Article

Not peer-reviewed version

Securing the Internet of Things: Strategies for a Resilient Cyber-Physical Ecosystem

Jared Tham Hor Win , Lim Ding Cong , Thtat Minn H Tut , Dylan Chan Kit Lun , Lee Tong Hua , Lim Hua Cong , Averil Lim Ka Wai , Chin Yi Wern , Woon Jia Min , Ali Danial Shahzad , Siva Raja Sindiramutty *

Posted Date: 8 January 2025

doi: 10.20944/preprints202501.0610.v1

Keywords: internet of things security; multi-factor authentication; edge computing; ai-driven threat detection; blockchain technology

Article

Securing the Internet of Things: Strategies for a Resilient Cyber-Physical Ecosystem

Jared Tham Hor Win, Lim Ding Cong, Thtat Minn H Tut, Dylan Chan Kit Lun, Lee Tong Hua, Lim Hua Cong, Averil Lim Ka Wai, Chin Yi Wern, Woon Jia Min, Ali Danial Shahzad and Siva Raja Sindiramutty *

Taylor's University

* Correspondence: magan.shiva91@gmail.com

Abstract: The Internet of Things (IoT) has created a cyber-physical ecosystem that has changed humans' lives and working manner. IoT connects everyday objects to other systems and devices through the Internet. Nonetheless, due to the rapid growth of IoT devices and their complex architecture, several key security challenges present themselves. That includes weak authentication, lack of firmware updates, as well as poor privacy. This paper highlights the importance of IoT security, its benefits, limitations, and future potential solutions. There are countermeasures to address these issues as well, including the use of strong passwords, device-based identity verification, multi-factor authentication, and encryption techniques. Aside from that, integrating edge computing, artificial intelligence, and machine learning into IoT brings a lot of benefits such as firmware update enhancement, intrusion detection, and user consent management. The proposed solutions aim to create a more robust and secure IoT ecosystem. They ensure the reliability and integrity of connected devices too. If these measures are adopted, sensitive data can be protected, cyber threats will be prevented, and user trust in IoT technologies can be maintained.

Keywords: internet of things security; multi-factor authentication; edge computing; ai-driven threat detection; blockchain technology

1. Background

1.1. The Internet of Things (IoT)

IoT is taking the world by storm, connecting everyday objects to the Internet and by extension, to each other. These physical objects are often embedded with sensors, software, and data processing technologies, ultimately allowing them to exchange data with other devices and systems across the web. (Fei, et al., 2023). Meanwhile, the Cloud-to-Thing Continuum describes IoT as "a global network and service infrastructure of variable density and connectivity" (Ananna et al., 2023). This network seamlessly integrates and establishes connections between heterogeneous devices that possess identities as well as physical and virtual attributes. (Lynn, et al., 2020). The main idea is to utilise this network of connected components to locate, transmit, and analyse data in all application sectors. (Mazhar, et al., 2023). Overall, the innovation that is IoT is the result of putting together an extensive variety of smart systems, frameworks, and intelligent devices and sensors. (Kumar, et al., 2019).

The application of IoT is boundless and is known for its potential to improve the quality of life in various contexts, from classrooms to smart cities. The recent rapid development of IoT has huge implications for areas like work, healthcare, and the economy. According to (Mazhar, et al., 2023), current IoT technology has enabled smart meters, remote monitoring, process automation (Javed et al., 2023), smart homes, and smart businesses (Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023). Recent research also estimates that, in the future (Gaur et al., 2022), IoT will make significant contributions to achieving public-sector goals such as remote healthcare and better green resource

 doi:10.20944/preprints202501.0610.v1

management in power grids. (Rana & Patil, 2023). To have such a large impact, IoT devices are incorporated into a myriad of products, ranging from ordinary household items to complex industrial appliances. (Fei, et al., 2023). For example, there are consumer devices such as mobile phones and wearables, or industrial sensors and actuators. (Lynn, et al., 2020).

With the number of smart systems, sensors, and intelligent devices burgeoning, the Internet of Things (IoT) can be sensed all around us. The International Data Corporation (IDC) projects that there will be 41.6 billion IoT devices in use by 2025 (Rajmohan, et al., 2022). Hence, the cyber and physical worlds (Sama et al.,2022) will continuously intertwine themselves. As the fastest-growing technology, IoT could radically alter our relationship with technology forever. (Saini & Saini, 2019). However, the rise in the number of intelligent devices has caused an explosion of new security threats and attacks specifically targeting IoT devices (Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023). As the complexity and size of IoT expand, so does the challenge of guaranteeing its security (Konatham et al, 2024).

1.2. An Overview of IoT Security and Existing Literature

Security management takes a backseat in IoT due to cost, size, and power. Due to these constraints, existing security solutions are rarely compatible with IoT devices (Williams, et al., 2022). Additionally, most manufacturers do not provide users with patches and updates after the products are released (Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023). They believe adding additional security measures would only increase production costs without increasing market value (Alex et al., 2022). Therefore, for a long time, there have been many easy-to-use, high-risk vulnerabilities in existing IoT devices, such as default passwords and plaintext transmission of keys. (Fei, et al., 2023). This is substantiated by the HP company reports that revealed nearly 70% of IoT devices are exposed to attacks and security violations (Ahmid & Kazar, 2021).

IoT security is also challenging due to the complexity of its layers. IoT devices tend to follow a four-layer model made up of the perception, network, support, and application layer. A decade of research on IoT architecture found that each layer faces its own set of security threats and creates vulnerabilities in smart systems. (Rajmohan, et al., 2022). Figure 1 illustrates how ubiquitous threats are in each layer of IoT devices, compromising the security of IoT and inducing a need for an all-encompassing security solution.

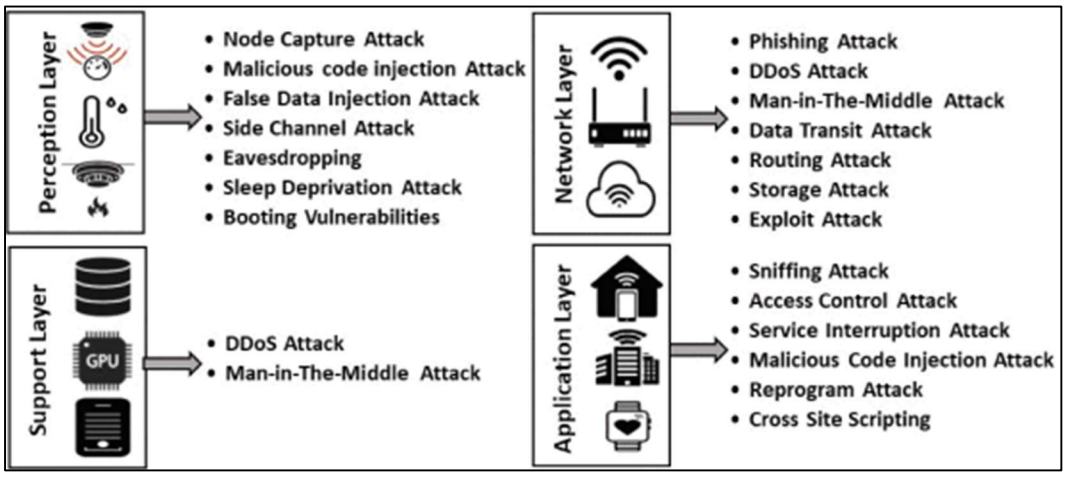

Figure 1. Security attacks in different IoT layers (Mishra & Pandya, 2021).

1.3. The Significance of IoT Security

The security of IoT plays a centric role with no margin for error. Since it is becoming such a staple in everyday life, the data collected by IoT devices is not just superficial. Smart Home setups and fitness bands track incredibly personal information such as daily and weekly routines and current location. The Computers & Security journal details incidents of many computers, smart TVs,

 doi:10.20944/preprints202501.0610.v1

phones, and cash machines connected to the IoTs being hacked. (Omolara, et al., 2022). This emphasizes the importance of prioritizing IoT security as their cyberattacks could even reach the comfort of consumers' homes (Shah et al., 2024).

Moreover, heart-rate monitors, telemedicine, and intelligent hospital systems monitor and transmit confidential patient data in real-time. If these IoT devices in hospitals were to suffer a breach, private medical records could be accessed by hackers, along with sensitive information about vital signs, sleep patterns, location of medical equipment, and medication adherence (Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023). Compromising or altering data in the Healthcare Internet of Things (H-IoT) could have bigger consequences than financial loss as it puts human lives at stake (Alferidah & Jhanjhi, 2020). Furthermore, organisations that utilise IoT devices are at risk as well. Any IoT-related vulnerability exploited in an organisation could lead to a system failure or cyberattack, leading to a large-scale impact. (Taherdoost, 2023).

All in all, IoT can authorise devices and sensors to be remotely detected, connected, and controlled anywhere over the Internet. (Rahmani, et al., 2021). The IoT will thus play a key role in the digitalisation of society and IoT security issues will "affect not only bits and bytes", but also "flesh and blood". Without solid security, intrusion detection, and prevention in place, attacks and malfunctions in IoT-based infrastructures may outweigh any of its benefits. (Rajmohan, et al., 2022). As a result, IoT security is and will continue to be one of the most crucial security-related technologies.

2.. How Iot-Related Security Technology Works

2.1. Components, Technologies, and Processes Involved

As previously mentioned, an IoT system's architecture is divided into four layers. The first layer, known as the sensing, physical, or perception layer, consists of sensors and actuators that collect data from the environment and perform tasks based on the input. The second layer, referred to as the network or transport layer, transmits the collected data through communication networks to the third layer, the middleware layer, where the data is managed and processed (Hussain et al., 2024). Finally, the fourth layer called the application layer, is where various end-to-end IoT applications and services reside, enabling interaction with users and other IoT-based systems. (Hassija, et al., 2019).

Each of these layers is important in ensuring the overall functionality and security of IoT systems. However, the interconnected nature of IoT devices and networks creates many vulnerabilities at every level (Hussain et al., 2024). Malicious actors are constantly looking for opportunities to infiltrate and exploit systems that are left unprepared or unprotected. But before addressing these challenges, it is essential to examine the components, technologies, and processes within each layer, starting with the perception layer.

2.1.1. Perception Layer

As the foundational layer, the perception layer enables IoT systems to sense and interact with their environment. A key technology in this layer is Radio Frequency Identification (RFID), which allows for the unique identification and tracking of objects using radio waves. An RFID system consists of three main components: a tag, a reader, and an application system. The tag (transmitter) with a microchip and antenna is attached to an object, and the reader (receiver) sends radio waves to activate the tag and collect data from it. This data is then sent to a controller for storage or use, such as tracking inventory.

RFID tags can be categorised into three types based on their power source: active, passive, and semi-passive. Active tags have a battery, enabling long-range communication and larger memory, making them ideal for high-value applications, though they are expensive (Jun et al., 2024). Passive tags on the other hand rely on energy from the reader's signal, having a shorter range but being cost-effective and widely used in mass applications like smart cards. Semi-passive tags combine features of both, using a small battery to improve performance while remaining compact and affordable,

 doi:10.20944/preprints202501.0610.v1

making them suitable for scenarios requiring better range without the high cost of active tags. (Gavoni, 2021). Meanwhile, the RFID reader transmits signals through its antenna to activate tags, transfer data, and communicate with application software.

Besides that, another key technology in the perception layer is wireless sensor networks (WSNs). They are comprised of many small sensing self-powered nodes which gather information or detect events (Alkinani et al., 2021). These nodes communicate with a base station (sink node), where data is aggregated, processed, and forwarded to the next layer. (Ali Khattak, et al., 2019). WSNs with their low energy consumption and low cost make them ideal for large-scale deployment in applications such as smart homes, transportation systems, and environmental monitoring, including air and water quality tracking and natural disaster detection. (Kandris, et al., 2020).

2.1.2. Network Layer

In the network layer, there exist specialised communication protocols that account for the unique characteristics of low-power and lossy links in IoT networks such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) and Routing Protocol for Low-Power and Lossy Networks (RPL), both optimised for reliable communication in resource-constrained environments (Manchuri et al., 2024; Nayyar et al., 2021). The network layer also integrates various network interfaces, supporting communication technologies like Wi-Fi, Bluetooth, and cellular networks, ensuring seamless connectivity and efficient data exchange across IoT devices. (Kim, 2024).

Not only that, but the network layer must also handle data transmission and routing efficiently, securely, and correctly. For example, in cars, the Internet of Vehicles (IoV) manages data transmission through distributed nodes like vehicles, roadside units, and sensors to optimise routes by considering factors such as speed, destination, and delay, ultimately enhancing traffic efficiency and safety. (Xu, 2023).

2.1.3. Middleware Layer

There are many approaches towards IoT middleware, differentiated by architecture type, deployment model, data handling capabilities, and many other factors. For example, in service-based middleware, there are two primary types: cloud-based middleware and edge-based middleware, with the former being the more widely adopted. Cloud-based middleware typically operates as a Platform as a Service (PaaS) or a Software as a Service (SaaS) (Medeiros, et al., 2022). These models provide services on-demand and are financed through a pay-as-you-go pricing structure. This approach allows service providers to deliver IT resources dynamically, scaling as large or as small to meet varying demands. (Hashemi-Pour, et al., 2024). Due to the restricted nature of resources in many IoT devices, the middleware helps address these limitations by providing services like unlimited storage capacity, remote resource management, service discovery, and data processing and visualisation.

Edge-based middleware, on the other hand, focuses more on the interoperability between IoT devices, with the minimum requirement of offering management and communication solutions between them. This can be achieved by translating between devices' communication protocols. (Medeiros, et al., 2022). Edge computing enabled data processing and analysis at or near the periphery of the network, as close to the originating source as possible, rather than relying solely on centralised cloud servers (Ravichandran et al., 2024 ; Shah et al., 2022). This localised approach minimises latency, reduces bandwidth usage, and avoids network disruptions. (Bigelow, 2021).

Some lesser-known enabling technologies include context-aware computing which enables systems to make intelligent decisions based on environmental data and dynamic conditions. It collects and processes raw data from sensors and transforms it into useful context, such as location or time which helps systems adapt to changes in real-time. (Zhang, et al., 2021).

2.1.4. Application Layer

 doi:10.20944/preprints202501.0610.v1

The application layer stands above the rest as the primary interface between the user and the system, often through applications, dashboards, or APIs. Within these interfaces, there are many measures that we can take to enhance security. One of the most standard forms of security that you will see almost everywhere is the user ID and password authentication pair. (IBM, 2024), where the password serves to authenticate the ID of the individual accessing the system. (insert something about encryption and salts)

Speaking of APIs, they also must be properly secured. An API or application programming interface is a set of rules and protocols that allows one piece of software to interact with one another (Seng et al., 2024; Sharma et al., 2021). If a program or application provides an API, external clients can use it to request services or access specific functionalities. (Cloudflare, 2024). Typically, one of the two most important ways developers prevent vulnerabilities is to perform schema validation, where an API's schema describes the expected behaviour of that API. It validates whether the requests it receives and responses it provides conform to this schema. Besides that, developers also set up web application firewall (WAF) rules. As its name suggests, it acts similar to a traditional firewall, monitoring traffic in and out of the system, and blocking requests and responses that could be potential threats.

2.2. Threats and Vulnerabilities of IoT Security-Related Technology

IoT devices often lack robust security measures, which makes them vulnerable to cyberattacks, data breaches, and exploitation by malicious actors. Understanding these threats and vulnerabilities is essential to develop stronger safeguards for IoT technology.

IoT security-related devices are increasingly faced with malware and botnets, most known as the infamous distributed denial-of-service (DDoS) attacks. (Fortinet, 2023). DDoS attacks involve flooding a server or website with multiple requests, usually in the hundreds of millions or even more (Babbar et al., 2021). This causes the server or website to be attacked to be unusable by legitimate users. Recently, as of 2023, Google Cloud claimed to have stopped a DDoS attack which peaked at 398 million requests per second. Google's DDoS response team also predicts that there will be an increase in DDoS attacks. (April & Kiner, 2023).

A common vulnerability would be the device's weak authentication. Weak, default passwords or passwords that are not changed often are subject to "brute-force" attacks by attackers, where the attackers use every possible combination of characters and numbers to gain unauthorised access to a system. These brute-force attacks are effective against weak unprotected passwords. (Yasar, et al., 2023).

Another common vulnerability would be the lack of updated firmware and software. (Fortinet, 2022). Insecure update mechanisms give the attackers the chance to hijack the systems and install malicious malware that can cause data breaches and lead to ransomware cases. (Mirza, 2024). According to Fortinet, most IoT devices do not have built-in IoT security, which makes it difficult to receive periodical updates and provide firmware updates and patches, leaving the organisation responsible for protecting its IoT devices and network environments from cybersecurity attacks. (Fortinet, 2022).

Insecure networks are susceptible to man-in-the-middle attacks, where the attacker can modify update packets and obtain credentials. (Fortinet, 2023). Privacy and data encryption is considered a vulnerability to IoT security-related technology. (Oliynyk, 2024). Most data transmitted across IoT devices are not encrypted which makes confidential and private information, such as medical imaging and security cameras, open to attackers. (Fortinet, 2022).

2.3. Examples of Security-Related Technology Usage

From individual devices to large-scale industries, IoT applications have brought convenience to every aspect of our daily lives. Most IoT applications rely on cloud-based infrastructure, allowing them to operate effectively and be deployed throughout the globe. Some notable IoT applications we encounter in our daily lives are household appliances embedded with smart systems such as security

 doi:10.20944/preprints202501.0610.v1

systems, water heaters, kitchen appliances, and sensor lighting (Sindiramutty et al., 2024). By using smart system software applications, the owner can control them in various ways, such as voice commands with an AI assistant like Apple Siri or even through mobile applications. (Bevis, 2023).

Smart Home Security

A common IoT system that is used to secure households. Security sensor devices such as windows and door sensors, and motion detectors are specifically designed to detect any suspicious activities such as attempted break-ins and help keep the home safe. These sensors integrate seamlessly with security systems such as alarm pads, security cameras and smart doorbells. The alarm system is designed to send immediate alerts to police, while security cameras capture crucial evidence of intruders, safeguarding everyone inside the house. In addition, environmental sensors including heat, smoke and water leak detectors are used to detect changes that indicate hazards such as fire or flood (Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024; Singhal et al., 2020). All these security features can be utilised through our mobile phones or computer apps, whether we want to arm or disarm the security system, it's just one tap away (Brohi et al., 2020). If we forget to arm the security system, geofencing reminders will always notify the users through mobile apps regardless of the distance from their homes. (Bevis, 2023)

Smart Driving

Although driverless vehicles are still at an early stage, it's only a matter of time until they become part of our daily lives. Even without driverless vehicles, IoT technology still dominates the automotive industry. Safety services provided by OnStar, a subsidiary of General Motors, designed a sensor that can be embedded into a car to detect collision or mechanical problems (Chesti et al., 2020). The data will be transmitted to a cloud-based service and sent to automotive service advisors or emergency services, sometimes without human intervention. If the emergency is severe, the advisor will contact the driver to take appropriate action to prevent further injury. If the problem is mechanical, the advisor will run a diagnostic on the car, so that the technical team is prepared when they arrive (Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024). Navigation apps like Google Maps, Apple Maps, and Waze are great examples of IoT applications. They gather all the information regarding the position of the vehicle and send it to the cloud. Moreover, the software can compute the relative movement of each vehicle and determine its speed and traffic slowdowns. Whenever there is traffic congestion, the app will reroute to avoid heavy traffic and recompute the driver's estimated arrival time. (Bevis, 2023)

Smart Toll Collection

The anticipated toll charges for each country vary; some use cameras to identify vehicle classifications, while others rely on axle-based tolling systems to determine toll fees. Electronic Toll Collection (ETC) is another example of IoT applications commonly found in urban areas with toll roads, bridges and tunnels (Dogra et al., 2021). This system is equipped with a sensor that scans the transponder tags on a vehicle windshield to determine which vehicle classification the driver had registered and assigns a toll fee to each driver (Sindiramutty et al., 2024). Even when the vehicle is moving at 50 miles per hour on the express lane, the toll booth can still read the transponder ID and transmit the data to the cloud for validation. (Bevis, 2023). Each toll booth is equipped with a camera to photograph the license plate for real-time checking whether the driver has registered with the system. Hence, people who didn't register on the system will also be assigned a toll bill. Transponders are only designed for vehicle classification; therefore, the toll booths are equipped with a sensor that counts the number of axles on a car and establishes an appropriate toll fee.

Smart Wearables

 doi:10.20944/preprints202501.0610.v1

Wearable devices like smartwatches and wristbands also dominate in various applications, such as personal fitness, leisure, healthcare, and wellness. These devices are equipped with biometric sensors to detect heart rates, temperature, blood glucose levels and respiration rates (Sindiramutty, Tan, Shah, et al., 2024). This feature will help the device collect and store data to upload into cloud infrastructure via an internet link, making it easier to monitor progress over time (Fatima-Tuz-Zahra et al., 2020). Most wearable devices are embedded with accelerometers that measure steps taken and the distance of golf shots. The device can link to global positioning satellites (GPS) to compute the distance travelled. The same concept is applied to golf courses, where it can display the position of each hole and the player's shot distance. (Bevis, 2023).

Healthcare

Wearable devices are typically equipped with wellness applications pre-installed, but there are a significant number of devices that have direct healthcare applications of IoT technology. Based on a report, shows that smartwatches can detect early signs of COVID-19 symptoms, up to a week before nasal swab tests. Nowadays, IoT has been integrated to form the Internet of Medical Things (IoMT), for example, a healthcare application including motion and trackers that runs diagnostics on patients to measure health indicators such as heart rate, blood pressure, and glucose level (Sindiramutty, Tan, & Wei, 2024). Smart Pillbox is an example of an IoMT application. Whenever a patient takes a medicine, the pillbox will transmit the data including dosage time, daily pill intake and other information to the cloud server, and store it as a patient's record. If the patient forgets to take a dosage, the server will notify the patient via SMS message. An internet-enabled pacemaker is another IoMT application, that is surgically implanted inside a patient's heart who has slow or irregular heartbeats; hence, the patient can monitor their heart condition via smartphones. (Bevis, 2023).

3. Impacts of IoT Security

3.1. Benefits

The rapid growth of IoT devices across industries has brought convenience and innovation but also significant security challenges. As of 2024, there are 18.8 billion connected IoT devices globally. (Sinha, 2024). IoT devices come with default passwords that users forget to change making devices very vulnerable. (Balbix, 2024). Thus, to prevent any threats or risks that could compromise data or device functionality, implementing security measures is very important. These security measures can provide benefits to users of these devices making it a critical component of sustainable IoT adoption.

3.1.1. Building Customer Trust

IoT devices are very vulnerable to malware and other malicious attacks, thus security measures are implemented to ensure that these issues don't arise. One of the benefits of implementing IoT security is to help build customer trust. Research carried out by the Pew Research Center stressed that 81% of Americans are concerned about companies collecting their data. (Ganji, 2023). Organisations can ensure that customers trust and remain loyal to their brand by implementing this security which will absolve any concerns they may have about private information leakage.

3.1.2. Prevention of Threats Against Smart Devices

IoT can be implemented in smart devices that people may use every day such as your fridge, coffee machine, heating system, and your car. (Kaspersky, 2020). These devices all can store your personal data and must ensure that there is no weak link for hackers to take hold of. Thus, ensuring that these devices are secure by implementing security features that IoT can offer will prevent any threat from these hackers making security very important.

3.1.3. Enhanced Business Security

 doi:10.20944/preprints202501.0610.v1

Corporations and enterprises use IoT devices in their businesses which may contain corporate secrets that they may not want rival companies to find out about. In 2021, 29% of enterprises in the European Union used IoT devices. (The European Commission, 2022). This shows that businesses will want to keep their data secure. Strong authentication and encryption that the security brings will maintain the privacy and prevent any attacks from hackers. Businesses can also avoid any major financial losses, including recovery costs, legal bills, and lost revenue, by preventing cyberattacks and data breaches.

3.2. Limitations of IoT Security

Although IoT devices offer numerous benefits to organisations, there still exist limitations to their security which will bring risks to them. These devices were built without security in mind hence, the chances of organisations being exposed to cyber threats are highly increased. (Fortinet, 2022). Below are a few limitations of IoT security:

3.2.1. Authentication

The first major disadvantage of IoT security is its weak authentication which makes it vulnerable to threats. Authentication usually relates to passwords as they are the first line of defence against malicious hackers. (IT Pillars, 2024).

IoT devices are usually left on default or weak passwords which make them easy targets for cybercriminals. Figure 2 shows that a hacker can just guess the password with brute force or dictionary attacks since the default passwords are weak and allow them to gain control of the IoT devices.

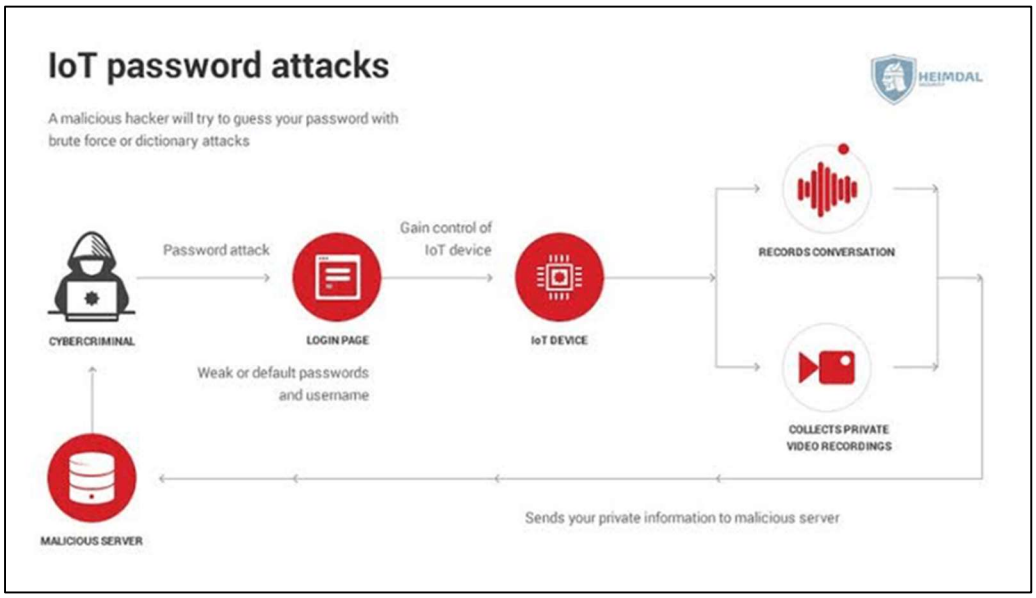

Figure 2. Security attacks in different IoT layers (AirDroid Sand Studios, 2023).

3.2.2. Firmware Updates

Another major IoT security limitation is the lack of firmware updates. IoT devices are designed with limited processing power in mind. (AirDroid Sand Studios, 2023), since they use very little data, it significantly helps in reducing costs and extending their battery life (Henke, 2023). However, this comes with a big cost which is making it difficult for IoT devices to update (Waheed et al., 2024). With limited network capabilities, some IoT devices may require physical fixes since they are not designed to receive regular security updates or patches even though remote updates are ideal. (IT Pillars, 2024)

 doi:10.20944/preprints202501.0610.v1

3.2.3. Privacy

IoT devices such as home security and wireless cameras such as CCTVs are meant to help us feel more secure. However, with IoT devices connected to the network which are also connected by different devices, it means that a breach or attack happening on the IoT devices can be spread to other devices connected to the same network due to a lack of network segmentation. (Fortinet, 2022). Not only that but private data is also sent all over the Internet through IoT devices without encryption, making us targets of hackers who can easily access any data sent by the IoT devices through the Internet. (Appsierra, 2024).

These are only a few major limitations of IoT devices out of many. Although IoT application helps us in various ways in our daily lives, they must be used wisely to prevent any backfire from happening.

3.3. Future Potential

The future of IoT security is vast and important to ensure the safe and efficient operation of interconnected devices. The vast network of interconnected devices from smart homes and cities to the healthcare, industry offers so much convenience and efficiency. But this also comes with several security challenges (Wen et al., 2023). Ensuring the protection of sensitive data, safeguarding against cyber threats, and maintaining user privacy are strong concerns (Gopi et al., 2021). The future of IoT security lies in several solutions such as advanced encryption, AI-driven threat detection, blockchain technology, and stringent regulatory measures. We will discuss a few of these here.

3.3.1. Enhanced Data Encryption

Encryption will play a pivotal role in the future of IoT data transmissions. It will prevent any tampering or eavesdropping from external users or attackers. Encryption will ensure that information transmitted between IoT devices and systems will remain confidential and secure from unauthorised access. (Sharma, 2024). Future advancements will focus on developing stronger and more advanced encryption algorithms. There will be a need for advanced encryption algorithms and robust authentication to safeguard sensitive data from the ever-evolving tactics of cyber criminals. One such encryption algorithm is quantum encryption which provides near unbreakable encryption by using the principles of quantum mechanics.

3.3.2. AI-Driven Security

With the potential advancements of Artificial Intelligence (AI) shortly it is no surprise that AI and machine learning will play a vital role in the future of IoT security. These technologies have the capability of processing large amounts of IoT data and can detect any kind of vulnerabilities or identify potential threats. (Conure, 2024).

AI-driven security systems can automatically adjust security measures based on detected threats, providing dynamic and adaptive protection. AI-powered security solutions for IoT are expected to reach a market size of $8.5 billion by 2027, according to a 2024 report by Forbes. (MAPL World, 2024).

3.3.3. Blockchain Technology

Blockchain Technology can help further improve IoT security by providing a decentralised and tamper-proof ledger for recording transactions. (MAPL World, 2024). Organisations can use blockchain technology to create unchangeable records of IoT transactions. Each transaction is encrypted and linked to each other forming a chain of records that are virtually impossible to change/alter. As the records are immutable, cybercriminals will not be able to manipulate the data or gain unauthorised access to it. (Conure, 2024).

This will allow to establish trust among stakeholders, ensure data integrity and transparency, and authenticate devices effectively. Blockchain can also be used to manage IoT devices, ensuring

 doi:10.20944/preprints202501.0610.v1

that only authenticated and authorised devices can communicate within the network. The blockchain technology market for IoT security solutions will reach $6.2 billion by 2030, according to a 2024 report by IoT Analytics. (MAPL World, 2024).

3.3.4. Stronger Authentication Methods

To ensure that only authorised users can access critical data and resources from/on networks, we need stronger authentication. Devices must be authenticated before they can access the network to access or transmit data. There are a few ways to authenticate such as Multi-Factor Authentication (MFA) (Lakhanpal, 2024). In MFA the user has to provide multiple forms of identification which include – something they know (Password or PIN), something they have (smartphone or token), and something they are (fingerprints or facial or voice recognition). These 3 combined form a strong sense of authentication.

Another way of authenticating users is using Digital Certificates. These are electronic documents that use cryptographic techniques to authenticate users. These are usually issued by trusted authorities and provide a way of verifying the user's identity. (Grayscale, 2023). It contains the user's information, public key, and a digital signature created by an encryption technique using the CA's (Certification Authority) private key.

4. Security Countermeasures

Weak authentication, lack of firmware updates, and poor privacy are some of the major issues currently in IoT devices as highlighted previously. To reduce these vulnerabilities, security countermeasures must be put in place. Security countermeasures are very important for protecting both devices and the sensitive data they manage from any potential attack as IoT systems are interconnected to one another.

4.1. Prior Discussion

4.1.1. Weak Authentication

Starting off to counter the issues of weak authentication, the most common way is to use passwords that are strong and unique for every IoT device. They usually consist of a combination of capital and lowercase letters, numbers and special characters. Besides that, techniques like multi-factor authentication (MFA) can be integrated to improve security by prohibiting unauthorised access across multiple IoT layers. To simply put it in words, MFA combines two or more authentication factors such as password, mobile device and biometric verification like fingerprints or facial recognition. MFA significantly minimises the risk of an attacker getting access even if one element from the authentication is compromised (Cvetković, et al., 2021). Moreover, a mutual authentication approach that uses hashing where passwords are transformed into a fixed-length cryptographic output and feature extraction that complements hashing by unique representations from raw input data are particularly critical for IoT devices that have limitations on their storage and power capacity. (Ma, et al., 2023). Together, it reduces repeatability of hashes therefore strengthening the authentication system's integrity.

4.1.2. Lack of Firmware Updates

Moving on to address the issue of the lack of firmware updates, a simple countermeasure would be implementing a system that would track when the next firmware update. Additionally, existing IoT devices should be redesigned to make it so that it's possible to update the devices over the air (OTA) without requiring human assistance. (Sandoval, 2020) This removes the need for physical updates, which are inefficient and time-consuming for IoT devices placed in "hard-to-reach" places. Updates can be distributed across several devices at once with wireless updates, which offer a more scalable and smoother option (Gouda et al., 2022). In the case where the limited network capabilities

 doi:10.20944/preprints202501.0610.v1

are the one that delays the firmware updates, small fixes that use little network resources can be made to address only the most critical vulnerabilities first. If the issue of firmware updates is not resolved, IoT devices will become open to exploitation. Attackers may target outdated devices which could result in compromised system operation, illegal access, and data breaches.

4.1.3. Lack of Privacy and Security

Finally, data encryption is essential for both in transit and at rest to address the problem of inadequate privacy. By encoding sensitive data in a way that only authorised users can decrypt, encryption techniques shield it from unauthorised access. The RSA algorithm is an example that is frequently used due to its high security and cryptographic hashes that are employed to maintain data integrity between devices (Humayun et al., 2022). For additional computationally complex applications, homomorphic encryption can securely handle data without revealing it, but it requires a large amount of computer power. (Obaidat, et al., 2020). Other than that, unauthorised data access can also be avoided by implementing robust access controls and user authentication for device interfaces. Users must also have control over their data, including the ability to opt out of data sharing when feasible and be informed about the data being gathered and how it is used.

4.2. Proposed Countermeasures

Although the countermeasures mentioned earlier to address the issues are already effective, there are other ways to enhance their efficiency to the fullest and other ways to tackle the issues. Below are proposed countermeasures and ideas to address the major issues in IoT.

Firstly, with the rise of the internet and AI, the threat of malware has also increased, and the systems nowadays are more vulnerable to phishing, credential stuffing, and brute force attacks than ever. Therefore, we overcome this issue by utilising the existence of AI specifically leveraging machine learning models to analyse real-time data to further enhance the authentication of a user where the model can adapt to the changes in the user behaviour's pattern. The machine learning model would also collect data about the user's behaviour which include the locations from which they access the system, typical usage times, and other relevant patterns for anomaly detection. The model is then trained to be able to spot unusual changes and react to them appropriately by flagging them as a potential anomaly. When an anomaly incident occurs, instead of forcing the user out of the system, a one-time password and a biometric scan such as the legitimate user's fingerprint would appear and is required for the user to verify themselves (Jhanjhi et al., 2021). If the verification fails, an alert will be sent to the legitimate user saying that someone is trying to access their system. This would protect the system from common attacks such as phishing, credential stuffing, and brute-force attempts. By relying on real-time behaviour rather than static passwords or credentials, these authentication measures render phishing attempts ineffective. Additionally, in credential stuffing attacks, unauthorised access is unlikely without matching the distinct behavioural fingerprint, even if login credentials are compromised. Unlike conventional passwords, behavioural biometrics cannot be deduced or brute-forced.

Furthermore, another proposed countermeasure to address the issue of the lack of firmware updates is to integrate edge computing into existing IoT devices. By adding more edge nodes nearer to an IoT device, it can act as a bridge between the cloud and the devices. IoT devices get updates through these local nodes rather than directly from the cloud, which lowers latency and eliminates the need for heavy reliance on stable and high-speed internet connections for firmware updates. (Iordache, 2024). The process works by compressing updated data and splitting it into smaller chunks within the edge nodes before incrementally sending it out for the IoT device. With that, the updates by edge nodes would generally reduce latency and are usually faster as data packets arrive at the destination faster when being compared against traditional cloud server's updates.

Finally, the proposed countermeasure to address the issue of the lack of privacy and security would be using AI which is going to be implemented with an Intrusion Detection System (IDS) in the IoT devices. By doing so, the IDS would have more potential to be able to adapt and identify complex

 doi:10.20944/preprints202501.0610.v1

threats that a traditional IDS could overlook. Machine learning algorithms can analyse and evaluate network data and device behaviours in real-time, identifying odd patterns that may lead to a privacy or security breach (Kumar et al., 2021). A real-time monitoring system can be implemented to monitor illegal access to private user information. In addition to that, machine learning models can be trained to analyse and understand the different types of IoT devices that collect different kinds of user information and data. For example, a fitness tracker that collects the health information of a user or a weather sensor that collects information from a temperature sensor, wind speed sensor and more (Lim et al., 2019). By leveraging AI, it helps ensure that any non-compliant activity such as unapproved sharing of data to third parties will be stopped right away. Additionally, AI can monitor and control user consent preferences across different IoT devices and platforms. Moreover, it also can instantly change the device's settings and make sure no further data is sent against the user's wishes if they withdraw their consent for data sharing for example, by choosing not to have their position tracked.

The combination of edge computing, machine learning, and artificial intelligence provides a strong and flexible way to handle the main security issues that IoT devices face. These countermeasures not only lessen current vulnerabilities but also build a more robust IoT ecosystem by strengthening user authentication through behavioural biometrics, enhancing firmware update mechanisms with localised edge computing, and protecting privacy with AI-powered intrusion detection systems by guaranteeing that IoT devices stay safe, effective, and in line with user privacy wishes, these creative solutions create a more secure environment for consumers as well as the larger network. In doing so, these cutting-edge technologies will be essential to protecting the dependability and integrity of linked devices as the IoT industry develops further.

5. Conclusion

IoT has changed everyone's life and the way they interact with devices. However, convenience brings security implications. With the growing number of these connected devices, their attack surface has expanded which makes it extremely difficult to secure IoT systems. This paper discussed the importance of IoT security, its benefits, limitations, as well as future potential. The main security challenges such as weak authentication, lack of firmware updates, and poor privacy have also been identified.

Some countermeasures have been suggested to overcome the challenges stated above which include the implementation of robust authentication methods like multi-factor authentication and digital certificates to avoid access to IoT devices by unauthorised users. There is another method, which is to implement a system to monitor firmware upgrades and provide over-the-air updates so that the IoT devices can be free from vulnerabilities and required updates. Apart from that, the role of edge computing to lower the latency and have faster firmware updates with the integration of AI and machine learning has been suggested for further strengthening IoT security. AI-based IDSs can analyse network traffic and device patterns in real-time. If it is implemented, complex attacks that would have been missed by conventional systems can be detected. It is also possible to use machine learning algorithms for the analysis and understanding of the various types of IoT devices as well as the data they produce thus being able to respect and protect user consent preference choices.

In summary, the security of IoT devices is vital to the security of connected systems, whether it is the integrity or reliability of the system. If robust security is implemented, the threats posed towards IoT devices can be reduced, and thus there will be a safer, more secure connected environment.

Reference

1. Ahmid, M. & Kazar, O., 2021. A Comprehensive Review of the Internet of Things Security. Journal of Applied Security Research.

 doi:10.20944/preprints202501.0610.v1

2. AirDroid Sand Studios, 2023. 5 Common IoT Security Challenges to Be Aware Of. [Online] Available at: https://blog.airdroid.com/post/5-common-iot-security-challenges/
3. Alex, S. A., Jhanjhi, N., Humayun, M., Ibrahim, A. O., & Abulfaraj, A. W. (2022). Deep LSTM Model for Diabetes Prediction with Class Balancing by SMOTE. *Electronics*, *11*(17), 2737. https://doi.org/10.3390/electronics11172737
4. Alferidah, D. K., & Jhanjhi, N. (2020). Cybersecurity Impact over Bigdata and IoT Growth. *2020 International Conference on Computational Intelligence (ICCI)*. https://doi.org/10.1109/icci51257.2020.9247722
5. Ali Khattak, H. et al., 2019. Perception security in the Internet of Things. Future Generation Computer Systems, Volume 100, pp. 144-164.
6. Alkinani, M. H., Almazroi, A. A., Jhanjhi, N., & Khan, N. A. (2021). 5G and IoT Based Reporting and Accident Detection (RAD) System to Deliver First Aid Box Using Unmanned Aerial Vehicle. *Sensors*, *21*(20), 6905. https://doi.org/10.3390/s21206905
7. Ananna, F. F., Nowreen, R., Jahwari, S. S. R. A., Costa, E. A., Angeline, L., & Sindiramutty, S. R. (2023). Analysing Influential factors in student academic achievement: Prediction modelling and insight. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.254
8. Appsierra, 2024. Disadvantages of the Internet of Things: Learn Major Threats. [Online] Available at: https://www.appsierra.com/blog/disadvantages-of-the-internet-of-things
9. April, T. & Kiner, E., 2023. Google mitigated the largest DDoS attack to date, peaking above 398 million reps. [Online] Available at: https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps
10. Available at: https://www.knowledgehut.com/blog/security/Iot-cyber-security
11. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.255
12. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., Tajwar, M. A., & Sindiramutty, S. R. (2023). Defending the digital Frontier: IDPS and the battle against Cyber threat. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.253
13. Azam, H., Tajwar, M. A., Mayhialagan, S., Davis, A. J., Yik, C. J., Ali, D., & Sindiramutty, S. R. (2023). Innovations in Security: A study of cloud Computing and IoT. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.252
14. Azam, H., Tan, M., Pin, L. T., Syahmi, M. A., Qian, A. L. W., Jingyan, H., Uddin, M. F., & Sindiramutty, S. R. (2023). Wireless Technology Security and Privacy: A Comprehensive Study. *Preprints.org*. https://doi.org/10.20944/preprints202311.0664.v1
15. Babbar, H., Rani, S., Masud, M., Verma, S., Anand, D., & Jhanjhi, N. (2021). Load balancing algorithm for migrating switches in software-defined vehicular networks. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *67*(1), 1301–1316. https://doi.org/10.32604/cmc.2021.014627
16. Balbix, 2024. Internet of Things (IoT) Biggest Security Challenges. [Online] Available at: https://www.balbix.com/insights/addressing-iot-security-challenges/
17. Bevis, R., 2023. 7 Examples of IoT in Everyday Life. [Online] Available at: https://www.cbtnuggets.com/blog/technology/networking/seven-examples-of-iot-in-everyday-life
18. Bigelow, S. J., 2021. What is edge computing? Everything you need to know. [Online] Available at: https://www.techtarget.com/searchdatacenter/definition/edge-computing
19. Brohi, S. N., Jhanjhi, N., Brohi, N. N., & Brohi, M. N. (2020). Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19.pdf. *TECHRxiv*. https://doi.org/10.36227/techrxiv.12115596.v1
20. Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. (2020). Evolution, Mitigation, and Prevention of Ransomware. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis49240.2020.9257708

 doi:10.20944/preprints202501.0610.v1

21. Cloudflare, 2024. What is API security? [Online] Available at: https://www.cloudflare.com/learning/security/api/what-is-api-security/
22. Conure, 2024. The Future of IoT Security: Trends and Predictions. [Online] Available at: https://www.iotforall.com/the-future-of-iot-security-trends-and-predictions?form=MG0AV3
23. Cvetković, A. S., Radojcic, V. & Adamović, S. Ž., 2021. Multi-factor Authentication for the Internet of Things. Zbornik Radova Univerziteta Sinergija, November.22(7).
24. Dogra, V., Singh, A., Verma, S., Kavita, N., Jhanjhi, N. Z., & Talib, M. N. (2021). Analyzing DistilBERT for Sentiment Classification of Banking Financial News. In *Lecture notes in networks and systems* (pp. 501–510). https://doi.org/10.1007/978-981-16-3153-5_53
25. Fatima-Tuz-Zahra, N., Jhanjhi, N., Brohi, S. N., Malik, N. A., & Humayun, M. (2020). Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis49240.2020.9257607
26. Fei, W., Ohno, H. & Sampalli, S., 2023. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. ACM Computing Surveys, 56(5), pp. 1-40.
27. Fortinet, 2022. What Is IoT Security? Challenges and Requirements. [Online] Available at: https://www.fortinet.com/resources/cyberglossary/iot-security
28. Fortinet, 2023. What Is IoT Device Vulnerability? [Online] Available at: https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities
29. Ganji, S., 2023. What Is IoT Security? Benefits, Challenges, and Solution. [Online] Available at: https://www.accelq.com/blog/iot-security/
30. Gavoni, L., 2021. RFID Exploitation and Countermeasures. p. 9.
31. Gaur, L., Arora, G. K., & Jhanjhi, N. Z. (2022). Deep learning techniques for creation of deepfakes. In *DeepFakes* (pp. 23-34). CRC Press.
32. Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N. Z., & Luhach, A. K. (2021). Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimedia Tools and Applications*, *81*(19), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6
33. Gouda, W., Almurafeh, M., Humayun, M., & Jhanjhi, N. Z. (2022). Detection of COVID-19 based on chest x-rays using deep learning. *Healthcare*, *10*(2), 343. https://doi.org/10.3390/healthcare10020343
34. Grayscale, 2023. Internet of Things (IoT) Security: A Critical Need for the Future. [Online] Available at: https://grayscale.my/internet-of-things-iot-security-a-critical-need-for-the-future/
35. Hashemi-Pour, C., Lutkevich, B. & Bigelow, S. J., 2024. XaaS (anything as a service). [Online] Available at: https://www.techtarget.com/searchcloudcomputing/definition/XaaS-anything-as-a-service
36. Hassija, V. et al., 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 20 June, Volume 7, pp. 82721-82743.
37. Henke, C., 2023. What Is IoT Security? Risks, Examples, and Solutions. [Online] Available at: https://www.emnify.com/iot-glossary/iot-security
38. Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022). A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma. *Healthcare*, *10*(6), 1058. https://doi.org/10.3390/healthcare10061058
39. Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. a. U., & Sindiramutty, S. R. (2024). Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, *2*, 1–8. https://doi.org/10.1109/khi-htc60760.2024.10482197
40. IBM, 2024. Application layer security. [Online] Available at: https://www.ibm.com/docs/en/zos-basic-skills?topic=features-application-layer-security
41. Iordache, T., 2024. How Edge Computing is Transforming the Future of Technology. [Online] Available at: https://www.thinslices.com/insights/edge-computing-transforming-the-future-of-technology
42. IT Pillars, 2024. Security Impact of IoT: Risks and Challenges. [Online] Available at: https://www.it-pillars.com/blog/security-impact-of-iot/
43. Javed, D., Jhanjhi, N. Z., & Khan, N. A. (2023, April). Football analytics for goal prediction to assess player performance. In *Innovation and Technology in Sports: Proceedings of the International Conference on Innovation and Technology in Sports,(ICITS) 2022, Malaysia* (pp. 245-257). Singapore: Springer Nature Singapore.

44. Jhanjhi, N., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. *Computer Systems Science and Engineering*, *37*(3), 361–380. https://doi.org/10.32604/csse.2021.015206
45. Jun, A. Y. M., Jinu, B. A., Seng, L. K., Maharaiq, M. H. F. B. Z., Khongsuwan, W., Junn, B. T. K., Hao, A. a. W., & Sindiramutty, S. R. (2024). Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions. *Preprints.org*. https://doi.org/10.20944/preprints202409.1325.v1
46. Kandris, D., Nakas, C., Vomvas, D. & Koulouras, G., 2020. Applications of Wireless Sensor Networks: An Up-to-Date Survey. Applied System Innovation, 25 February, 3(1), p. 14.
47. Kaspersky, 2020. Why IoT security is important for your home network. [Online] Available at: https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network
48. Kim, J.-D., 2024. A Comprehensive Analysis of Routing Vulnerabilities and Defense. October.
49. Konatham, B., Simra, T., Amsaad, F., Ibrahem, M. I., & Jhanjhi, N. Z. (2024). A Secure Hybrid Deep Learning Technique for Anomaly Detection in IIoT Edge Computing. *Authorea Preprints*.
50. Kumar, M. S., Vimal, S., Jhanjhi, N., Dhanabalan, S. S., & Alhumyani, H. A. (2021). Blockchain based peer to peer communication in autonomous drone operation. *Energy Reports*, *7*, 7925–7939. https://doi.org/10.1016/j.egyr.2021.08.073
51. Kumar, S., Tiwari, P. & Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, Volume 6.
52. Lakhanpal, M., 2024. The State of IoT Security: Challenges and Opportunities. [Online] Available at: https://the-tech-trend.com/big-data/iot-security-challenges-and-opportunities
53. Lim, M., Abdullah, A., Jhanjhi, N., Khan, M. K., & Supramaniam, M. (2019). Link Prediction in Time-Evolving Criminal Network with deep Reinforcement learning technique. *IEEE Access*, *7*, 184797–184807. https://doi.org/10.1109/access.2019.2958873
54. Lynn, T. et al., 2020. The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In: T. Lynn, J. G. Mooney, B. Lee & P. T. Endo, eds. The Cloud-to-Thing Continuum. s.l.:Palgrave Macmillan, Cham, pp. 1-22.
55. Ma, Q., Tan, H. & Zhou, T., 2023. Mutual authentication scheme for smart devices in IoT-enabled smart home systems. Computer Standard & Interfaces, Volume 86.
56. Manchuri, A., Kakera, A., Saleh, A., & Raja, S. (2024). pplication of Supervised Machine Learning Models in Biodiesel Production Research - A Short Review. *Borneo Journal of Sciences and Technology*. https://doi.org/10.35370/bjost.2024.6.1-10
57. MAPL World, 2024. The Future of IoT The Future of IoT Security: Trends and Predictions. [Online] Available at: https://www.linkedin.com/pulse/future-iot-security-trends-predictions-maplworld-8blrc/
58. Mazhar, T. et al., 2023. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sciences, 13(4), pp. 1-30.
59. Medeiros, R., Fernandes, S. & Queiroz, P. G. G., 2022. Middleware for the Internet of Things: a systematicliterature review. Journal of Universal Computer Science, 28(1), pp. 54-79.
60. Mirza, D., 2024. Top 10 IoT Device Vulnerabilities to Enhance IoT Security. [Online] Available at: https://www.hostduplex.com/blog/top-iot-device vulnerabilities/#What_are_the_Top_IoT_Vulnerabilities_that_Make_Devices_Insecure
61. Mishra, N. & Pandya, S., 2021. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. IEEE Access, Volume 9, pp. 59353-59377.
62. Nayyar, A., Gadhavi, L., & Zaman, N. (2021). Machine learning in healthcare: review, opportunities and challenges. In *Elsevier eBooks* (pp. 23–45). https://doi.org/10.1016/b978-0-12-821229-5.00011-2
63. Obaidat, M. A. et al., 2020. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers, 9(2), p. 44.
64. Oliynyk, K., 2024. IoT Security: Risks, Examples, and Solutions. [Online] Available at: https://webbylab.com/blog/iot-security-issues-and-solutions/
65. Omolara, A. E. et al., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, Volume 112.

66. Rahmani, A. M., Bayramov, S. & Kalejahi, B. K., 2021. Internet of Things Applications: Opportunities and Threats. Wireless Personal Communications, Volume 122, pp. 451-476.
67. Rajmohan, T., Nguyen, P. H. & Ferry, N., 2022. A decade of research on patterns and architectures for IoT security. Cybersecurity, 5(2).
68. Rana, P. & Patil, P. B., 2023. Cyber security threats in IoT: A review. Journal of High Speed Networks, 29(2), pp. 105-120.
69. Ravichandran, N., Tewaraja, T., Rajasegaran, V., Kumar, S. S., Gunasekar, S. K. L., & Sindiramutty, S. R. (2024). Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. *Preprints.org*. https://doi.org/10.20944/preprints202409.1369.v1
70. Sama, N. U., Zen, K., Humayun, M., Jhanjhi, N. Z., & Rahman, A. U. (2022). Security in wireless body sensor network: A multivocal literature study. *Applied System Innovation*, *5*(4), 79.
71. Saini, M. K. & Saini, R. K., 2019. Internet of Things (IoT) Applications and Security Challenges: A Review. SSRN Electronic Journal, 7 June.
72. Sandoval, N., 2020. What Is Over-the-Air? OTA Provisioning Explained. [Online] Available at: https://www.emnify.com/iot-glossary/over-the-air [Accessed 20 November 2024].
73. Seng, Y. J., Cen, T. Y., Raslan, M. a. H. B. M., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., & Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. *Preprints.org*. https://doi.org/10.20944/preprints202408.2261.v1
74. Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2022). Cybersecurity and blockchain usage in contemporary business. In *Advances in information security, privacy, and ethics book series* (pp. 49–64). https://doi.org/10.4018/978-1-6684-5284-4.ch003
75. Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Enabling Explainable AI in Cybersecurity Solutions. In *Advances in Explainable AI Applications for Smart Cities* (pp. 255-275). IGI Global.
76. Sharma, R., Singh, A., Kavita, N., Jhanjhi, N. Z., Masud, M., Jaha, E. S., & Verma, S. (2021). Plant disease diagnosis and image classification using deep learning. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *71*(2), 2125–2140. https://doi.org/10.32604/cmc.2022.020017
77. Sharma, V., 2024. IoT Cyber Security: Trends, Challenges and Solutions. [Online]
78. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., & Manchuri, A. R. (2024). Cybersecurity measures for logistics industry. In *Advances in information security, privacy, and ethics book series* (pp. 1–58). https://doi.org/10.4018/979-8-3693-3816-2.ch001
79. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., Yun, K. J., Ray, S. K., Jazri, H., & Hussain, M. (2024). Future trends and emerging threats in drone cybersecurity. In *Advances in information security, privacy, and ethics book series* (pp. 148–195). https://doi.org/10.4018/979-8-3693-0774-8.ch007
80. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Yun, K. J., Manchuri, A. R., Ashraf, H., Murugesan, R. K., Tee, W. J., & Hussain, M. (2024). Data security and privacy concerns in drone operations. In *Advances in information security, privacy, and ethics book series* (pp. 236–290). https://doi.org/10.4018/979-8-3693-0774-8.ch010
81. Sindiramutty, S. R., Jhanjhi, N., Tan, C. E., Lau, S. P., Muniandy, L., Gharib, A. H., Ashraf, H., & Murugesan, R. K. (2024). Industry 4.0. In *Advances in logistics, operations, and management science book series* (pp. 342–405). https://doi.org/10.4018/979-8-3693-1363-3.ch013
82. Sindiramutty, S. R., Tan, C. E., & Wei, G. W. (2024). Eyes in the sky. In *Advances in information security, privacy, and ethics book series* (pp. 405–451). https://doi.org/10.4018/979-8-3693-0774-8.ch017
83. Sindiramutty, S. R., Tan, C. E., Shah, B., Khan, N. A., Gharib, A. H., Manchuri, A. R., Muniandy, L., Ray, S. K., & Jazri, H. (2024). Ethical considerations in drone cybersecurity. In *Advances in information security, privacy, and ethics book series* (pp. 42–87). https://doi.org/10.4018/979-8-3693-0774-8.ch003
84. Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Kavita, N., Rodrigues, J. J. P. C., Jhanjhi, N. Z., Ghosh, U., Jo, O., & Iwendi, C. (2020). Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned railway level crossings. *IEEE Access*, *8*, 113790–113806. https://doi.org/10.1109/access.2020.3002416
85. Sinha, S., 2024. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. [Online] Available at: https://iot-analytics.com/number-connected-iot-devices/

86. Taherdoost, H., 2023. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics, 8(12).
87. The European Commission, 2022. Use of Internet of Things in enterprises. [Online] Available at: https://ec.europa.eu/eurostat/statistics explained/index.php?title=Use_of_Internet_of_Things_in_enterprises#Enterprises_using_IoT
88. Waheed, A., Seegolam, B., Jowaheer, M. F., Sze, C. L. X., Hua, E. T. F., & Sindiramutty, S. R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure. *preprints.org*. https://doi.org/10.20944/preprints202407.2338.v1
89. Wen, B. O. T., Syahriza, N., Xian, N. C. W., Wei, N. G., Shen, T. Z., Hin, Y. Z., Sindiramutty, S. R., & Nicole, T. Y. F. (2023). Detecting cyber threats with a Graph-Based NIDPS. In *Advances in logistics, operations, and management science book series* (pp. 36–74). https://doi.org/10.4018/978-1-6684-7625-3.ch002
90. Williams, P., Dutta, I. K., Daoud, H. & Bayoumi, M., 2022. A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, August.Volume 19.
91. Xu, Y., 2023. Routing Strategies and Protocols for Efficient Data Transmission in the Internet of Vehicles: A Comprehensive Review. International Journal of Advanced Computer Science and Applications, January, 14(9), pp. 955-965.
92. Yasar, K., Shea, S. & Wigmore, I., 2023. IoT security (internet of things security). [Online] Available at: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security
93. Zhang, J., Ma, M., Wang, P. & Sun, X.-d., 2021. Middleware for the Internet of Things: A survey on requirements, enabling technologies and solutions. Journals of Systems Architecture, August.Volume 117.