Categories
(1)
(7)
(4)
(3)
(2)
(3)

MAY 18, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY / UNCATEGORIZED

Internet of Things (IoT) Security: A Critical Need for the Future

The Internet of Things (IoT) has emerged as one of the most transformative technological innovations in recent years, with an estimated 31 billion connected devices being in use globally by 2022 alone and will rise to 75 billion by 2025[1]. This rapid growth presents immense opportunities for businesses and individuals alike, offering unparalleled connectivity, convenience, and efficiency.

However, with this increased connectivity comes an increased risk of cyber attacks and breaches, as IoT devices can be vulnerable to hacking and data theft. Without proper security measures in place, the potential consequences of a breach could be catastrophic.

This article will examine key challenges related to IoT security, along with emerging strategies to address these vulnerabilities and foster secure environments within which interconnected devices can operate effectively.

What is the Internet of Things (IoT)?

The Internet of Things (IoT) can be best described as a vast network of interconnected devices collecting and exchanging data to improve efficiencies and create new opportunities in various industries.

These connected devices range from everyday household appliances such as smart thermostats and lighting systems to large-scale industrial machineries like manufacturing equipment and transportation vehicles.

The Growing Prevalence Of IoT Devices

Smart Home Security

Smart home security devices, such as cameras, motion sensors, and smart locks, are becoming more advanced and affordable, making it easier for consumers to protect their homes. However, this interconnectedness also raises pressing concerns about security vulnerabilities in these systems.

They become targets of cyberattacks due to lax security measures, potentially leading to privacy breaches and unauthorised access to sensitive data. Hackers can exploit vulnerabilities in smart home devices to access sensitive information or even control the devices themselves.

Industrial IoT Security

Industrial IoT (IIoT) devices are employed in manufacturing plants, energy management systems, and logistics networks for monitoring equipment health, asset tracking, and predictive maintenance, among other applications. These, in turn, operational efficiency and facilitate real-time data collection.

However, like their residential counterparts, IIoT security remains a critical concern. Cybersecurity threats can lead to catastrophic consequences, such as disrupting essential services or even physical harm due to malfunctioning machinery. In addition, the increasing use of cloud-based services and the interconnectivity between different systems has made IIoT security even more complex.

Prominent IoT Security Breaches

Mirai Botnet Attack

The Mirai botnet attack2, which occurred in October 2016, serves as a significant example of the potential severity and widespread damage that can result from IoT security breaches.

This large-scale cyberattack involved infiltrating thousands of connected devices such as cameras and routers by exploiting their weak default passwords to create a network of infected 'bots' capable of launching devastating distributed denial-of-service (DDoS) attacks.

The most notable instance was when the Mirai botnet targeted Dyn, a major DNS provider, causing widespread internet outages across numerous popular websites like Amazon, Twitter, and Netflix.

Jeep Cherokee Hack

Moving from the realm of large-scale cyber warfare to consumer-facing IoT devices, another notable security breach occurred in 2015 with the widely publicised Jeep Cherokee attack3.

In this instance, cybersecurity researchers demonstrated their ability to remotely exploit vulnerabilities in the vehicle's onboard computer system and gain control over critical functions such as acceleration, braking, and steering – all while a journalist drove the SUV on a busy highway.

This alarming proof-of-concept exposed significant flaws in automotive IoT security measures at a time when connected vehicles were becoming increasingly prevalent on roads worldwide.

Unique Challenges Associated With Securing IoT Devices

Limited Processing Power

This challenge is particularly prevalent in smaller IoT devices, which often lack the resources necessary for robust security features. These limitations make it difficult for manufacturers to implement complex encryption algorithms or comprehensive threat detection systems on their devices.

As cybercriminals become increasingly sophisticated, this leaves countless IoT devices vulnerable to attacks that can compromise user privacy and device functionality.

Difficulty Of Updating And Patching

Legacy systems or consumer electronics often lack regular firmware updates due to manufacturers focusing on newer products or simply neglecting older models. This makes it increasingly difficult for users to keep their devices secure against emerging threats and vulnerabilities.

Additionally, many IoT devices are designed without an easy-to-use interface for applying patches or performing updates, leaving non-technical consumers at a disadvantage when attempting to maintain device security.

Privacy Protections Vulnerabilities

In addition to the challenges posed by insecure communication channels and inadequate authentication measures, insufficient privacy protections further contribute to the potential security vulnerabilities of IoT devices.

As these devices collect, store, and transmit vast amounts of sensitive data, often including personal information pertaining to users' habits and preferences, there is an urgent need for adequate safeguards that prevent unauthorised access or misuse.

This entails robust encryption techniques, adherence to best practices in data management and storage, and compliance with relevant regulations such as the Malaysian Personal Data Protection Act (PDPA) 2010.

Potential Solutions For Improving IoT Security

Device Authentication Protocols

A robust device authentication protocol means that each device connected to the IoT network must be authenticated before it can access or transmit data. This is important because it prevents unauthorised access to the network by devices that are not authorised to be there.

One example of a device authentication protocol is the use of digital certificates. Digital certificates are electronic documents that verify the identity of a device or user. They are issued by a trusted authority and contain information such as the device's public key, owner information, and expiration date. When a device tries to connect to the IoT network, it must present its digital certificate to the web for authentication.

Improve Encryption Methods

Encryption serves as a cornerstone in safeguarding sensitive data transmitted between connected devices by converting it into an unreadable format that can only be deciphered using a decryption key.

Techniques such as symmetric and asymmetric encryption algorithms, homomorphic encryption, and lightweight cryptography are instrumental in bolstering privacy and thwarting cyberattacks.

Better Privacy Regulation Enforcement

Regulatory frameworks can provide guidelines for manufacturers, service providers, and users on how IoT devices should handle personal information while ensuring that data protection remains a top priority.

Privacy regulations such as the Malaysian Personal Data Protection Act (PDPA) 20104 have to be improved in terms of enforcement to promote transparency and data security in today's interconnected environments.

Building upon the potential solutions for enhancing IoT security, it becomes evident that a comprehensive and collaborative approach is indispensable in addressing this pressing issue.

By implementing robust security frameworks, promoting transparency, embracing industry standards, and fostering an environment conducive to knowledge sharing and cooperation among various sectors, we can collectively work towards mitigating cyber threats within this domain.

If you want to learn more about the best practices for keeping your IoT data safe and enhancing your overall IoT security, contact us today by emailing us at enquiries@grayscale.my.

SEPTEMBER 29, 2022 / BUSINESS / EDUCATIONAL / MARKETING

Grayscale Hosts Cybersecurity Workshop for Government Agencies

APRIL 6, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY

IT Audit Explained

MAY 18, 2022 / EDUCATIONAL / INFORMATION TECHNOLOGY

The Rise of Ransomware: A Deep Dive into the Latest Threats

grayscale

A subsidiary under TechnoDex Group of Companies

Unit E-07-03, Menara Suezcap 2, KL Gateway, No. 2, Jalan Kerinchi, 59200 Kuala Lumpur, Federal Territory of Kuala Lumpur

T: +603 7932 0111

E: enquiries@grayscale.my