INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of First International Conference on Management, Science and Technology (ICMST 2021)

Internet of Things (IOT)-Data Security Challenges and Solutions

N.Priyanka[1], D.Swetha[2], G.Anjali[3]
[1,2,3] Assistant Professor, Department of Computer Science, RBVRR Women's College, Telangana, India
Priyankanandi08@gmail.com[1], dastariswetha@gmail.com[2], anjalig0411@gmail.com[3]

Abstract

Our everyday life starts with an electronic device with internet connectivity. Today every object of our lives is relying on internet and the powerful data capability which transforms the way we work and live. In this pandemic situation of COVID-19 every company/business/organizations/educational institution and many more are working only with the help of internet connectivity and new emerging technologies. Internet of Things (IoT) is one such technology that has gained as a popular research concept from recent years and it is playing a vital role in the pandemic situation of COVID-19 by incorporating technological, business and social scenarios. As there is an increase in the usage of IoT devices and more IoT ecosystems there by facing many challenges like technical, business, societal and legal. Among the all-Data Security is being the most prominent one. This article discusses different ways the data can be protected on IoT devices by which the enterprises can successfully ensure secure data on IoT devices.

Keywords: COVID-19, IoT, IoT devices, Data Security.

1. Introduction

Internet of Things (IoT) as known, it is where billions of physical devices are all connected, there by collecting and sharing the data. IoT gives intelligence to different objects/devices to communicate, by adding sensors and making them to work with real time data without the involvement of human being. IoT is used mainly on those devices which are not expected to have an internet connection and without any interference of human being, for example PCs and Smartphones are not considered as IoT devices generally, rather fitness trackers, medical sensors, home automation devices, TV's, Camera's etc are all considered as IoT devices. The history of IoT started in early 1980's where the projects were progressing slow because of the big and bulky chips, by which the communication between devices was simple. But with the adoption of RFID tags the chips were able to communicate wirelessly and with the adoption of IPV6 every device used over the world was provided with IP address.Developing IoT devices with network connectivity is easy however deploying IoT apps and providing it globally is another task. But network connectivity is not only the one that can be considered, there are many other things which can disrupt the connectivity like cell towers, proxy servers, slow/fast connectivity and firewalls. Based on the connectivity issues IoT faces some of the challenges like signalling, security, presence detection, and bandwidth and power consumption. Among the all-challenges, security is being the most important factor in the pandemic situation of COVID-19. With the increase in number of IoT devices and IoT ecosystem there is an increase in security vulnerabilities. The world has been struggling with the pandemic situation caused by Coronavirus since 2020, where it forced entire countries to propose lockdown in order to reduce the spread of virus. There by all educational institutions, business, industries, multi-national companies,

different organizations required to work from home. With this the role of IoT and internet connectivity became crucial and important.[1-5].

1.1 IOT in Healthcare

IoT technology playing an important role in health sector during COVID. IoT devices were used to speed up the process of detecting people by taking information from patients, by capturing the body temperature and taking samples. When people are detected with the virus and asked to isolate themselves at home, IoT devices were used to monitor patients remotely and also to disinfect the areas affected. Examples of IoT devices used are tracking wearable bands, disinfecting devices, drones, robots, smart phone applications and more. If it observed each and every device will be storing some or other data with in it. Privacy of data is still a substantial issue. For example, a health monitor tracks information of the patients for hospital's medical reports. Hackers can manage to steal the data that violates the hospital's privacy policy.

1.2 IoT in Remote Education

Though the physical closing of educational institutions due to the pandemic of COVID-19 had halted the teaching process initially, in a hope to return to normal functioning. But as things took a different turn and as one could not even predict how long will this go on, learning management systems and digital tools for online collaboration ensured a safe distance and continuity of teaching-learning process. However, this rapid transition to remote learning in has created a number of challenges in higher education. The possibilities of IoT technology for continuous monitoring and flexible management of the learning process were explored. Whether it's via laptops, tablets, or smartphones, remote learning would not be possible without connected devices. IoT components like web cameras, wearable sensors, microphone, GPS tracker are used in giving lectures and seminars, for laboratory classes, examinations and attendance using the machine Learning algorithms like face recognition, Deep learning, classification algorithms. Though the IoT is helping out in continuation of teaching-learning process, the data that is collected is vast and hackers are targeting IoT devices such as routers, webcams and also the smartwatches which is allowing them to track the wearer's location or even communicate.

1.3 IOT in Business

IoT is the most important and crucial part in business and manufacturing where it has turned homes and offices smarter. People spending much on IoT for their smart home, personal wellness, connected vehicles, wearables and much more. Thereby the industries spend more on such components on manufacturing, transportation, asset management, fleet management etc. Utilities will be the most important user of IoT. COVID-19 pandemic has disrupted the manufacturing, supply chain and all other processes of business and forced the companies to shut down, where lot of people and companies has faced great loss. IoT was the most useful technology that helped businesses to continue. It allowed the employees to collaborate remotely by using IoT-based solutions and one such example is Manufacturing Execution System (MES) which is a US tier-one supplier, used by managers for important discussions in videoconferences that provides a valuable output. Manufacturers have restarted their process by using IoT-based solutions such as remote monitoring of production setup and machinery, machine learning software to perform automated tasks and many more. Companies which need a lot of man power for supply chain started using IoT technology for smooth and transparent flow of material with few men power. IoT devices for warehouses, GPS for routes and digital formats for paper processes are used by the companies.As many industries and companies adopted IoT devices which stores a numerous amount of data on cloud which they use that data for any future decisions. But cyberattacks on the other hand is posing vulnerabilities on IoT devices. Every IoT device that are used in industries are vulnerable to cyberattacks.[6-10].

2. Challenges and Techniques to overcome the Data Security

2.1 Challenge 1: Guessable credentials are a bonus for hackers to attack the IoT device directly. Using default passwords, the attackers may know the passwords of the machines. Mirai Malware is a good example of such kind of attacks in 2016. In early 2020 ZDNet, a business technology news website, has given information and detailed how the hackers have obtained a dump of credentials of telnet servers, routers and IoT devices by using default usernames, passwords and guessable

default passwords', a type of Mirai attack has become the most active botnet from 2019.

Solution: IoT device manufacturers has included mechanisms like password complexity and expiration, one time password which ensures the users modify the credentials of the device. IoT identity and Access Management solutions have been used by the network managers which have a wide range of device management features that reduces the exposure of IoT attack.

To ensure that the devices which are connected cannot be accessed by unauthorized user, Two-factor authentication, multi-factor authentication, biometric authentication and digital certificates will be helpful. Gartner, a global research and advisory firm, has mentioned that Privileged access Management (PAM) is essential for the devices for reducing IoT security issues and ensures IoT network cannot be hacked.

2.2 Challenge 2: At the time of purchase, the IoT devices will be secured but later hackers can find a new security bugs. These has to be fixed with regular updates or they will be exposed to vulnerability. One such kind of attack is Satori which is similar to Mirai. It first targets the known vulnerabilities in a specific range of WiFi routers and then delivers a worm by which the infection spreads from one device to another with no human interaction.

Solution: For this to get fixed the enterprises and manufacturers should go an extra mile by providing security updates for the IoT devices and network managers should include only signed updates and exchange encrypted formats for ensuring authenticity.[10-14].

2.3 Challenge 3: IoT devices will process the data and also communicate with data, for this it needs apps, services and different protocols. These interfaces can be insecure and can be related to web, application API, mobile interfaces. Issues that arise include insufficient device authentication, authorization and weak encryption.

Solution: In order to get rid of such issues Device authentication is used to provide secured access to devices and applications, for the people who are only authorized. Digital certificates which enable the digital objects/devices to securely transfer the data to authorized users. X509 certificates are standard certificate formats that allow the user to identify each IoT device uniquely. NIST and ENISA has provided documents since 2019, that details how to implement security for IoT by design, for latest security standards and protocols which are recommended for manufacturers to read and follow.

2.4 Challenge 4: Insecure communications and data storage is another challenge of IoT applications, where the compromised devices are used to access the confidential data. The hackers have accessed a database of big spenders by accessing the network through a thermostat attached to a fish tank, this was the information revealed by researchers in 2017. With the help of smart toys the hackers were able to access the data via Bluetooth with no password protection and the children who are playing with such dolls were in danger as per security and privacy.

Solution: In order to fix a solution cryptography is effective technology. Data encryption and decryption ensures the data privacy and confidentiality and reduces the risk of lost or theft of data. This cryptography fixes the eavesdropping attack and man-in-the-middle attack, where the hackers capture related messages and puts new ones between the two communicating devices.

2.5 Challenge 5: Another challenge is the poor maintenance of IoT devices. The connections between organizations are becoming unsafe and putting them in risk.

Ransomware is one such malware which is targeting healthcare more in US. By 2020 the ransomware attacks have risen with 50%, according to a research paper. This kind of attacks understand how to stop critical applications and they hold the patient's data and they can put their lives at risk so that the health organizations have to pay a deal. [12-16].

Solution: But these attacks can be reduced with the help of IoT device management platforms, which provides class-leading lifecycle management capabilities that can be deployed, monitored, maintained and update the devices. With device management the security risks were reduced as it provides end-to-end solution needs.

Other solutions: Industries are using the cybersecurity solutions such as Blackberry security software services. Cisco IoT solutions and services, Subex IoT security coverage from real-time monitoring to response and recovery. Bitdefender BOX IoT device security, F-secure

detection and response solutions, ZingBox cloud-based solution for IoT. Block chain technology enables the privacy and security of data sharing and it is one of the fastest growing trendy technologies. Artificial intelligence and different technologies of AI, is another way of assisting the devices that are in communication.

Conclusions

IoT plays a very important role in every field such as health care, forecasting the situation of future, academics, corporate professionals, supply chain, manufacturing and many more thereby reducing the risk of spread of COVID-19. Though it faces a lot of challenges people across the world are trying to provide the effective solutions to fix the challenges. By implementing the solutions with less computational cost one can win in providing the IoT services with proper security.

References

Web Sources:

[1]. https://www.pubnub.com/blog/5-challenges-of-internet-of-things-connectivity/
[2]. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats
[3]. https://www.verimatrix.com/markets/internet-of-things/?utm_term=iot%20devices%20security&utm_campaign=Asia+-+IoT+-+EN&utm_source=adwords&utm_medium=ppc&hsa_acc=5556708784&hsa_cam=9520856355&hsa_grp=97551877872&hsa_ad=421714927160&hsa_src=g&hsa_tgt=kwd-337405655921&hsa_kw=iot%20devices%20security&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI76XW0-3T8AIVTg9yCh0k5A-bEAAYASAAEgLE5vD_BwE
[4]. https://www.lepide.com/blog/how-to-secure-data-on-iot-devices-in-5-easy-steps/
[5]. https://www.sciencedaily.com/releases/2019/10/191010164838.htm
[6]. https://link.springer.com/article/10.1007/s41666-020-00080-6
[7]. https://www.internetsociety.org/resources/doc/2015/iot-overview/?gclid=EAIaIQobChMIksGKxO7T8AIV_4dLBR31LwpAEAAYASAAEgLqvfD_BwE
[8]. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
[9]. https://www.researchgate.net/publication/343229055_IoT_meets_COVID-19_Status_Challenges_and_Opportunities
[10]. https://iotbusinessnews.com/2020/07/27/04054-how-businesses-can-implement-iot-to-restart-during-covid-19/
[11]. https://auto.economictimes.indiatimes.com/news/industry/opinion-iot-key-to-indias-plans-for-secure-efficient-covid-19-vaccine-delivery/82455064
[12]. https://www.internetsociety.org/resources/doc/2015/iot-overview/?gclid=EAIaIQobChMIksGKxO7T8AIV_4dLBR31LwpAEAAYASAAEgLqvfD_BwE
[13]. https://www.sciencedaily.com/releases/2019/10/191010164838.htm
[14]. https://www.apriorit.com/dev-blog/521-iot-toy-attacks
[15]. https://nymag.com/intelligencer/article/ransomware-attacks-2021.html
[16]. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html