , Department name Computer Science and Engineering Institute of Advanced Research , Gandhinagar.*

Prof. S O Khanna, *Samrat.khanna@iar.ac.i, Department name Computer Science and Engineering Institute of Advanced Research , Gandhinagar.*

1. INTRODUCTION

IoT term was invented by Kevin Ashton in the year 1999. The main goal of IoT was for promoting the Radio Frequency Identification (RFID) concept. RFID includes sensors, actuators and program counter. However, the original idea of IoT was discovered in the 1960s. In 1960, IoT was known as pervasive computing or embedded Internet. IoT vision is to connect anything, anyone, everywhere and at any time via identification technologies. The identification technology such as bar codes, smart cards, biometrics, sensors and voice recognition which are connected through wired or wireless systems. This vision will give a different view of the opportunities and challenges for IoT. The main concept behind IoT is to highlight the interconnection between reality/ realism and physical world via the Internet. IoT follow the hyper connectivity concept, which refers organization and individual‟s person can contact or communicate with each other from worldwide locations.
IoT deals in industry with wide range of software/application such as transportation, smart cities, agriculture, emergency services, medical services, education sector services and logistics. The IoT is the collection of devices that are both connected and smart. The IoT devices are rooted with hardware, software, sensors, and network connectivity. IoT network connectivity enables collect and exchange of data via network. IoT application can be controlled remotely across worldwide network infrastructure locations; this creates an opportunity for more direct integration of devices into IoT network which results in more improve, efficient and accurate.



Graph 1: The growth and Market Value of IoT devices in Healthcare Sector

Healthcare sector is the fast-growing industries in IoT with existing various applications like as remote monitoring to integrated mobile medication devices. Health-monitoring products enable the patient to monitor their blood pressure, nutrition, pulse, fitness and receive real-time feedback from hospitals, doctors. These identification devices are rooted with smart healthcare system and are simultaneous to a network to collect and send patients‟ data via the internet. [1] IoT healthcare system requires a healthcare bionetwork which include human, process and technology. In general way, there are four main components of an IoT Healthcare System[2] which are Data, Devices, Human and Process. Data represents all the health information obtained and stored in an IoT Cloud. Devices consist of all medical equipment that are built IoT-ready, while People refer to all stakeholders in the healthcare practice such as doctors, patients and all types of medical practitioners. Finally, the Health-related process represents, namely, Care Delivery, Wellness and Preventive Care. Figure 1 represents the how an IoT Platform works in healthcare system

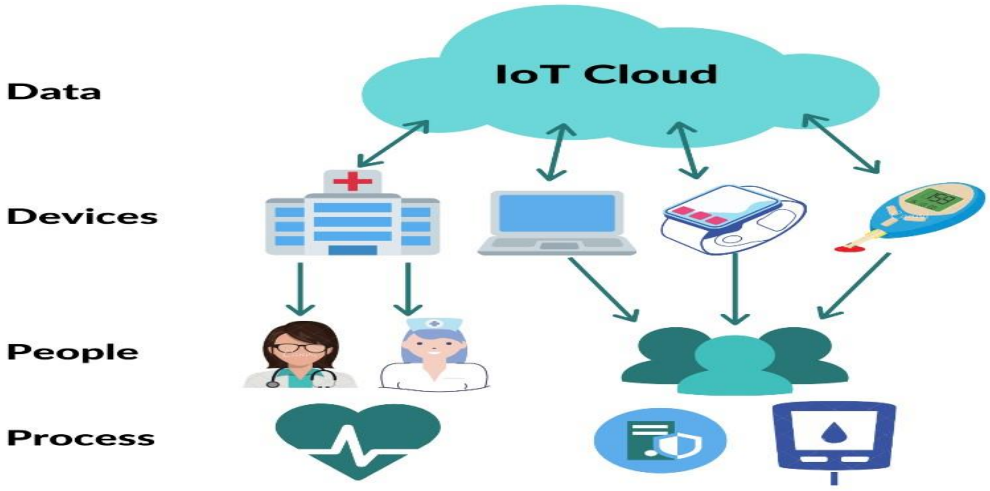


Fig.1 IoT Platform for Healthcare system

2. RELATED WORK

2.1Medical Internet of Things (MIoT)

Medical Internet of Things is the collection of devices associated through internet, to perform the processes and provide the services of healthcare sector. MIoT developing as a new technology in computer engineering for e-healthcare. MIoT devices collect vital body parameters of patients and monitors their medical details by wearable devices or sensors in body. MIoT has provide better people‟s health and supports wide range of application from wearable devices or sensor implantable in human body. Normally, MIoT structure is combination of three layers, respectively Perception layer, Network layer, and Application layer, as shown in Fig. 2.

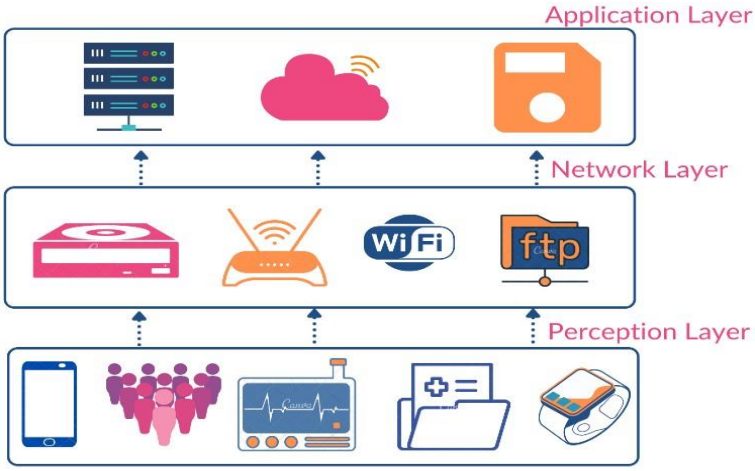


Fig.2 Structure of Medical Internet of Things

The main role of the perception layer is to collect data from human with help of IoT enabled medical devices. The network layer, which is composed of wireless and wire system, processes and send/submitting the i/p data receive by the perception layer. Network layer work with OSI transport protocols layer for transmission data and reduce energy consumption, and also ensure security and privacy of human data. The application layer integrates the information resources to provide medical services and fulfil users‟ needs

2,2 Security and Privacy Concerns

IoT is the networking of wired devices that are connected to each other to serve a specific purpose. With help of various software and sensors, these devices manage to share their data. The necessity of IoT has been increasing exponentially, as its application covers various sectors and tenacities, including education, infrastructure, business development, daily communication, and transportation. As these IoT devices consists of sensors and actuators, the technology becomes a part of cyber-physical systems, where the control of mechanism lies in the algorithm used to develop the embedded systems. There is a huge variety of available IoT application, ranging from home appliances such as lighting, colling/heating systems, and microwave ovens to large organizations including governments for smart parking, tolls, e-challans, etc. Experts are predicting that by the year 2025 there would be at least 30 Billion devices in IoT networks by 2022.
[3] Fortunately, a substantial portion of these will be having medical applications, consisting of daily gadgets such as fitness band and health trackers, to medical equipment such as pacemakers and cochlear implants, to hospital scale devices such as infusion pumps, ventilators and vital tracking monitors, mobile medical workstations and ambulances. The cyber security risks and unwanted access into IoT devices have seen a growth leading to misuse of data and losing of information eventually resulting in crisis. Such inappropriate security attacks increase the chances of data breaches and other threats, which may encounter in loss of data, property or human life. The primary reason of such attack being weak security policies which happen to be easily intercepted during wireless transfer. In late 2015, a team of two security researchers exposed over 68,000 medical systems that were available unprotected online, and 12,000 of them belonged to a single healthcare organization. The most troublesome of it was that most of those integrated devices found had their computers running expired versions of Win-XP, known to have lots of exploitable vulnerabilities. All of these devices were easily discoverable via Shodan, a search engine usually used to find Internet-connected devices online, and are also easy to hack via brute-force attacks and using hard-coded logins.

[4] During their research, these two infosec experts found anaesthesia equipment, cardiology devices, nuclear medical systems, infusion systems, pacemakers, MRI scanners and communications gear, all via simple Shodan queries. This is not the sole instance which may help determine the feebleness with privacy and security of IoT oriented devices. Any erroneous mindset might have led to deception of these medical equipment resulting in loss of human life, thus acting as a life taking weapon.

2.2.1 Security Issues:

It is clear now that IoT is quite diverse from traditional computers and computing devices, making it more vulnerable to security challenges in various ways:
Many devices in the IoT are produced for deployment on a huge scale. The perfect example of this is sensors.
Usually, the deployment of IoT embraces of a set of alike or nearly identical appliances that bear similar characteristics. This similarity amplifies the magnitude of any vulnerability in the security that may significantly distress many of them.

This obviously helps to decode the rise in data security and liability risks in the healthcare sector because of IoT. Another major factor adding to this risk is that these IoT device act at their own

(automatically) without human intervention, making it more vulnerable to control by end-users. One such example is of implantable cardioverter-defibrillator (or ICD) programmed monitors, used by Doctors to monitor a patient‟s heart condition conveniently from anywhere inside the hospital or withing the stipulated range defined for the device. These IoT embedded ICD devices can deliver data and statistics about a person‟s heart rhythms to a doctor. In case of abnormal rhythm, as required, the doctor may portably send signals to generate a specific amount of electrical shock to get the heart beating properly.[5] Researchers have been able to demonstrate how a malicious hacker can trigger the device to malfunction, or to intercept the signals from both ends delivering a dangerous shock, all of this without being caught.

2.2.2 Privacy:

Healthcare data are collected from IoT devices on a regular basis. These processes of information gathering takes place through remote access mechanisms which have some challenging effects to the privacy and security. Here, the data being collected by embedded sensors is transmitted to the required destination via the same Internet through which the IoT device are connected and communicate with each other. Thus, here the vulnerability lies in losing of the health data over the process of transmission. Additionally, similar sorts of healthcare data are collected from different health units, which in turn share them with other departments. Thus, is should be the utmost priority to secure these data and ensure that your network is leakproof, because healthcare data includes essential significant information about one‟s health condition.[6] The primary perspective of the utility of the IoT is solely dependent on how well it can respect the privacy choices of people. It is a prerequisite to know that the rights of privacy and user‟s privacy should always be protected under the service offered by the IoT device manufacturing company. Since data is transmitted online preferably through wireless networks, protecting the confidentiality and integrity of patients‟ records are important to ensure the correct treatments are given to the correct patients. Recent research suggested that the primary objective of any attacker is to take hold of one‟s health issues in order to blackmail or threaten that person. Therefore, the privacy of data must be protected at any cost to avoid any mishappenings. As perfectly mentioned by Tarouco[7], there are five main risks of IoT implementation in healthcare, namely (1) Risk of patients‟ privacy exposure, (2) Threats of cyber-attacks on privacy, (3) Data eavesdropping and data confidentiality, (4) Identity threats and privacy of stored data and (5) Location privacy. However, distracted by the new features and capabilities of IoT, requirements for security and data privacy aspects have been gradually unheeded.

Fig. 3. Top 5 Risk of IoT implementation Healthcare Sector

3. Privacy Issues:

The most common issues related to privacy of one‟s data are mentioned below as: -

3.1 Risks of Patients' Privacy Exposure

The primary privacy issue is to manage/control the patient‟s health data safe and confidential. A Personal Health record data (PHRD) is "an individual electronic record of health-related information that conforms to the nationally recognized interoperability standards". PHRD are pinched from multiple sources and are directly reported to electronic healthcare centre. Belonging personal information, they can become the objectives for cyber attacks ending in the private data.

3.2. Data Eavesdropping

Basically, patient‟s health data are available only to authorized persons and organization. However, such data can be out while flowing over the wireless links. For Ex., IoTbased insulin delivery system use wireless communication links, which are frequently used to launch privacy attacks and therefore needs sufficient protection of the transferred data**.**

3.3. Ownership of data

Every country has laws to protect his people‟s health data but government law vary from state to state. moreover, in certain cases, such as in case with fitness wearable devices , many people would think that the data tracked and collected is be bound to be protected by government law but in many cases it is not.

3.4. Location privacy

Location privacy is concerned with eavesdropping on a patient‟s location. Location privacy in WSNs, specifically hiding the message sender‟s location, can be achieved through routing to a randomly selected intermediate node (RRIN).

4 Attacks

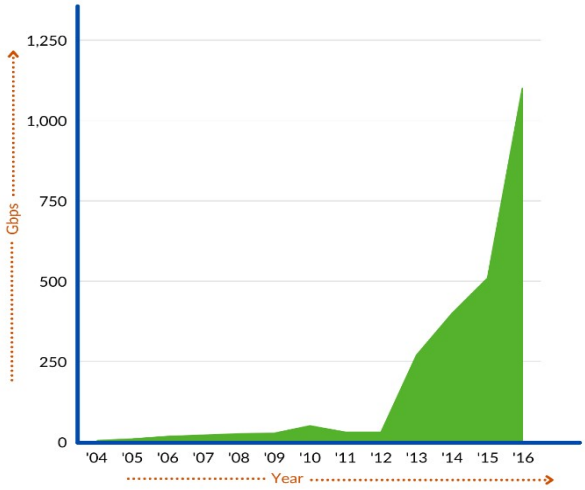
4.1 Distributed denial of service (DDoS)

Distributed denial of service (DDoS), is an attack where multiple compromised systems are used to target a single system causing a denial of service and eventually resulting that system to crash. To understand better, here,
a hacker temporarily manages to take control of a number of internetenabled devices into an arrangement regarded as botnet and then make simultaneous requests to a server or a group of servers for a specific service, thereby overwhelming the server with bogus requests and make it ignore legitimate requests from end-users. A hacker can do this for different reasons, earlier it was for bragging rights and financial gains, but in today‟s world, it may be used to take control of any hospital server and extract the database or disrupt the working efficiency. For an instance, Anonymous, a decentralized group of hackers besieged the Boston‟s Children‟s
Hospital with a DDoS attack after the hospital firmly asked one of their patients, a 14-year-old girl, to be admitted as a ward of the state and that custody to be withdrawn from her parents. The doctors

of BCH believed the child‟s ailment was actually a psychological illness and that her parents were pushing for unnecessary treatments for a disorder the child did not have.

This was followed by a custody debate, surrounding Boston Children‟s Hospital in the middle of this controversial case, and some, including members of Anonymous, viewed this as an infringement on the girl‟s rights, therefore steering DDoS attacks against the hospital‟s network, which resulted in others on that network, including Harvard University and all its hospitals, to lose Internet access as well. The networks experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information, according to the Boston Globe. As a result, the hospital spent more than $300,000 responding to and mitigating the damage from this attack, according to the attacker‟s arrest affidavit.[8] Remark 1. The below graph represents the statistics of the largest attacks faced by the Hospitals of United Stated of America in terms of incoming traffic rate represented through Gigabits per second on yearly basis between year 2004 and 2016.

(1Gbps = 106Kbps or 109 bps)



Graph 2. The biggest DDoS attacks on Hospitals encountered each year

Some of the individual connected medical devices, like pacemakers, can only send statistics information, while others hold the power to send as well as receive data. This may leave the patients vulnerable to a hacker trying to harm (or kill) them or use their device as a portal to access medical data, without any risk of getting caught. Billy Rios, a security researcher who helps the US Department of Homeland Security proved he could remotely administer a lethal dose of drugs through a patient‟s insulin pump. Following this, his team was ultimately able to figure out the passwords. Since then, the Food and Drug Administration (FDA), which is assigned to regulate the sale of medical devices, has been helping out with formal guidelines on the issue. They have also been publishing new recommendations on how medical device makers should take cyber-security attacks into account.[1]

4.2 Medjacking

Fig. 4 Pictorial Representation of Medjacking

Medjacking, as the name suggests is the process of hijacking the biomedical devices available in hospitals in order to create backdoors with the intention to harm and/or threaten a patient. In history, this process of attack has been commonly referred to as „a ticking time bomb" and the threat is considered so dangerous that the FDA, HITECH and HIPPA (US) have been constantly working to countermeasure and eradicate such disasters. Healthcare institutions continue to remain attractive targets because of all of the internet-connected systems and medical devices. This presents an attacker with a highly connected community that brings these vulnerable medical devices together with high value patient data. All it takes is one successful attempt for the attacker to establish a backdoor, find and steal data, or use automated tools to set a ransomware attack in motion. The list of devices vulnerable to MEDJACK and MEDJACK.2 is very large. This includes diagnostic equipment (PET scanners, CT scanners, (infusion pumps, medical lasers, surgical machines), life support equipment (heart - lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines) and more. As we noted above, most of these devices run standard and often older operating systems and the medical devices" proprietary internal software. TrapX recently released a report[9] providing details about incidents of medjacking (MEDJACK.2) stating of its reference in three hospitals. For an instance, with the case of the one hospital, the attackers infested multiple medical machines including Radiation Oncology System, Trilogy LINAC Gating System (both of them used in treatment of cancer) and the Fluoroscopy Radiology System (Fig. 5). Reports by TrapX suggest that they used two various forms of Malware on these old and vulnerable Windows XP systems to steal passwords to access other systems in the hospital, along with some confidential data belonging to the hospital association.

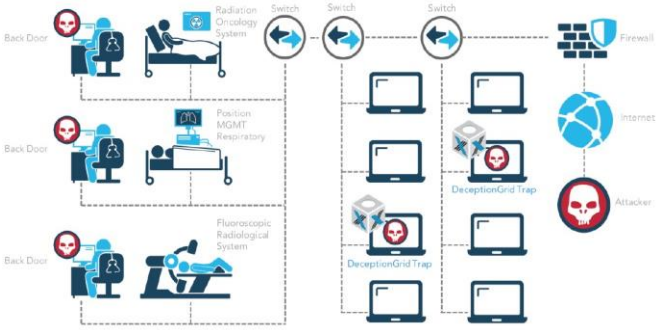


Fig. 5 Diagrammatical Representation of Attack Process (Source: TrapX)

Insulin pumps are medical devices that automatically delivers required dose on insulin to the body at a frequency predefined by the doctor. It also holds the functionality to release insulin in body in case of irregular change in body sugar levels to prevent any sorts of medical emergencies relating to it. The Animas OneTouch Ping and Medtronic, are two of the companies that sold these Insulin Pumps with a feature of wireless remote control that patients could use to order the pump to deliver a dose of insulin without awkwardly pressing buttons on the attached device under the clothes. The hackers, using signal-boosting equipment and brute-force technique managed to get into the insulin pump system and thus control the pump through their application (Fig. 6). All they had to do is generate a specific frequency to overdose the patient with insulin before the machine could detect security issues and alert the patient.

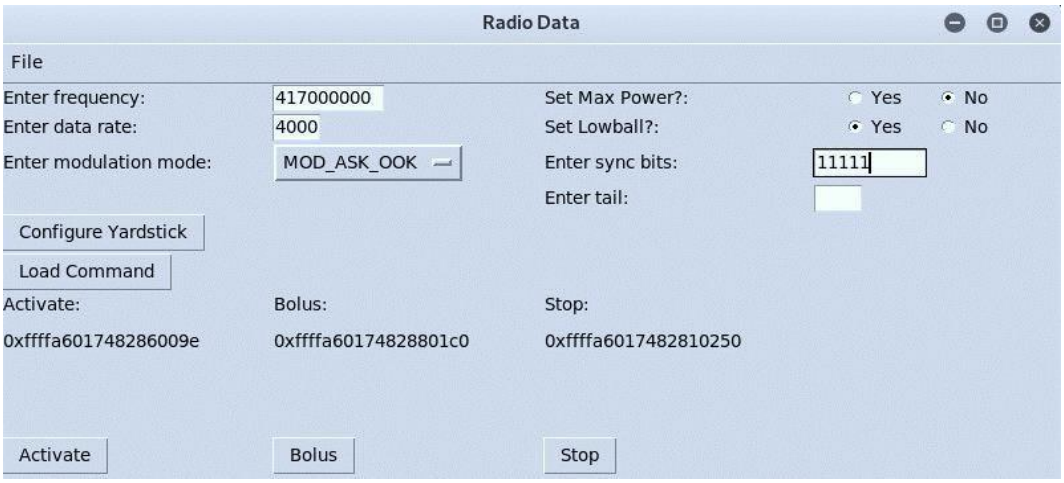


Fig 6. Screenshot of Attackers Computer (Source: QED Security Solution[10]

Medjacking has been continuously evolving, adding newer layers of camouflage to the strategies of the attackers. Through such attacks the attackers hold the power to launch cyber-attacks on hospitals, and exfiltrate data leading to breach in data integrity and resulting in probable manipulation in an individual‟s health.[9] Clearly, biomedical devices have a profoundly beneficial impact on the quality of healthcare. But medjacking is an unescapable and grave threat, and traditional security solutions being offered are not proving to be effective enough for IoMT security, and thus requires a proper attention to overcome all the security challenges.

5. PRPOSED WORK

All sorts of security measures need to be incorporated while designing the IoT device keeping in mind all forms of risk and strategy to overcome them. Some of the primary facts to be ensured are implementation of Privacy enhancing technologies (PET), improvisations to new data encryption techniques as well as to establish some strict Access control to avoid jeopardy of such active and passive attacks from happening. [11] Privacy enhancing techniques include ways to fulfil the customer's privacy requirements by various implementations in technology such as Virtual Private Networks (VPN), Transport Layer Security (TLS), DNS Security Extensions (DNSSEC) and Private Information Retrieval (PIR) System. Cryptography is a technique where a plain text is transformed into cipher-text using numerous encryption algorithms. The message transmission takes place through public channel making it important to generate a cipher text. Data encryption can be done via three levels of communication mode: (1) link encryption, (2) node encryption, (3) end-to-end encryption. In link encryption, the message receive from the former link will be decrypted into

plaintext and plaintext to cipher text by help secret key of next link. Node encryption does not allow messages in plaintext form in the network node. thus, node encryption can provide more security for network. When using end-to-end encryption, the message is not decrypted until it will not transmitting to the destination node. Because messages are always present as cipher-text throughout the transmission process and there is no leakage of information, even any node is corrupted.[3] Access control refers to the mechanism through which a data system is created containing identity of a user along with some set of rules and policies to prevent access to its resources by any unauthorized user. Some common encryption method applied in access control include symmetric key encryption, asymmetric key encryption, and attribute-based encryption

6 CONCLUSION:

A variety of medical devices along with software relating to healthcare sectors are being developed and utilized to expand the eminence of medical services in monitoring and curing the patients. Thus, lately, the demand and innovation to various IoT devices and its application in this sector has seen an exponential growth. These devices primarily deal with private information of individual‟s healthcare, including their vitals and past history of their medical conditions. This may turn out to be a disadvantage giving the attackers a chance to control your body‟s health by modifying medical equipment and devices. Therefore, it is important to identify the features of security requirements in IoT Healthcare segments, followed by some precise and sensitive steps to overcome all the vulnerabilities and make IoT a safer environment for medical sector.

References

[1]. A. Chacko and T. Hayajneh, “Security and Privacy Issues with IoT in Healthcare,” EAI Endorsed Trans. Pervasive Heal. Technol., vol. 4, no. 14, pp. 1–7, 2018, doi: 10.4108/eai.13-7-2018.155079. [2] F. I. Salih, N. Azaliah, A. Bakar, N. H. Hassan, F. Yahya, and N. Kama, “IOT Security Risk Management Model for Healthcare Industry (Special Issue 2019) pp. 131-144 IOT SECURITY RISK MANAGEMENT MODEL FOR HEALTHCARE INDUSTRY,” pp. 131–144, 2019.

[2]. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and Privacy in the Medical Internet of Things: A Review,” Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/5978636.

[3]. “Thousands of IoT Medical Devices Found Vulnerable to Online Attacks.” https://news.softpedia.com/news/thousands-of-iotmedical-devices-found-vulnerable-to-online-attacks493144.shtml (accessed Mar. 20, 2021).

[4]. D. Thilakanathan, Y. Zhao, S. Chen, S. Nepal, R. A. Calvo, and A. Pardo, “Protecting and Analysing Health Care Data on Cloud,” in Second International Conference on Advanced Cloud and Big Data, 2014, pp. 143–149, doi: 10.1109/CBD.2014.25.

[5]. C. Eken and H. Eken, “Security Threats and Recommendation in IoT Healthcare,” Proc. 9th EUROSIM Congr. Model. Simulation, EUROSIM 2016, 57th SIMS Conf. Simul. Model. SIMS 2016, vol. 142, pp. 369–374, 2018, doi: 10.3384/ecp17142369.

[6]. Tarouco et al., “Internet of Things in healthcare: interoperability and security issues,” in conference on communications (ICC), 2012, pp. 6121–6125.

[7]. “DDoS Attacks: In the Healthcare Sector.” https://www.cisecurity.org/blog/ddos-attacks-in-thehealthcare-sector/ (accessed Mar. 20, 2021).

[8]. T. R. Labs, “MEDJACK.2 Hospitals Under Siege,” pp. 1–30, 2016.

[9]. “Hackers Made an App That Kills to Prove a Point | WIRED.” https://www.wired.com/story/medtronicinsulin-pump-hack-app/ (accessed Mar. 20, 2021).

[10]. Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A. (2021). Vulnerability Analysis at Industrial Internet of Things Platform on Dark Web Network Using Computational Intelligence. In: Bansal, J.C., Paprzycki, M., Bianchini, M., Das, S. (eds) Computationally Intelligent Systems and their Applications. Studies in Computational Intelligence, vol 950. Springer, Singapore. https://doi.org/10.1007/978-981-16-0407-2_4

[11]. R. H. Weber, “Internet of Things - New security and privacy challenges,” Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, 2010, doi: 10.1016/j.clsr.2009.11.008.

[12]. Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A. (2021). Blockchain-Based Model for Expanding IoT Device Data Security. In: Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A. (eds) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol 1319. Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5

[13]. Anand Singh Rajawat, Pradeep Bedi, S. B. Goyal, Piyush Kumar Shukla, Sajjad Shaukat Jamal, Adel R. Alharbi, Amer Aljaedi, "Securing 5G-IoT Device Connectivity and Coverage Using Boltzmann Machine Keys Generation", Mathematical Problems in Engineering, vol. 2021, Article ID 2330049, 10 pages, 2021. https://doi.org/10.1155/2021/2330049

[14]. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions,” Appl. Sci., vol. 10, no. 12, pp. 1–17, 2020, doi: 10.3390/APP10124102. [13] S. Nasiri, F. Sadoughi, M. H. Tadayon, and A. Dehnad, “Security requirements of internet of thingsbased healthcare system: A survey study,” Acta Inform. Medica, vol. 27, no. 4, pp. 253–258, 2019, doi: 10.5455/aim.2019.27.253-258.

[15]. Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N., Ghosh, A. (2022). Reliability Analysis in Cyber-Physical System Using Deep Learning for Smart Cities Industrial IoT Network Node. In: Piuri, V., Shaw, R.N., Ghosh, A., Islam, R. (eds) AI and IoT for Smart City Applications. Studies in Computational Intelligence, vol 1002. Springer, Singapore. https://doi.org/10.1007/978-981-16-7498-3_10

[16]. X. C. Yin, Z. G. Liu, B. Ndibanje, L. Nkenyereye, and S. M. R. Islam, "An iot-based anonymous function for security and privacy in healthcare sensor networks," Sensors (Switzerland), vol. 19, no. 14, Jul. 2019, doi: 10.3390/s19143146.

[17]. K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets," arXiv, pp. 1–17, 2017.

[18]. M. Gloukhovtsev, "Iot Security: Challenges, Solutions & Future Prospects," pp. 1–44, 2018, [Online]. Available:https://education.dellemc.com/content/dam/ dell-emc/documents/en-us/2018KS_GloukhovtsevIoT_Security_Challenges_Solutions_and_Future_Pros pects.pdf.

[19]. D. Dziak, B. Jachimczyk, and W. J. Kulesza, "IoTbased information system for healthcare application: Design methodology approach," Appl. Sci., vol. 7, no. 6, 2017, doi: 10.3390/app7060596.

[20]. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278– 4209

[21]. O. C. Is, "HC3 Intelligence Briefing **** Botnet Threat to the Healthcare Industry ***," 2020. [19] W. Boonyanusith and P. Jittamai, "Transforming Blood Supply Chain Management with Internet of Things Paradigm Transforming Blood Supply Chain Management with Internet of Things Paradigm," Proc. Hambg. Int. Conf. Logist., vol. 23, p. 23, 2017, [Online]. Available: https://pdfs.semanticscholar.org/855d/163941e536b16 5ada2fc739160a5a68cd5a8.pdf.

[22]. "Hackers create more IoT botnets with Mirai source code | PCWorld." https://www.pcworld.com/article/3132571/hackerscreate-more-iot-botnets-with-mirai-source-code.html (accessed Mar. 20, 2021).

[23]. "Healthcare‟s „Internet of Things‟ should be the „Security of Things‟ | Healthcare IT News." https://www.healthcareitnews.com/blog/healthcaresinternet-things-should-be-security-things (accessed Mar. 20, 2021).

[24]. Kumar, R., Singh, J.P., Srivastava, G. (2014). Altered Fingerprint Identification and Classification Using SP Detection and Fuzzy Classification. In: , et al. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1602-5_139

[25]. "Medjacking: The newest healthcare risk? | Healthcare IT News." https://www.healthcareitnews.com/news/medjackingnewest-healthcare-risk (accessed Mar. 20, 2021).

[26]. Gite S.N, Dharmadhikari D.D, Ram Kumar," Educational Decision Making Based On GIS" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-1, April 2012.

[27]. "Medjacking – An Epidemic in Healthcare | Healthcare IT News." https://www.healthcareitnews.com/sponsoredcontent/medjacking-–epidemic-healthcare (accessed Mar. 20, 2021).

[28]. Ram Kumar, Sarvesh Kumar, Kolte V. S.," A Model for Intrusion Detection Based on Undefined Distance", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1 Issue-5, November 2011

[29]. "IoT in Healthcare: Use Cases, Trends, Advantages and Disadvantages | Existek Blog." https://existek.com/blog/iot-in-healthcare/ (accessed Mar. 20, 2021).

[30]. Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N., Ghosh, A., Aggarwal, S. (2022). Anomalies Detection on Attached IoT Device at Cattle Body in Smart Cities Areas Using Deep Learning. In: Piuri, V., Shaw, R.N., Ghosh, A., Islam, R. (eds) AI and IoT for Smart City Applications. Studies in Computational Intelligence, vol 1002. Springer, Singapore. https://doi.org/10.1007/978-981-16-7498-3_14

[31]. Vibhor Mahajan, Ashutosh Dwivedi, Sairaj Kulkarni,Md Abdullah Ali, Ram Kumar Solanki," Face Mask Detection Using Machine Learning", International Research Journal of Modernization in Engineering Technology and Science, Volume:04/Issue:05/May-2022