International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Review Paper Volume-9, Issue-5, 2022 Regular Edition E-ISSN: 2349-7084

Internet of Things (IoT) in Mining: Security Challenges and Best Practices

*Rayikanti Anasurya

Academic Consultant, Electronics and Communication Department ,University College of Engineering, , Kakatiya University, Badradri Kothagudem, Telangana.
Corresponding Author Email: anuravikanti7@gmail.com

Available online at: http://www.ijcert.org

Received: 06/03/2022, Revised: 09/04/2022, Accepted: 19/05/2022, Published: 26/05/2022

Abstract: Data-exchanging computer devices that are built into everyday items and linked to the internet. The Internet of Things is one of the modern technological inventions that is developing the fastest (IoT) By 2025, more than 27 billion connected gadgets are expected to exist globally, according to IoT Analytics. But increasing security concerns over issues like software bugs and hackers may detect many users from using IoT devices. For companies working in the healthcare, finance, Mining, manufacturing, logistics, retail, and other sectors that have already started adopting IoT devices, these IoT security issues are especially crucial. The definition of IoT security, its significance, and the major threats it is vulnerable application in mining are covered in this paper.

Keywords: Data; IoT; Security; Communication; Gateways, Mining.

1. Introduction

Computer gadgets that are integrated into common objects and are connected via the internet to exchange data. One of the current technology innovations with the quickest rate of development is the Internet of Things (IoT). IoT Analytics predicts that by 2025, there will probably be more than 27 billion linked devices worldwide. However, growing security worries about things like software flaws and hackers may discourage many users from utilising IoT devices. These IoT security issues are particularly important for businesses operating in the healthcare, finance, manufacturing, logistics, retail, and other sectors that have already begin implementing IoT devices. In this chapter, we discuss the definition of IoT security, its importance, and the main threats it is vulnerable to. We also go over how to secure networks, devices, and data in IoT environments.

1.1 What is IoT and IoT security?

A network of intelligent gadgets known as the "Internet of Things" connects to one another and uses the internet to exchange data without the need for human involvement. Wireless networks, cloud databases for communication, sensors, data processing software, and interconnected smart devices make up the architecture of IoT systems in most cases. The following elements are used by IoT systems to exchange and process data.

Smart devices: Smart gadgets that gather information about the environment and other objects and components, store it, and then share it

Embedded systems: Smart devices use embedded systems, which can be made up of a range of processors, sensors, and communication equipment, and whose purpose is to gather, send, and act on environmental data.

IoT gateways: Devices that transit data between IoT devices and the cloud, such as IoT gateways, hubs, or other edge devices

Cloud or on-premises data centres: Data communication between remote servers and on-site or cloud data centres via wireless connectivity. Industries like manufacturing, transportation, healthcare, logistics, energy, agriculture, and more use IoT technologies. Depending on the objectives of a particular IoT system, smart devices might range from straightforward sensors to DNA analysis technology.

1.2 The most popular IoT use cases and devices are:

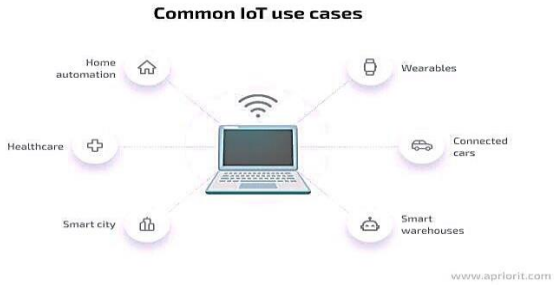


Fig 1: Common Use Cases

Home Automation Systems: Automation systems for homes keep an eye on and regulate features including lighting, temperature, entertainment, appliances, and alarm systems. Thermostats, refrigerators, plugs, and light bulbs are examples of common smart home appliances.

Healthcare Medical IoT (MIoT): Healthcare. Medical IoT (MIoT) offers numerous chances for patients to self-monitor as well as for healthcare professionals to monitor patients. Glucometers, blood pressure and heart rate monitor cuffs, and wirelessly connected fitness bands are examples of smart devices for the Internet of Things (IoT).

Smart Cities: To improve infrastructure, public utilities, and services, smart cities leverage data collected by smart devices. These gadgets can be connected to air quality monitoring equipment, waste bins, metres, lighting, and sensors.

Wearables: Sports and healthcare are the two main uses of wearable's. These gadgets include smart watches, ECG monitors, blood pressure monitors, and fitness trackers.

Connected Cars: Vehicles with internet access and the ability to share their data with devices inside and outside the car are referred to as connected automobiles. With the help of this technology, users can enhance security, remotely access car functioning via a mobile app, and automatically pay tolls.

Smart Warehouses: To help organisations enhance productivity and efficiency, smart warehouses use automated and linked technologies.

Why does IoT security matter?

Organizations must pay close attention to system security because IoT systems are used so widely. A system failure or hacking assault could result from any vulnerability, which could then have an impact on hundreds or thousands of individuals. For example, a home security system could be turned off by criminals, or traffic signals could cease operating, resulting in auto accidents. Because some IoT devices are utilised for human protection or healthcare, their security might be extremely important for people's lives.

In order to protect their data, IoT systems must place a high priority on security. Numerous cyber security laws, standards, and regulations must be followed in order to protect the massive amounts of sensitive data that smart devices collect, including personally identifiable information. A breach of such information may lead to legal action and penalties. Additionally, it can result in a loss of client trust and reputational harm. Internet of Things security is a collection of methods and procedures for defending against a variety of IoT security intrusions on the physical objects, networks, operations, and technology that make up an IoT ecosystem.

The remainder of this paper is organized as follows. In Section 2, we will provide an overview of IoT-based agriculture and sustainability, discussing the key benefits and challenges associated with this technology. In Section 3, we will explore the various applications of IoT in agriculture, including precision farming, smart irrigation, livestock management, and supply chain management. We will discuss how these applications can improve efficiency and sustainability in agriculture. In Section 4, we will delve into the challenges associated with implementing IoT-based sustainable agriculture, such as cost, complexity, and security concerns. Finally, in Section 5, we will summarize our findings and offer conclusions on the potential of IoT-based sustainable agriculture to transform the industry.

2. Key Goals of IoT Security

The two key goals of IoT security are to:

i. Make sure all data is collected, stored, processed, and transferred securely
ii. Detect and eliminate vulnerabilities in IoT components

Most common Internet of Things security challenges

a. Software and firmware vulnerabilities
b. Insecure communications
c. Data leaks from IoT systems
d. Malware risks
e. Cyber attacks

Software and firmware vulnerabilities: IoT security is challenging to maintain, mainly due to the resource limitations and low processing power of many smart devices. As a result, they are less able to conduct robust, resource-intensive security operations and are more vulnerable than non-IoT devices.

There are security flaws in a lot of IoT systems for the following reasons:

- Lack of computational capacity for efficient built-in security
- Poor access control in IoT systems
- Limited budget for properly testing and improving firmware security
- Lack of regular patches and updates due to limited budgets and technical limitations of IoT devices
- Users may not update their devices, thus restricting vulnerability patching
- With time, software updates might be unavailable for older devices

- Poor protection from physical attacks ;an attacker can get close enough to add their chip or hack the device using radio waves

An IoT system is a target for malicious actors who want to infiltrate its communications, introduce malware, and steal sensitive data. Hackers were able to access Ring smart cameras, for instance, by using weak, recycled, and default credentials. Even remotely speaking to victims over the camera's microphone and speakers was possible.

Insecure Communications: Since IoT devices have limited resources, it is challenging to deploy the majority of existing security techniques. Traditional security methods are therefore less effective at safeguarding the communication of IoT devices. The potential for a man-in-the-middle (MitM) assault is one of the most harmful dangers brought on by insecure communications. If your device doesn't use secure encryption and authentication protocols, hackers can easily carry out MitM attacks to compromise an update process and take control of your device. Even malware installation and functional changes are possible by attackers. Even if your device is not the target of a MitM attack, cybercriminals may still be able to intercept the data it transfers via clear text messages with other devices and systems.

Devices that are connected are vulnerable to assaults from other devices. Consider how quickly all other unisolated devices in a home network can be compromised if an attacker gains access to just one of them.

Data leaks from IoT systems: We've already demonstrated that hackers can access the data that your IoT system processes by intercepting unencrypted messages. This may even contain private information like your location, financial information, and medical history. Attackers can also obtain useful information by leveraging inadequately protected communications, albeit this is not the sole method. All data is transported through and kept in the cloud, and services hosted in the cloud are likewise susceptible to outside threats. As a result, both the devices themselves and the cloud environments to which they are attached could leak data.

Another potential cause of a data leak in your IoT systems are third-party services. For instance, it was discovered that Ring smart doorbells were improperly transferring user data to Face book and Google. Due to third-party tracking services being enabled in the Ring mobile app, this event occurred.

Malware Risks: Set-top boxes, smart TVs, and smart watches were determined to be the gadgets most susceptible to malware attacks, according to a recent study by Zscaler. An IoT system's functionality could be altered, personal information could be collected, and other attacks could be launched if attackers manage to introduce malware into the system. In addition, some gadgets may come pre-infected with viruses if their producers don't take proper software security precautions.

The most well-known IoT-targeted malware has already been dealt with by several firms in creative ways. A Microsoft tutorial on how to proactively defend your systems against the Mozi IoT botnet is available, and an FBI agent recently discussed how the agency stopped the Mirai botnet attacks. However, hackers continue to develop new exploits for IoT networks and devices. BotenaGo, malware created in Golang in 2021, can take advantage of more than 30 different vulnerabilities in smart devices, according to researchers.

Cyber Attacks: In addition to the malware and MITM attacks mentioned above, IoT systems can be vulnerable to a number of other intrusions. The following is a list of the most typical IoT device attack

Denial-of-service (DoS) attacks: IoT devices are extremely susceptible to denial-of-service attacks because of their low computing capability. A DoS attack compromises a device's capacity to react to real requests by flooding it with phoney traffic.

Denial-of-sleep (DoSL) attacks: In order to continuously monitor their surroundings, sensors connected to wireless networks are frequently powered by batteries that don't need to be charged frequently. By leaving the Smartphone mostly in sleep mode, battery life is prolonged. The control of sleep and wakefulness depends on the communication requirements of various protocols, such as medium access control (MAC). Attackers may use MAC protocol flaws as opportunities to launch a DoSL attack. This kind of assault depletes the battery, rendering the sensor inoperable.

Device Spoofing: A device that has wrongly integrated digital signatures and encryption is vulnerable to this attack. For instance, hackers may use a weak public key infrastructure (PKI) to "spoof" a network device and interfere with IoT deployments.

Physical Intrusion: Even though most attacks are carried out remotely, if a device is taken, it may still be physically accessed. Device parts can be tampered with by attackers to cause them to function improperly.

Application-Based Attacks: These kinds of attacks are conceivable when embedded system software or device firmware contain security flaws, or when cloud servers or backend apps have holes. Let's move on to the Internet of Things security best practises that can assist you in safeguarding your IoT system while keeping these difficulties in mind.

3. The best ways to guarantee the security of IoT systems

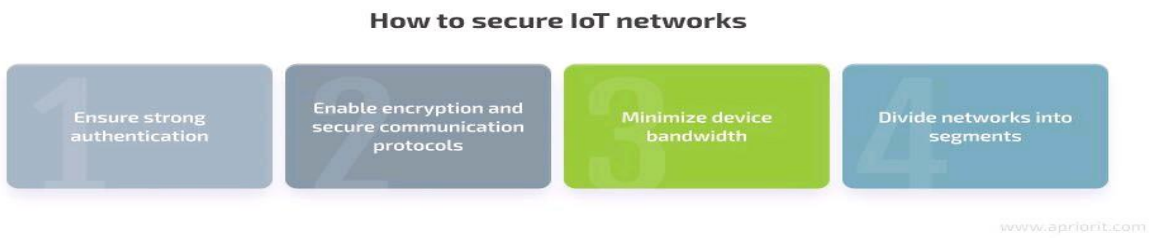
IoT security best practices can help you increase the protection of three main components of IoT systems: devices, networks, and data. Let’s start by discussing ways to secure smart devices.

Secure Smart Devices:

Fig 2: Secure smart devices

- Make sure the hardware is tamper-proof. Attackers may steal IoT devices to tamper with them or access private data. Make sure your product is tamper-proof to protect device data. By implementing port locks, camera covers, strong boot-level passwords, and other measures that will render the device inoperable in the event of tampering, you may assure physical security.
- Updates and patches are needed. Continuous device upkeep requires additional expenses. However, regular updates and patches are the only way to guarantee effective product security. It is best to implement automatic and required security updates that don't need end users to take any activity. Customers should be made aware of the length of the product's support period as well as what to do after it expires. Once your system is available, be sure to monitor future vulnerabilities and create updates as necessary.
- Conduct extensive testing. Your primary tool for identifying flaws in IoT firmware and software and minimising the attack surface to the greatest extent is penetration testing. The most blatant problems can be located using static code analysis, and concealed vulnerabilities can be discovered via dynamic testing.
- Implement data protections for devices. IoT devices should guarantee data security before, during, and after use. Ensure that non-volatile device memory is used to store cryptographic keys. You can also provide a mechanism for people to get rid of used items without disclosing private information.
- Meet the performance requirements for the component. Hardware for IoT devices must adhere to a set of performance standards to guarantee optimal functionality. IoT devices, for instance, should have high computing capability while using less power. Devices must also guarantee reliable wireless connections, data encryption, and permission. Additionally, it's better for your Internet of Things solution to function even if its internet connection is just fleeting.

Secure Networks:



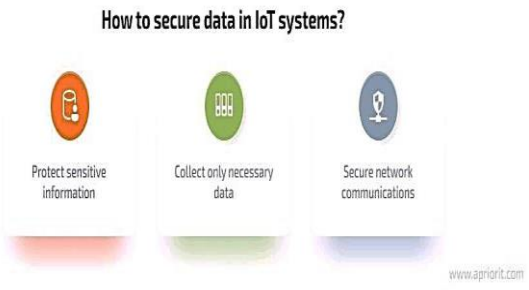
- Enable reliable authentication. By using distinctive default credentials, this is possible. Use the most recent protocols when identifying or addressing your products to ensure their continued usability. Give your product multi-factor authentication if at all possible.

- Enable safe communication methods and encryption. Security protection is also necessary for device communication. However, given the IoT devices' constrained capabilities, cryptographic algorithms should be modified. You can use Lightweight Cryptography or Transport Layer Security for these applications. You can employ wireless or wired technologies including RFID, Bluetooth, Cellular, ZigBee, Z-Wave, Thread, and Ethernet with an IoT architecture. Additionally, using optimised protocols like IPsec and Secure Sockets Layer, you can guarantee network security.

- Reduce the device's bandwidth. Only allow the amount of network traffic required for the IoT device to function. Programming the device to restrict hardware and kernel-level bandwidth and flag suspicious activity is recommended. This will defend your product against potential DoS assaults. As malware can be used to take control of the device and use it as part of a botnet to launch distributed denial-of-service attacks, the product should also be built to reboot and clean code if malware is found.

- Networks should be segmented. By dividing large networks into numerous smaller ones, you can implement next-generation firewall protection. Use IP address ranges or VLANs for this purpose. You should integrate a VPN into your IoT system for safe internet access.

Secure Data:



- Safeguard critical data. Install different default passwords for every product, or demand quick password updates upon device start-up. Make use of strong authentication to guarantee that only legitimate users have access to the data. If the user chooses to return or resell the device, you can also provide a reset function to enable the deletion of private data and wiping of configuration settings. This will go an extra mile to improve privacy protection.

- Only gather the information that is required. Make sure that your IoT gadget only gathers the information required for it to function. This will lessen the chance of data leakage, safeguard the privacy of consumers, and take care of any potential issues with non-compliance with various data protection standards, laws, and regulations.

- Communications across a secure network. Limit unnecessary communication between your product and the IoT network for increased security. Don't rely just on the network firewall, and make your product invisible via incoming connections by default to maintain secure communication. Use encryption algorithms such as the Advanced Encryption Standard, Triple DES, RSA, and Digital Signature Algorithm that are tailored to the requirements of IoT devices.

- Along with the above-mentioned procedures, be careful to abide by advice from documents like the NIST guide on IoT device cyber security, which was published in response to issues identified by the IoT Cyber security Improvement Act of 2020.

4. IoT in Mining Industry

Many major mining companies are planning and evaluating how to begin their digital journey and the digitalization of the mining industry to manage day-to-day mining operations in light of the numerous incentives it offers. Utilizing sensors on mining equipment and systems that track the equipment's performance can reduce costs and increase output. Big data is being used by mining companies to find more affordable methods to run their operations and to cut down on overall operational downtime. Utilize IoT to continuously monitor ventilation and toxicity levels in underground mines to ensure the protection of workers and machinery. It makes evacuations or safety exercises quicker and more effective. Converting servicing from preventive to predictive improved decision-making speed the mining business experiences emergencies almost every hour, often with little warning. IoT aids in balancing situations

and in helping people make wise choices when several factors are present at the same time.

4.1 Challenges for IoT in Mining

- IoT has advantages for the mining sector, but there have also been difficulties with its implementation in the past.
- Particularly in underground mine sites, there is poor or nonexistent connectivity
- Remote locations may struggle to pick up 3G/4G signals
- Declining ore grade has increased the requirements to dig deeper in many mines, which may increase hindrances in the rollout of IoT systems

4.2 Cyber security will be another major challenge for IoT-powered mines over the coming years

As mining operations become more connected, they will also become more vulnerable to hacking, which will require additional investment into security systems. Following a data breach at Goldcorp in 2016, that disproved the previous industry mentality that miners are not typically targets, 10 mining companies established the Mining and Metals Information Sharing and Analysis Centre (MM-ISAC) to share cyber threats among peers in April 2017.

In March 2019, one of the largest aluminium producers in the world, Norsk Hydro, suffered an extensive cyber-attack, which led to the company isolating all plants and operations as well as switching to manual operations and procedures. Several of its plants suffered temporary production stoppages as a result. Mining companies have realized the importance of digital security and are investing in new security technologies.

5.Concussion

It's crucial to start considering security at the research and development phases of IoT projects. However, due of the frequency of intrusions and the difficulty of looking for potential system vulnerabilities, guaranteeing effective cyber security of devices, networks, and data in IoT contexts is difficult. It can be challenging to implement strong security measures in IoT applications. In addition to clashing with hardware constraints, adding security measures could raise a solution's price and length of development, which is undoubtedly undesirable for enterprises.

It takes skilled IoT software engineers and quality assurance professionals with penetration testing experience to create secure IoT devices. At Apriority, we've put together teams of experts in security testing, embedded and IoT solutions development, and engineering for cyber security projects.

References

[1] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, “A Review on Internet of Things (IoT), Internet of Everything (IoT) and Internet of Nano Things (IoNT)”, in 2015 Internet Technologies and Applications (ITA), pp. 219– 224, Sep. 2015, DOI: 10.1109/ITechA.2015.7317398.

[2] P. J. Ryan and R. B. Watson, “Research Challenges for the Internet of Things: What Role Can OR Play?,” Systems, vol. 5, no. 1, pp. 1–34, 2017.

[3] M. Miraz, M. Ali, P. Excell, and R. Picking, “Internet of Nano-Things, Things and Everything: Future Growth Trends”, Future Internet, vol. 10, no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.

[4] E. Borgia, D. G. Gomes, B. Lagesse, R. Lea, and D. Puccinelli, “Special issue on" Internet of Things: Research challenges and Solutions".,” Computer Communications, vol. 89, no. 90, pp. 1–4, 2016.

[5] K. K. Patel, S. M. Patel, et al., “Internet of things IOT: definition, characteristics, architecture, enabling technologies, application future challenges,” International journal of engineering science and computing, vol. 6, no. 5, pp. 6122–6131, 2016.

[6] S. V. Zanjal and G. R. Talmale, “Medicine reminder and monitoring system for secure health using IOT,” Procedia Computer Science, vol. 78, pp. 471–476, 2016.

[7] R. Jain, “A Congestion Control System Based on VANET for Small Length Roads”, Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 1, pp. 17–21, 2018, DOI: 10.33166/AETiC.2018.01.003.

[8] S. Soomro, M. H. Miraz, A. Prasanth, M. Abdullah, “Artificial Intelligence Enabled IoT: Traffic Congestion Reduction in Smart Cities,” IET 2018 Smart Cities Symposium, pp. 81–86, 2018, DOI: 10.1049/cp.2018.1381.

[9] Mahmud, S. H., Assan, L. and Islam, R. 2018. “Potentials of Internet of Things (IoT) in Malaysian Construction Industry”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 44-52, Vol. 2, No. 1, International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.04.004.

[10] Mano, Y., Faical B. S., Nakamura L., Gomes, P. G. Libralon, R. Meneguete, G. Filho, G. Giancristofaro, G. Pessin, B. Krishnamachari, and Jo Ueyama. 2015. Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. Computer Communications, 89.90, (178-190). DOI: 10.1016/j.comcom.2016.03.010.

