A Comprehensive Analysis Of Internet Of Things (IoT) Driving New Business Models With Emphasis On Challenges Associated With Security, Privacy And Awareness Factors

Tejas Thakral
Vivekananda Institute of Professional Studies
Delhi

[1]*Date of Receiving: 30 November 2022; Date of Acceptance: 21 January 2023; Date of Publication: 10 March 2023*

ABSTRACT

One of the hottest topics in business and research right now is the Internet of Things (IoT), often known as the Internet of Intelligent Things. In order to facilitate monitoring, automation, and decision-making within organizations, the term "Internet of Things" (IoT) refers to systems that incorporate compute, sensing, and communication. It also involves the link between humans and non-human physical objects. A network of "smart" gadgets that connect and communicate over the Internet is known as the Internet of Things (IoT). The Internet of Things (IoT) aims to create a pervasive and ubiquitous environment (i.e., an IoT ecosystem) with a variety of things or objects (e.g., washing machines, smart TVs, RFID tags, sensors and actuators, smart phones, etc.) that can cooperate and work autonomously to achieve shared objectives and provide smart services for the benefit of humanity. IoT allays worries about security and privacy because of the general public's lack of awareness of devices, the lack of standards for devices, and the features of the technology, which are extremely dynamic and constantly changing due to mobility. The research in this paper primarily focuses on the idea of the Internet of Things (IoT), architecture, new business models, security and privacy challenges, and cyber security awareness in relation to IoT threats. It also provides ideas for mitigating or reducing these IoT

INTRODUCTION

One of the most popular and talked-about topics in business and research today is the Internet of Things (IoT), often known as the Internet of Intelligent Things. In order to facilitate monitoring, automation, and decision-making within organizations, the term "Internet of Things" (IoT) refers to systems that incorporate compute, sensing, and communication. It also involves the link between humans and non-human physical objects. A network of "smart" gadgets that connect and communicate over the Internet is known as the Internet of Things (IoT). Establishing a pervasive and ubiquitous environment (also known as an IoT ecosystem) with a range of items or objects (such as RFID tags, sensors and actuators, smart phones, washing machines, smart TVs, etc.) is the idea behind the Internet of Things. that are able to work together autonomously and cooperatively to achieve shared objectives while offering intelligent services for the good of humanity. The consumer market and the global environment are about to enter a new era of business models where everything will be connected to each other through the Internet of Things. These "things" include things like routers, security cameras, smart TVs, doorbells like Google Nest, home assistants like Amazon Echo or Google Assistant, energy management (like the Smart Grid), healthcare management (like heart monitors), and urban living (like the Smart City). as well as a smart refrigerator (Figure 1-NIST) that can notify your smartphone. The internet of things extends to autos as well, as some models can transmit diagnostic data to your email or phone. Embedded processors will enable at least 50 billion more things to become intelligent by 2020. The Internet of Things aims to unify everything under a unified communication infrastructure, enabling organizations to manage anything from any location. Global researchers have estimated that by the end of 2025, there will be roughly 100

[1] *How to cite the article:* Thakral T (2023) A Comprehensive Analysis Of Internet Of Things (IoT) Driving New Business Models With Emphasis On Challenges Associated With Security, Privacy And Awareness Factors; *International Journal of Inventions in Engineering and Science Technology*, Vol 9, Issue 1, 37-43

billion connected IoT devices, with a corresponding $11 trillion in economic impact. Such Internet of Things (IoT) will have a remarkable effect on our civilization. About that figure, the only thing that is definite is its exponential rise. additional connections seem to lead to additional risks, though. Cybercriminals are constantly searching for new ways to break into networks by taking advantage of security holes. IoT allays worries about security and privacy because of the general public's lack of awareness of devices, the lack of standards for devices, and the features of the technology, which are extremely dynamic and constantly changing due to mobility. Cybersecurity features that guard against potential dangers and harmful cyber activities are essential for these smart devices in our homes and companies.

The concept of IoT, architecture, new business models, security and privacy issues, suggested countermeasures, and cyber security awareness in IoT threats are the main topics of discussion in this chapter. It also outlines recommendations for mitigating or reducing the effects of these IoT concerns, as well as for raising public awareness of cybersecurity threats related to IoT.

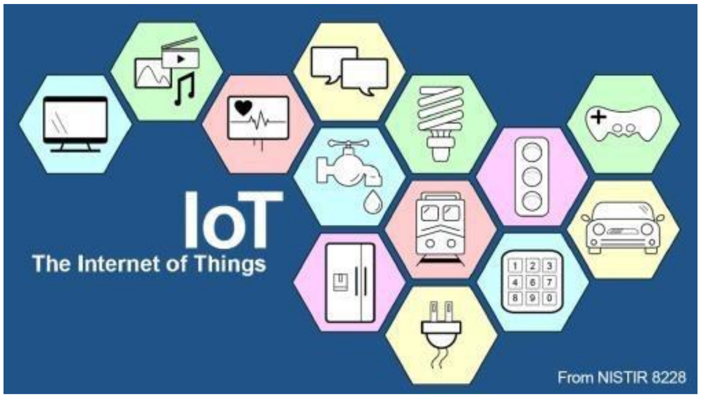

Fig 1 from the NIST-IoT report

THE WORLD-WIDE WEB'S ARCHITECTURE

According to [11-figure 2] Three levels make up a general Internet of Things architecture: the application layer, the transport layer (which includes gateways, networks, management and security services), and the sensing and connectivity layer. The application layer acts as a user interface for the Internet of Things and uses intelligent computing technologies (such as data mining and cloud computing) to extract useful information from processing large amounts of data or big data. While the sensing layer is in charge of gathering data and information, the transport layer handles network activities.

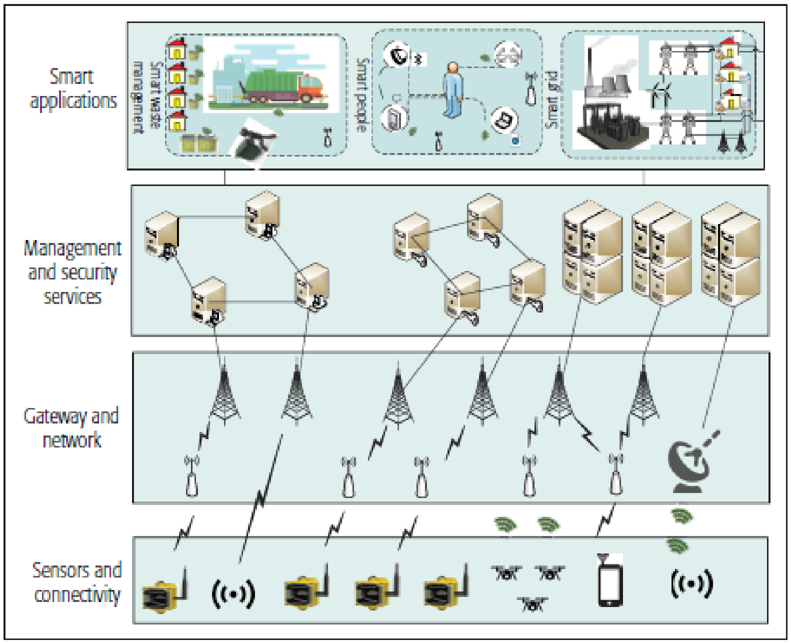

Fig 2: Internet of Things Architecture [11]

Based on [12], the structure of IoT is divided into five layers as illustrated in Fig. 3. These layers are briefly explained as follows:

1) Perception Layer: Also known as the "Device Layer," this layer is made up of physical objects and sensor devices. Depending on the method used to identify the objects, the sensors can be any of the following: temperature, pressure, proximity, accelerometer, gyroscope, infrared, gas, smoke, RFID, or 2D-barcode. This layer essentially deals with the identification and collection of information and data specific to objects by the sensor devices. In terms of type of sensors, Location, temperature, direction, motion, vibration, acceleration, humidity, and chemical changes in the air are a few examples of the data that can be included. After that, the information and data are transferred to the network layer so that the information processing system may receive them securely.

2) Network Layer: Another name for this layer is "Transmission Layer." The data and information from sensor devices are securely transferred to the information processing system by this layer. Depending on the sensor devices, the transmission channels may be wired (guided) or wireless (unguided), and the networking technologies may include 3G, 4G, 5G, 6G, UMTS, WiFi, WiMax, Bluetooth, infrared, ZigBee, etc. Information is therefore transferred from the Perception layer to the Middleware layer via the Network layer.

3) Middleware Layer: By acting as a connectivity layer for sensors, middleware is a component of the architecture that enables connectivity for a vast array of different Things. The Internet of Things' sensor devices carry out various services. Only other devices running the same service type are connected to and communicate with by each device. This layer connects to the database and is in charge of service management. It stores the data in the database after obtaining it from the network layer. It does ubiquitous computation, information processing, and automatic decision-making based on outcomes. The major objective is to put in place an autonomous decision-making mechanism that will operate as a relay for actuation commands to be sent back to the physical objects, allowing them to carry out activities that will modify the physical environment's overall conditions. The Application layer may use the gathered and analyzed data to control the system as a whole or to provide it to an end user.

4) Application Layer: Based on the data from the objects that the Middleware layer processed, this layer offers worldwide application management. Smart manufacturing, smart transportation, smart agriculture, smart homes, smart cities, smart manufacturing, and smart health are just a few of the uses for IoT.

5) Business Layer: This layer is in charge of overseeing the management of the applications and services as well as the entire Internet of Things ecosystem. Using information from the application layer, it creates graphs, flowcharts, and business models, among other visual aids. Effective business models are also essential for the long-term success of IoT technology. This layer will assist in determining the tasks and business strategies for the organization's future activities based on the analytical modeling of the outcomes. System administrators may strategically oversee and manage the IoT platform's overall functionality thanks to the Business layer.

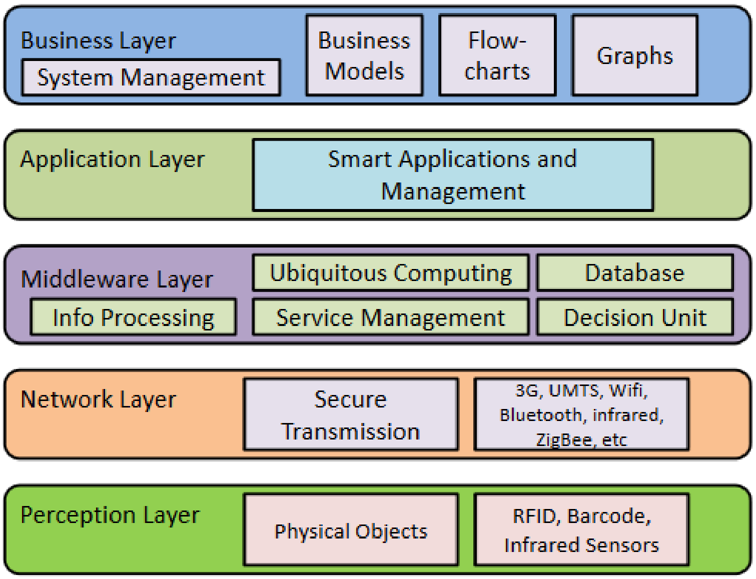

Fig 3: The Architecture of the Internet of Things [12]

Business model for the Internet of Things IoT platforms were listed as a new business model architecture in Gartner's Hype Cycle for Emerging Technologies in 2018. Because IoT devices are inherently linked and provide data, there are numerous fresh approaches to creating creative business models. Products can now provide a variety of digital services beyond core functionality thanks to the IoT business model. Vendors integrate several features to provide a distinctive consumer experience along with improved online services. According to [16], IoT has the potential to significantly innovate company models. Innovation in business models will be particularly noticeable in areas where IoT enterprises engage with their clientele. It might be difficult for farmers in the front lines of business to monitor farm water and determine when to refill their water tanks. An Internet of Things (IoT) device can be used to install a sensor in the water tanks to track the water level and notify the controlling station through text or email if the water level, flow, or pressure deviates from a pre-established range. Applying IoT product solutions improves the business farm's water usage efficiency. Monitoring of senior care is crucial to the health care industry; therefore, IoT device movement sensors are positioned throughout the house to send activity data. Data is gathered by the sensors and transmitted via cellular technology to an application. By keeping the healthcare practitioner informed about their activities, the monitoring system can help ease the tension of the family. How can we increase the effectiveness of waste collection in a smart city? The smart garbage can can be equipped with Internet of Things goods to track and report on its condition and to notify users when it needs to be emptied. drained away. Applying IoT products reduces pollution because there is less traffic on the streets and trash cans are never full. How can we defend our home in the smart home? IoT device sensors are used throughout the house to pick up sound and motion. You can use a web interface or a smartphone app to monitor the security system. As a result, there is less crime in the area. Philips, a company in the medical field, has developed networked CT, ultrasound, and X-ray scanners. Rather than only supplying hospitals with the equipment, the company has collaborated with them to gather data in imaging rooms, determine the optimal machine count, and remove inefficiencies. GE Farm has created sensors specifically for wind farms. The sensors, which are affixed to turbine blades, can assist in automatically modifying the blade angle to benefit from variations in wind direction. Through the use of IoT products, GE is able to better schedule turbine maintenance, prioritize repairs, and make better use of the time spent by maintenance staff. According to [17] From the standpoint of business models, one of the major effects on a lot of firms is the shift from manufacturing and retailing physical goods to service-oriented company models. For instance, producers of lightbulbs, have historically been concentrated on production costs and product quality, depending on the markets in which they offer services. But the manufacturer of smart lightbulbs, Philips, is moving away from this more traditional business strategy of emphasizing the production process and toward being a service provider as well. Their internet-connected smart lights create data that may be used to track consumption trends and malfunctions. The Internet of Things (IoT) is a significant advancement in the field of computing and communication technology. It is creating new business models to capitalize on the opportunities that arise from integrating various technologies within an enterprise.

INTERNET OF THINGS SECURITY, CONFIDENTIALITY, AND VIGILANCE

In order for the Internet of Things to positively impact society, cybersecurity awareness, education, and training for aided users will be necessary. We must so enlighten and teach the public on ways that users might reduce the risks associated with IoT environments. The Australian government issued and published The Code of Practice in August 2020. Protecting Consumers' Access to the Internet of Things The best practices for protecting consumers' internet of things, and the voluntary code of conduct is predicated on thirteen guiding ideas. The following is a list of these principles: No redundant default passwords or weak passwords Establish a policy for disclosing vulnerabilities, maintain software updates safely, Keep credentials safe. Make sure personal information is secure, reduce the number of areas that are open to attack, make sure communication security, make sure software integrity, enable systems to withstand disruptions. Track telemetry data from the system, make it simple for customers to remove personal information, make device maintenance and installation simple, and Verify the info that was entered. The Code of Practice for Consumer IoT Security was also released in the United Kingdom. It compiles the generally accepted best practices for IoT security into thirteen outcome-focused standards. The Internet of Things Security for Small and Medium Organizations is a document published by the Canadian government that explains the internet of things and how to safeguard customers in its environment. The report's points of awareness center around protecting your wireless network. Use secure passwords and alter the device's default username and password. Networks containing sensitive data should be kept apart. Think about putting IoT devices on different networks, make sure the device can be reset to remove sensitive configuration data permanently; regulate who can access your network and from where; encrypt commands, data, and communications in transit and at rest; configure operating systems, software, and firmware to update automatically whenever possible; and set up periodic manual updates as needed. Understanding your IoT devices is one of the most important aspects of IoT security. The FBI compiled information in their study "Be Vigilant with Your Internet of Things (IoT) Devices" to help consumers reduce the risks associated with IoT devices. Since many devices come with default passwords or open Wi-Fi connections, the research advises changing them to strong passwords and limiting the device's use to networks with secured Wi-Fi routers. Handle and safeguard your wireless networks; for instance, install firewalls, create secure, complicated passwords, and think about limiting the devices that can connect to your network by utilizing media access control address filtering. Create a layer of security for your home. If your router is capable of supporting several networks, you may divide your computer devices from your Internet of Things devices and route them across multiple networks. In this manner, the damage caused by cybercriminals breaking into a single network will be restricted to the devices on that single network. Disable your router's Universal Plug and Play (UPnP) protocol. Many IoT devices can be accessed by exploiting UPnP. Before making a purchase, research devices. Examine reviews to obtain suggestions; conduct study their security capabilities, buy Internet of Things (IoT) devices from suppliers who have a reputation for producing safe products, and enable automatic upgrades for your devices when they become available. Additionally, a law pertaining to Internet of Things devices was approved in the US in order to use federal government procurement power to promote improved cybersecurity for Internet of Things devices. There are two studies on the Internet of Things from the perspective of the European Union. The first report was prepared by the Working Group on a cybersecurity consumer perspective of the ENISA (The European Union Agency for Network and Information Security) Advisory Group, and it was released in relation to the Good Practices for Security of Internet of Things. The study aims to raise awareness of the relevant dangers and risks with an emphasis on "security for safety" and to serve as a reference point for collaboration on Industry 4.0 and Industrial IoT security across the European Union. ESTI is the one who prepared the second report. The European Standards Organization (ETSI) is an ESO. CYBER, or Cyber Security for Consumer Internet of Things, is the subject of the study report. The study report compiles a number of high-level, outcome-focused security best practices for consumer devices with internet connections. The consumer IoT's cyber security features are built around, Not a single default password for everyone, Establish a system for handling vulnerability reports, Update your software. Store critical security parameters in a secure manner. Talk safely, Reduce the amount of open attack surfaces, guarantee program integrity, and make sure personal information is safe. Enable systems to withstand disruptions. Analyze data from system telemetry, Make user data deletion simple for users. Make device maintenance and installation simple, and ensure that input data is accurate.

CONCLUSION

Our lives are being affected by the rapidly evolving digital world of today, and we are becoming more and more dependent on the internet. As the world transitions to Industry 4.0, IoT has become more widespread and is continuing to broaden its reach across all industries. Through its capacity to help businesses create value-added services with their network of machines and devices, enhance their service business models, and boost sustainability, the Internet of Things has brought about a paradigm shift that is drastically altering how businesses conduct business. IoT security is a process rather than an absolute and cannot be guaranteed. Since new vulnerabilities are always being found, it is necessary to continuously monitor, Maintain and routinely examine the policy, practice, and risk. Every stage of the Internet of Things journey carries a danger to digital security, as there are hackers waiting to exploit any weakness in a system. Because of this, risk management is crucial to this procedure. Any IoT company should start with a comprehensive security risk identification and assessment, which looks for weaknesses in user and customer backend systems, network systems, and devices. Throughout the deployment's whole IoT lifespan, risk must be reduced. Furthermore, it is crucial for customers to recognize that they can lessen the danger of cyberattacks by making sure their devices are updated and patched, which helps to minimize vulnerabilities and threats.

REFERENCES

[1] ETSI (European Telecommunications Standards Institute). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101 p.pdf

[2] Australian Government- Code of Practice-Securing the Internet of Things for Consumers.https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[3] Canadian Government for IoT. https://cyber.gc.ca/en/guidance/internet-things-security-small-and-medium-organizationsitsap00012

[4] FBI https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iotdevices

[5] ENISA (The European Union Agency for Network and Information Security). https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/agpublications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

[6] NIST -IoT. https://csrc.nist.gov/publications/detail/nistir/8259/archive/2020-01-07

[7] Marcel Medwed, IoT Security Challenges and Ways Forward, ACM ISBN 978-1-4503-45675/16/10., DOI: http://dx.doi.org/10.1145/2995289.2995298

[8] Elisa Bertino, Research Challenges and Opportunities in IoT Security, ACM. ISBN 978-1-4503-5393-9/17/10…. DOI: https://doi.org/10.1145/3139531.3139535

[9] Internet of Things (IoT) Cybersecurity Improvement Act of 2019-Law. https://www.scribd.com/document/401616402/Internet-of-Things-IoT-CybersecurityImprovement-Act-of-2019

[10] United Kingdoms-Code of Practice for Consumer IoT Security https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file /773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[11] Yaqoob et al., "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," in IEEE Wireless Communications, vol. 24, no. 3, pp. 10-16, June 2017, doi: 10.1109/MWC.2017.1600421.Volume: 24, Issue: 3, June 2017), DOI: 10.1109/MWC.2017.1600421

[12] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges. In 2012 10th International Conference on Frontiers of InformationTechnology (FIT): Proceedings (pp. 257-260). Institute of Electrical and Electronics Engineers Inc..https://doi.org/10.1109/FIT.2012.53

[13] Antão, Liliana & Pinto, Rui & Reis, João Pedro & Gonçalves, Gil. (2018). Requirements for Testing and Validating the Industrial Internet of Things. 10.1109/ICSTW.2018.00036.

[14] Amaral, Leonardo & de Matos, Everton & Tiburski, Ramão & Hessel, F. & Tessaro Lunardi, Willian & Marczak, Sabrina. (2016). Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G. 10.1007/978-3-319-30913-2_15.

[15] Michael Blanding, the internet of things needs a business model. Here it is, 2019, The Internet of Things Needs a Business Model. Here It Is - Harvard Business School Working Knowledge (hbs.edu)

[16] Imen Ben Chaabane, Busines model of IoT-From supplier to customer, International Telecommunication Union, 2017, business model of IoT.pdf (itu.int)

[17] De Saulles, Martin. (2019). Building Business Models for the Internet of Things: a Literature Review. 10.13140/RG.2.2.23201.15200.

[18] In Lee, The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model, Internet of Things, Volume 7, 2019, 100078, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2019.100078.