INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1469-1473

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

THE FUTURE OF CYBERSECURITY IN INDUSTRIAL IOT: OVERCOMING CHALLENGESAND SEIZING OPPORTUNITIES

Syeda Aliya Muskan[1], Meghana M A[2], Pallavi H, Nimra Taj[3]

[1,2,3,4]Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, affiliated to VTU Belagavi, Karnataka, India.

ABSTRACT

The Internet of Things (IoT) represents the integration of the physical and cyber worlds in various aspects of people's lives, offering benefits such as convenience and entertainment in smart homes, process optimization, cost savings and business opportunities in sectors such as cities, energy and healthcare. However, thesebenefits come with significant security concerns. Protecting sensitive data and critical infrastructure is essential for IoT systems. With estimates suggesting that the number of networked devices will reach 20 to 50 billion by 2020 worldwide, security risks, particularly in Industrial Internet of Things (IIoT) applications, can become costly and even dangerous for businesses, governments and individuals. As a result, strategies are being developed to combat cybercrime. The three main challenges to address security issues in IoT and IIoT are: (1) the operation of applications in highly distributed environments, (2) the use of heterogeneous smart objects, and (3) the limitations of sensors andactuators in terms of power and computing resources. Thesefactors make traditional security countermeasures ineffective in IoT systems. A major security challenge in the IoT context is the expansion of the overall attack surface, making systems more vulnerable to malicious attacks compared to isolated and disconnected systems. To address these issues, cybersecurity management must focus onraising awareness, improving skills, and exploring new technologies such as blockchain and Software DefinedNetworking (SDN). In addition, opportunities in 5G and "green" IoT are being explored, especially in relation to energy efficiency and CO2 emission reduction. This review article examines the current status, trends, and developments in the challenges and opportunities surrounding IoT cybersecurity management.

Keywords: Cybersecurity; Computer Security; IT Security; Internet of Things (IoT); Safety; Industrial Internet of Things (IIoT); Blockchain; Software- Defined Networking (SDN); 5G

1. INTRODUCTION

The Internet of Things (IoT) aims to seamlessly integrate the physical and digital worlds into a unified system, offering significant business opportunities in sectors as diverse as healthcare and energy. However, the IoT faces many security challenges that are often more complex than those in other fields due to the complex environment and the large number of devices, many of which are resource-constrained. The term "IoT" was coined by Kevin Ashton, a British technology pioneer and author, in 1999. He defined the IoT as a system in which the Internet connects to the physical world through ubiquitous sensors. The IoT can be described as a network of physical devices, vehicles, equipment and other devices (mechatronic systems), equipped with integrated electronics, software, sensors, actuators and connections, which allow them to connect, collect and exchange information. A major application of IoT is the "smart factory," which is made up of four main elements: people, processes, technology ecosystems, and smart objects. It is estimated that by 2025, IoT applications in smart factories will generate between $1.2 trillion and $3.7 trillion in economic value annually. IoT extends traditional Internet connectivity, which typically includes computers (desktops, smartphones, tablets), to a wide range of physical devices and everyday objects that are either "dumb" or not connected to the Internet, such as fire alarms, refrigerators, cars, and electricity. IoT wearables are closely related to digital manufacturing, which aims to create high-quality, low-cost, and highly personalized products by integrating the Industrial Internet of Things (IIoT), big data analytics, cloud computing, and advanced robotics into manufacturing plants. The IoT ecosystem has become ubiquitous, with specialized networks such as the Internet of Medical Things (IoMT), the Internet of Battlefield Things (IoBT), and the Internet of Vehicles (IoV), among others. Two key issues that potentially threaten IoT devices are the security and privacy of the data shared or collected, which is often deeply connected to users and their personal lives.

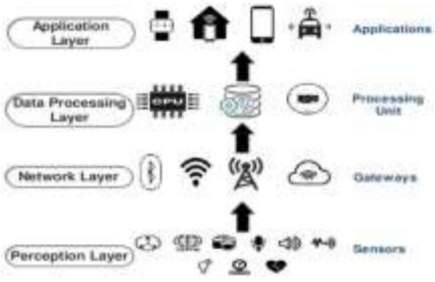

Figure 1: An Typical architecture of IoT

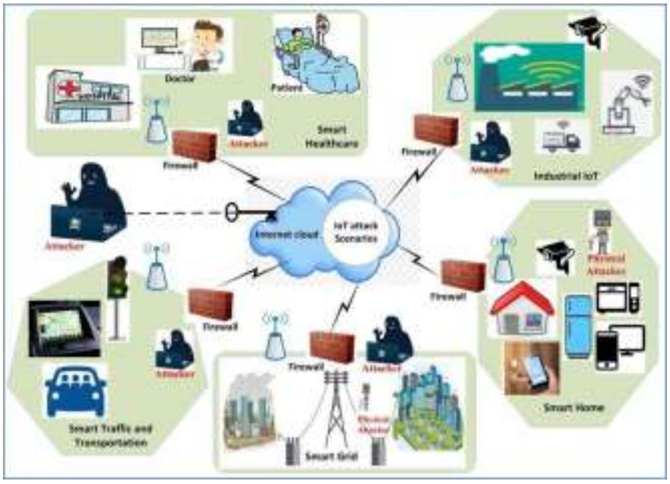

Figure 2: IoT Security Attack Scenarios in DifferentApplication Areas

Cybersecurity's primary focus is on safeguarding hardware,software, data, people, and the processes through which systemsare accessed, including the physical security of systems and theprotection of information stored within them. Key security goalsare commonly summarized in the CIA triad, which stands for: Confidentiality: Ensuring that sensitive information is not disclosedto unauthorized individuals or systems.

Integrity: Protecting data from unauthorized alteration ordestruction.

Availability: Ensuring that authorized users can access informationand systems when needed. as society becomes increasingly dependent on information technology—from desktop computers to smartphones and connected devices in the Internet of Things (IoT)—cybersecurity threats grow more pervasive, exposing systems to a variety of malicious attacks. These attacks can exploit vulnerabilities indifferent ways, such as:

Backdoors: Hidden methods for bypassing standard security protocols, either intentionally placed during system design or added by an intruder later.

Denial-of-Service (DoS) Attacks: Disrupting access to systems by overwhelming them with traffic or locking users out by repeatedly entering incorrect credentials.

Direct Access Attacks: Gaining unauthorized entry into systems withthe intent to steal data or modify system configurations.

Phishing: Deceptively gathering sensitive information, such as login credentials or financial data, typically via fraudulent emails or websites.

Social Engineering: Manipulating individuals into revealing confidential information, often by impersonating trusted figures like managers or representatives from legitimate organizations.

Spoofing: Falsifying data, such as an IP address or email sender identity, to mislead or gain unauthorized access.

These threats highlight the critical need for robust cybersecurity measures to defend against both external and internal risks.

Cybersecurity

Cybersecurity is increasingly important due to the widespread connectivity of devices to the Internet, making them vulnerable tohacking. A key aspect of cybersecurity is intrusion detection, which monitors computer or network activities for potential security issues, including system weaknesses and unusual behaviors. There are two primary types of intrusion detection: signature-based, which identifies known attacks through specific behaviors, and anomaly- based, which employs statistics and Al to detect unknown threats.Additionally, risk determination is the process of assessing the level of risk associated with a system.

Challenges: Cybersecurity faces several challenges, including the rapid evolution of sophisticated cyber threats like ransomware, phishing, and zero-day exploits. The growing adoption of cloud computing and the Internet of Things (IoT) expands the attack surface, while a global shortage of skilled cybersecurity professionalshinders effective threat management. Additionally, maintainingsecurity in hybrid work environments and ensuring compliance with complex regulations adds to the difficulty. Attackers often exploit human error, making user education and awareness crucial. Balancing robust security with usability and cost-effectiveness remains a constant challenge in the ever-changing digital landscape Cybersecurity challenges are multifaceted and continually evolving. One significant issue is the rise of advanced persistent threats (APTs) where attackers infiltrate systems and remain undetected for long.

Energy providers Eneregy generation	Transmission	Distribution	Consumers

time generationmonitoring	'ransmissionlines controlling	Jnderground cable system monitoring	omatic meter reading (smartmetering)
Power plants controlling	Power monitoring	ansformers stations controlling	Home (Residential) eneregy management
ternate energy sources controlling			solar panels management
Residential (distributed) Production monitoring			predicting future solar panels and wind turbineproduction (using sensor data like temperature or humidity)

Internet of Things (IoT)

The Internet of Things (IoT) is a system that connects the internet with physical objects from various areas like smart homes, industrial processes, healthcare, and environmental monitoring. IoT increases the number of internet- connected devices in our daily lives. While the internet brings many benefits, it also creates security challenges. IoT applications can range from simple smart home devices to complex industrial equipment. In a smart home, devices communicate wirelessly through a network called a Wireless Sensor Network (WSN), which is an important part of IoT.

To protect your smart home, it is advised to:

- Secure your devices and keep their software updated.
- Buy smart devices from trusted vendors.
- Upgrade your home network's security.
- Decide if you want to use public or private cloud services.
- Use a Virtual Private Network (VPN) to protect yournetwork from attacks.

In smart cities, which are expected to grow significantly by 2030, IoT is used for things like smart parking, traffic management, waste management, water and energy management. By 2035, more than 70% of people are expected to live in cities, and there will be around 50 smart cities globally.

IoT operations happen in three stages: collection, transmission, and processing. The collection stage gathers data about the physical world, while the transmission stage sends this data to applications and users. Different networks like Ethernet, WiFi, and DSL help transmit the data over long distances.

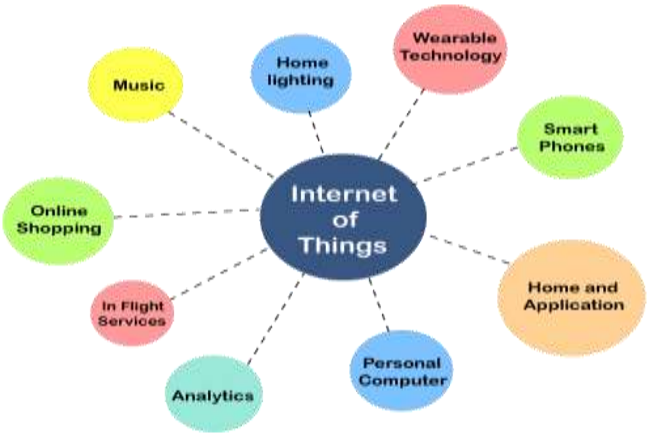

Fig-3: Application of IoT

Table 2: Intrusion detection methods. Reproducedwith permission

Category	Method
Signature-based	State Transition Analysis PetriNets
Anomaly-based	Markov Chain
	Neural Networks
	Support Vector MachinesDecision Tree
	Random Forests K-means
	k-Nearest Neighbor Clustering

"Green" IoT focuses on addressing key challenges, including:

- Integrating energy efficiency across the IoT system to ensuregood performance.
- Reducing the environmental impact.
- Ensuring the reliability of green IoT systems.
- Incorporating context-awareness.
- Making devices and communication protocols energy-efficient with low power usage.
- Simplifying the green IoT infrastructure.
- Balancing dynamic spectrum sensing with effective spectrum management.
- Using energy sources like wind, solar, vibration, and thermal for IoT.
- Managing cloud resources efficiently to minimize power consumption.
- Implementing energy-efficient security measures, such as encryption and control commands.

Green IoT focuses on making Internet of Things (IoT) technologies more sustainable by improving energy efficiency, reducing e-waste, and promoting eco-friendly practices. It involves designing low-energy devices, using sustainable materials, and optimizing data transmission to minimize power consumption. Additionally, it encourages edge computing, where data processing occurs closer to the source, reducing the need for cloud-based energy use. Green IoT also supports smart energy systems like smart grids, which optimize energy usage, and promotes a circular economy by encouraging the reuse and recycling of IoT devices. Overall, Green IoT aims to make technology more environmentally friendly while maintaining its functionality.

Fig-4: Smart Home

The Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) differs from the IoT in a domestic setting, where the focus is on convenience andentertainment. In contrast, IIoT aims to optimize industrial processes, particularly supply chains. Often referred to as "Industry 4.0" (or "Industrie 4.0" in Germany), IIoT is a termencompassing technologies and concepts that reshape valuechain organization. In the modular "Smart Factories" of Industry 4.0, Cyber-Physical Systems (CPS) monitor physicalprocesses, create virtual representations of the real world, and enable decentralized decision-making. These systems communicate in real-time over the Internet of Things (IoT) and collaborate with both other CPS and humans. Through the Internet of Services (IoS), participants in the value chain can access and offer internal and cross-organizationalservices.

Another definition of IoT describes it as a network ofinterconnected infrastructures that manage connected objects.These objects, often sensors or actuators, perform specific functions and communicate with other devices. These "smart objects" can generate, exchange, and consume data with little or no human intervention. They typically feature connectivity to remote data collection, analysis, and management systems.

However, the increasing use of IIoT also brings concerns aboutcybersecurity. Hacking attacks on industrial control systems (ICS) are becoming more frequent, and four primary security challenges are associated with IIoT:

1. Understanding the transition from offline to onlineinfrastructure.

2.Managing security across temporal dimensions.

3.Bridging the gap in implementing best security practices.

4.Addressing the complexity of industrial infrastructure.

These issues must be addressed to ensure the secure and efficient integration of IIoT into industrial environments.

Safety And Security:

Integrity: Protects data from unauthorized or accidental alterations, ensuring its accuracy and consistency. **Authentication**: Verifies the identity of the data source,confirming that it is indeed who it claims to be.

Non-repudiation: Guarantees that the sender of a messagecannot deny having sent it, ensuring accountability.

Availability: Ensures that the system and its services remainaccessible and functional for authorized users when needed.

Privacy: Safeguards users' identities by making themuntraceable and unlinkable to their behaviors or actions.

Confidentiality: Ensures that information is kept secure and inaccessible to unauthorized individuals, entities.

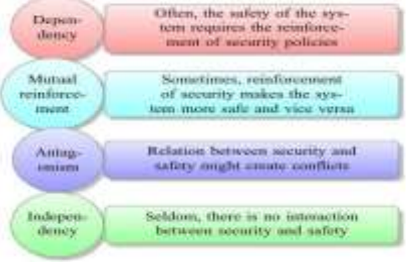
Depen-dency
Often, the safety of the system requires the reinforcement of security policies
Mutual reinforce-ment
Sometimes, reinforcement of security makes the system more safe and vice versa
Antag-onism
Relation between security and safety might create conflicts
Indepen-dency
Seldom, there is no interaction between security and safety

Fig-5: Relationship between safety and security incyber-physical systems

2. CONCLUSION

In the Internet of Things (IoT), the digital world intersects with the physical one, introducing unique security challenges. Unlike traditional hacking, which typically focuses on manipulating data, IoT attacks can extend to controlling physical devices and their operations. The sheer volume of data generated by IoT devices is immense, often surpassing the data produced by human-driven internet activity. As a result, IoT systems are vulnerable to several security risks. A key issue highlighted in the literature is thatmany IoT devices are often deployed and then left unmonitored or unupdated, making them easy targets for hackers. Scanning IoT devices for potential vulnerabilities iscrucial to safeguard both security and privacy. Critical security concerns in the IoT include privacy, authorization, verification, access control, system configuration, and the management of information storage. To address these challenges, organizations need to develop and implement robust cybersecurity strategies. Simple solutions, such as deploying two firewalls from different vendors, have also been suggested, as the likelihood of a vulnerability affecting both systems is low**.**

Outlook: Future internet technologies relevant to the Internet ofThings (IoT) include cloud computing, semantic technologies, autonomy, situation awareness, and cognitive systems. Additionally, emerging technologies like blockchain, Software Defined Networking (SDN), and 5G areplaying crucial roles in enhancing security, particularly for IoT and Industrial IoT (IIoT) applications. For instance, IBM developed the first IoT platform leveraging blockchain,called ADEPT (Autonomous Decentralized Peer-To-PeerTelemetry), back in 2013. As IoT security continues toevolve, there is an increasing focus on mobile devices andservice robots. Security risks in IT-driven industries areexpected to surpass those in non-IT sectors, underscoringthe critical need for robust security frameworks. Given therapid expansion of IoT devices across various domains of modern life.

3. REFERENCES

[1] Djamel Eddine K, Abdelmadjid B, Hicham L (2018) Internet of things security: A top-downsurvey. Computer Networks 141: 199-221.

[2] Saad Albishi, Ben Soh, Azmat Ullah, Fahad Algarni (2017) Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science 124: 608-614.

[3] http://www.itrco.jp/libraries/RFIDjournal- That%20Internet%20of%20 Things%20Thing.pdf

[4] Stojkoska BR, Trivodaliev KV (2017) A review of Internet of Things for smart home: Challenges and solutions. J Clean Prod 140: 1454-1464.

[5] Sfar AR, Natalizio E, Challal Y, Chtourou Z (2017) A roadmap for security challenges in the Internet ofThings Digital Communications and Networks 4:118-137.

[6] Ray PP (2016) A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences 30: 291-319.

[7] Sahmim S, Gharsellaoui H (2017) Privacy andSecurity in Internet-based

[8] Wu D, Ren A, Zhang W, Fan F, Liu P, et al. (2018) Cybersecurity for digital manufacturing. Manuf Syst, pp: 647.Banerjee M, Lee J, Raymond Choo KK (2017) A blockchain future for internet of things security: a position paper. Digital Communications and Networks 4: 149-160.