Leveraging the Internet of Things (IoT) Algorithms, Tools and Techniques in Creating Disruptive and Innovative Business Models

Shweta

Symbiosis College of Arts and Commerce, Pune

ABSTRACT

The Internet of Things (IoT), also known as the Internet of Intelligent Things, is a focal point of discussion and innovation in business and research realms. It encompasses systems integrating computation, sensing, and communication to connect human and non-human entities, fostering organizational monitoring, automation, and decision-making. IoT establishes a network of 'smart' devices interconnected via the Internet to create a pervasive and ubiquitous environment or IoT ecosystem. This ecosystem comprises various objects, including RFID tags, sensors, actuators, smartphones, and household appliances, collaborating autonomously to deliver intelligent services for humanity's benefit. However, challenges such as public awareness gaps, device standardization issues, and the inherently dynamic nature of IoT, influenced by factors like mobility, pose significant hurdles.

Consequently, concerns regarding security and privacy have been raised. This paper delves into IoT's conceptual framework, architecture, and emerging business models and addresses security and privacy issues. It proposes countermeasures and emphasizes cybersecurity awareness's importance in mitigating IoT-related threats effectively. Additionally, recommendations are provided to alleviate the impacts of these concerns on IoT deployment and utilization.

INTRODUCTION

The Internet of Things (IoT), alternatively termed the Internet of Intelligent Things, dominates contemporary discussions within the business and research spheres. It encompasses systems integrating computation, sensing, and communication, facilitating connections between human and non-human entities to enable organisational monitoring, automation, and decision-making. The IoT manifests as a network of 'smart' devices interconnected via the Internet, aiming to create a pervasive and ubiquitous environment known as the IoT ecosystem. This ecosystem comprises diverse objects such as RFID tags, sensors, actuators, smartphones, household appliances, and more, which autonomously collaborate to deliver intelligent services for humanity's benefit.

The advent of IoT marks a significant shift in business models, where virtually everything communicates with each other via IoT. These 'things' span a broad spectrum, from routers, security cameras, and smart TVs to home assistants like Amazon Echo or Google Assistant, doorbells like Google Nest, energy management systems (e.g., Smart Grid), healthcare devices (e.g., heart monitors), and urban infrastructure (e.g., Smart City initiatives). Even everyday items like smart refrigerators, capable of sending alerts to mobile phones, and cars transmitting diagnostic information to emails or phones are integral to the Internet of Things. Projections suggest that by 2020, an additional 50 billion devices will transition to smart status through embedded processors. IoT aims to unify diverse elements under a single communication infrastructure, empowering organizations with unprecedented control from any location.

Global projections estimate that the number of connected IoT devices will nearly double to 100 billion by the end of 2025, with an anticipated financial impact exceeding $11 trillion. This exponential growth underscores the extraordinary societal impact of the Internet of Things, albeit accompanied by escalating vulnerabilities.

Cybercriminals continuously exploit vulnerabilities to gain unauthorized access to systems, necessitating robust cybersecurity provisions for smart devices in homes and businesses.

However, challenges persist, including public awareness gaps, lack of device standardization, and the dynamic nature of IoT influenced by mobility. Consequently, concerns regarding security and privacy loom large. It is imperative to address these challenges effectively by implementing suggested countermeasures, fostering cybersecurity awareness, and devising strategies to mitigate the impacts of IoT-related concerns.

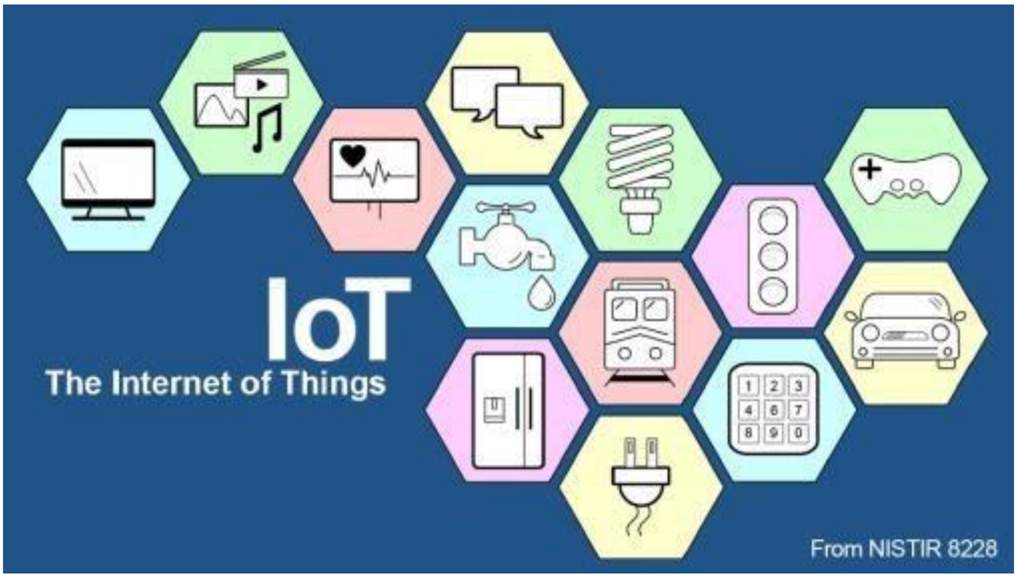

Figure 1-NIST-IoT publication

This chapter primarily focuses on elucidating the concept of IoT, its architectural framework, emerging business models, and the security and privacy challenges it poses. It proposes countermeasures to mitigate IoT threats and underscores the importance of cybersecurity awareness among the public. Furthermore, it explores strategies to enhance public understanding of cybersecurity threats associated with IoT, emphasizing the critical role of proactive measures in safeguarding IoT ecosystems.

INTERNET OF THINGS ARCHITECTURE

Drawing from [11, Figure 2], a typical IoT architecture comprises three layers: the application layer, the transport layer (encompassing management and security services, gateways and networks), and the sensing and connectivity layer.

The application layer employs intelligent computing technologies, such as data mining and cloud computing, to extract valuable insights from vast amounts of data or big data. It serves as the interface between users and the IoT system.

The transport layer manages network operations, ensuring the smooth data flow between different IoT ecosystem components.

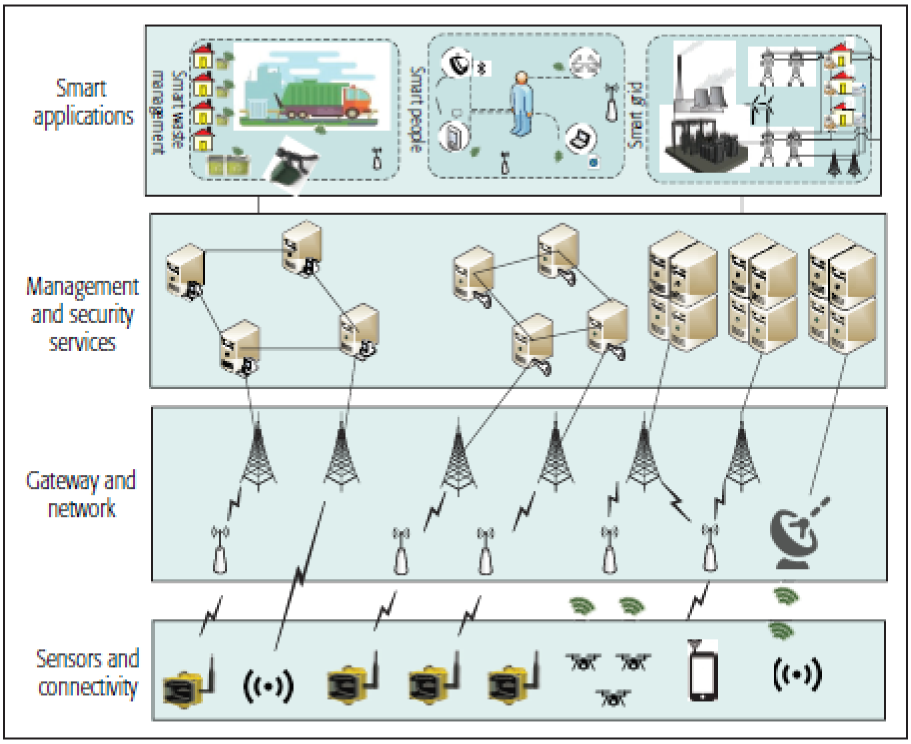

Figure 2: Internet of Things Architecture [11]

Meanwhile, the sensing layer collects data and information from various sources within the IoT network.

Based on [12], the structure of IoT is divided into five layers, as depicted in Figure 3. These layers are briefly described below:

1) Perception Layer: Also known as the "Device Layer," this layer comprises physical objects and sensor devices. Sensors may include Temperature Sensors, Pressure Sensors, Proximity Sensors, Accelerometers, Gyroscope Sensors, Infrared Sensors, Gas Sensors, Smoke Sensors, RFID, and 2D-barcode sensors, depending on the method of object identification. The Perception Layer primarily identifies and collects object-specific data and information using sensor devices. This information can pertain to location, temperature, orientation, motion, vibration, acceleration, humidity, chemical changes in the air, etc. The collected data and information are transmitted securely to the Network layer for further processing.

2) Network Layer: Also referred to as the "Transmission Layer," this layer securely transmits data and information from sensor devices to the information processing system. Transmission channels can be wired (guided) or wireless (unguided), and networking technologies may include 3G, 4G, 5G, 6G, UMTS, Wifi, Wifi 6, WiMax, Bluetooth, infrared, ZigBee, etc., depending on the sensor devices. The Network Layer facilitates the transfer of information from the Perception Layer to the Middleware Layer.

3) Middleware Layer: Middleware is a crucial architecture component, enabling connectivity for a vast array of diverse Things by providing a connectivity layer for sensors. Sensor devices within the IoT ecosystem execute various services, each connecting and communicating with others implementing the same service type. This layer manages service provision and maintains links to the database. It receives information from the Network layer, stores it in the database, conducts information processing and ubiquitous computation, and implements automatic decisions based on the results. The primary objective is to implement an autonomous decision-making process that sends actuation commands back to physical objects to execute actions affecting the overall environmental conditions. The collected/analyzed information can be presented to end-users via the Application layer, which may also be used to control the overall system.

4) Application Layer: This layer oversees the global management of applications based on the object's information processed in the Middleware layer. Applications performed by IoT can include innovative health, smart homes, smart farming, smart cities, smart manufacturing, intelligent transportation, etc.

5) Business Layer: Responsible for managing the overall IoT ecosystem, including applications and services; this layer constructs business models, graphs, flow charts, etc., based on data received from the Application layer. The success of IoT technology also hinges on robust business models. Analytical modelling of results supports determining future actions, tasks, and business strategies within organizations. The Business layer enables system administrators to manage and strategically control the overall functionality of the IoT platform.

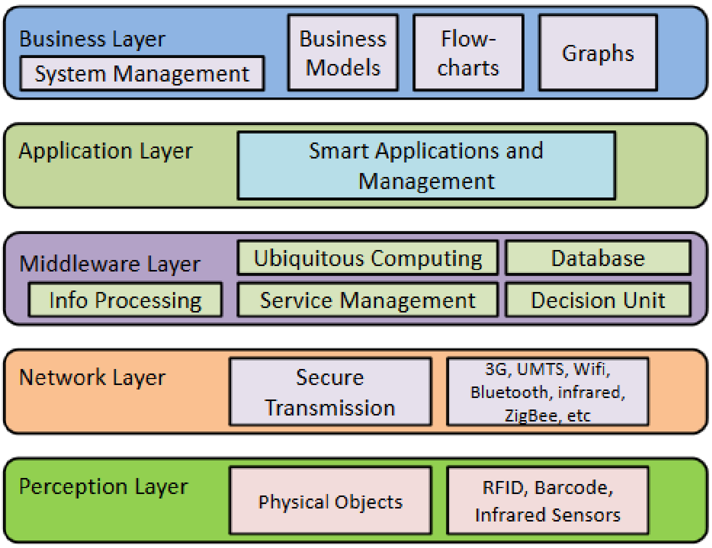

Figure 3- The IoT Architecture[12]

THE EVOLVING BUSINESS MODELS OF THE INTERNET OF THINGS (IoT)

In 2018, Gartner's Hype Cycle for Emerging Technologies recognized IoT platforms as pivotal to new business models. IoT devices, inherently interconnected and data-producing, facilitate diverse avenues for innovative business strategies. This evolution allows products to offer digital services beyond their core functions, enhancing customer interaction and expanding service offerings. Notably, IoT's impact on business models is most pronounced in customer interactions.

In various sectors, IoT applications have revolutionized operations. For instance, in agriculture, IoT aids in water monitoring, notifying farmers when tanks need refilling, thereby optimizing water usage. Similarly, in healthcare, IoT sensors enable elderly care monitoring, easing family concerns and providing vital data to healthcare providers. In urban settings, IoT enhances waste management efficiency by monitoring smart garbage bins, reducing pollution and traffic congestion.

In the realm of security, IoT finds extensive application. Home security systems utilize IoT sensors to detect motion and sound, empowering homeowners with remote monitoring capabilities. In healthcare, companies like Philips leverage IoT to not only sell imaging machines but also provide data-driven services, improving operational efficiency for hospitals. Likewise, GE employs IoT sensors in wind farms to optimize turbine maintenance schedules, enhancing productivity.

From a business model perspective, the shift is palpable, moving from product-centric models to service-oriented ones. Traditional manufacturers, like Philips, transition to service providers, utilizing IoT-generated data to offer value-added services. This shift underscores IoT's role in driving business innovation and service expansion.

SECURITY, PRIVACY, AND AWARENESS IN THE IoT LANDSCAPE

The proliferation of IoT devices necessitates a focus on cybersecurity awareness and education. Governments and organizations worldwide have released guidelines and codes of practice to mitigate IoT-related risks. These encompass principles such as avoiding default passwords, implementing vulnerability disclosure policies, ensuring software updates, and safeguarding personal data.

Various countries, including Australia, the UK, and Canada, have issued comprehensive guidelines to enhance IoT security. Recommendations include securing wireless networks, using strong passwords, isolating sensitive networks, and enabling automatic updates. Additionally, the FBI advises consumers to research devices before purchase, change default passwords, and segregate IoT devices from computing devices.

Legislation, such as the US law leveraging Federal procurement power for IoT cybersecurity and EU studies on IoT security standards, further emphasizes the importance of securing IoT ecosystems.

CONCLUSION

As society embraces Industry 4.0, IoT assumes a central role in transforming businesses across sectors. However, with this transformation comes the imperative of addressing security challenges. IoT security is an ongoing process, requiring continuous monitoring, risk assessment, and consumer awareness.

Effective risk management is essential throughout the IoT lifecycle, from deployment to maintenance. Consumers play a vital role in mitigating cyber threats by keeping devices updated and patched. Ultimately, a collaborative effort involving industry, governments, and consumers is crucial to harnessing the potential of IoT while ensuring its security and privacy.

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.