Journal of Electrical Engineering and Automation (ISSN: 2582-3051)
www.irojournals.com/iroeea/

# Security Challenges: M2M Communication in IoT

**Devasis Pradhan[1], Hla Myo Tun[2]**

[1]Department of Electronics & Communication, Acharya Institute of Technology, Bangalore, India
[2]Research Department, Yangon Technological University, Yangon, Republic of the Union of Myanmar

**E-mail:** [1]devasispradhan@acharya.ac.in , [2]hlamyotun@ytu.edu.mm

## Abstract

In recent times, smart devices, smart homes, smart manufacturing, and even smart cities, all of which are connected to the Internet of Things (IoT) have become quite common. IoT technology heavily relies on Machine-to-Machine (M2M) communication in order to make all smart technologies behave in a smart way. Any type of connection between two devices that does not require human intervention is referred to as "machine-to-machine" communication technology. The IoT is a system of devices with unique identifiers that can transmit information over a network. There is no interaction between humans or machines in the IoT. The IoT is now widely used in a variety of sectors, including banking (connected branches), and industries where secrecy and privacy of data are the important components. The IoT allows multiple machines to design a connected data network, whereas M2M makes it possible for devices to communicate with one another. Therefore, this paper gives a brief review work on security challenges faced in the connection between IoT and M2M communication and the significance of both technologies.

**Keywords:** M2M, IoT, Security, Privacy

## 1. Introduction

The market for the Internet of Things (IoT) permits various combinations of sensor network technologies and smart objects. A dynamic heterogeneous/multi-modal network can be deployed in remote or unreachable locations (mines, oil platforms, forests, pipes, tunnels, etc.) according to people who use communication protocols that are diverse and interoperable spaces or in emergency situations like fire, earthquakes, floods, radiation, and others. By sharing resources and significantly expanding the scope and dependability of the services that


*DOI: https://doi.org/10.36548/jeea.2022.3.006*
*Received: 12.08.2022, received in revised form: 09.09.2022, accepted: 25.09.2022, published: 06.10.2022*

result, these "things or objects" will realize, explore, and learn to take advantage of one another data in IoT infrastructure.

The majority of the information that is required by people, things, or objects will be accessible locally if storage capacity is increased at lower costs. Enhanced processing capabilities and always-on connectivity can go hand in hand with this. As a result, terminals/nodes will play a larger role in communications. Businesses and consumers alike stand to gain from the IoT. However, it also brings about new difficulties for security. The proliferation of IoT technology has resulted in the development of new security flaws that criminals can take advantage of. IoT between machines (M2M) presents a particular challenge i.e., hackers have the opportunity to interfere with the physical world through networked machines, which means that they put infrastructure and possibly human health and safety at risk.

## 2. Related Works

M2M is part of the IoT, which includes a lot of other technologies. Researchers have a lot of different ideas about IoT and M2M, so it has become a debate like “egg first” versus “hen first”. However, these two ideas technically differ in a great deal. The machine-to-human (M2H) interface communication protocol is used for interactions between intelligent machines and humans. The networking service that makes it possible for all smart machines to work together is IoT [1-3]. The bank ATM's credit or debit card is an illustration of M2M because the machine reads the information on the card and responds to the user's needs, and when the user leaves the bank, the lights and fans will automatically turn off. [2,5].

The IoT has emerged as a burgeoning field of study, and numerous approaches from a variety of perspectives have been investigated in an effort to boost its growth and popularity [4,6]. One trend is to think of the IoT as the Web of Things, where open Web standards are used to share information and connect devices. Traditional web services must be enhanced and integrated with the physical world when smart things are added to the existing web [4-7]. In the context of contemporary wireless telecommunications, the IoT is rapidly gaining a lot of attention. The fundamental idea behind concepts like RFID tags, sensors, actuators, mobile phones, and others, which are able to communicate with one another and work together with their neighbors to accomplish common objectives is due to distinctive addressing schemes [5-8]. In point of fact, before the IoT concept was widely accepted, there were a lot of difficult issues that need to be resolved, both technologically and socially, in order to guarantee trust,

privacy, and security, giving them a higher level of intelligence by allowing them to adapt and behave on their own. Additionally, the IoT concept introduces a number of brand-new networking issues.

## 3. IoT Technology

The idea of connecting devices, applications, sensors, and actuators through the internet is known as the IoT. They can exchange data with each other and with other devices thanks to this connection. They can be controlled and monitored from a distance using IoT. M2M technology was replaced by IoT technology. To put it in another way, the IoT is built on top of M2M's fundamental ideas by expanding them to large cloud networks of devices that use cloud networking platforms to communicate with one another. All IoT devices can use the cloud architecture's infrastructure, software, and platform. It enables users to construct networks that are quick, adaptable, and efficient, connecting a large amount of devices. The early IoT only served a limited purpose. In 1999, the term was only used to describe networked RFID tags. The development of faster mobile networks (known as 5G) made it possible for devices to transmit more complex data at a faster rate, which sparked the industry's rapid growth. The architecture of IoT environment enabled to 5G is depicted in Figure 1.

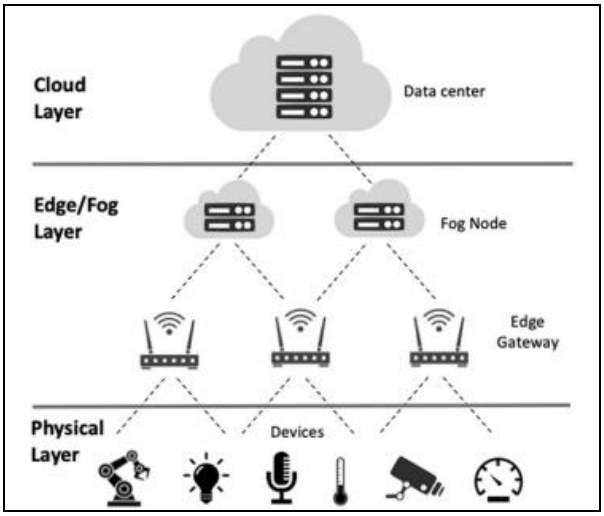


**Figure 1.** Basic IoT Architecture [2]

### 3.1 Factor adapting in IoT

**3.1.1 Cloud Flexibility**: Cloud storage and processing power are becoming more accessible and less expensive as a result of the growth of services like Microsoft Azure, enhancing the

capacity to analyze massive amounts of data. IoT scenarios give businesses the scalability and adaptability they need to start or expand an IoT solution.

**3.1.2 Connectivity:** Because mobile operators charged prohibitive prices for M2M connections, IoT solutions were previously restricted to wired or wireless local area network connections. However, not anymore. Mobile operators are embracing the IoT, fueled by the additional capacity provided by advanced cellular networks.

**3.1.3 Advancement of Software:** Companies all over the world now have access to high-level data analysis capabilities thanks to today's rich and dynamic business software.

**3.1.4 Cost of Hardware:** As production volumes have grown, components for the IoT like accelerometer, GPS sensors, and microchips have become less expensive. And it's not just about saving money; tiny microchips can now run more advanced software than ever before.

### 3.2 Building Blocks

The basic building block of IoT is shown in Figure 2.

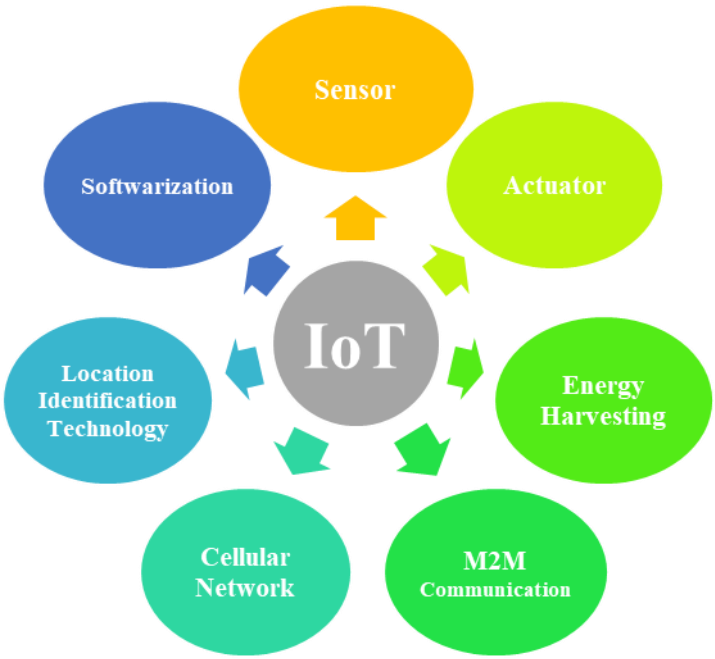


**Figure 2.** Basic Building Block of IoT Technology

**3.2.1 M2M Communication:** The protocol has been set between nodes by which electronic communication takes place machine-to-machine interfaces.

**3.2.2 Cellular Communication:** The majority of people in developed nations familiar with IoT could benefit greatly from a wide range of wireless technologies, including short- and long-range channels, as well as channels that are unidirectional and bidirectional.

**3.2.3 Energy Harvesting:** The Radio Frequency (RF) harvesting is one of the building blocks of IoT. The main advantage of harvesting is to store energy and can be used in an efficient manner. The consumption of power made by sensor, RFID tags and other interface toward network is very less which gives an implication of minimal usage of energy for a certain duration. This also helps in selecting channel which communication between the M2M inclined to IoT usage in a smarter way.

**3.2.4 Sensor & Actuators:** Sensor designers have access to a wide variety of environmental signals, including sound, light, atmospheric conditions, vibrations, and others. A relay, for instance, is an actuator that flips a mechanical switch. As a result, it can cause a lot of responses, such as turning on the lighting, heating system, and audible alarm, among other things. Fluids and objects can be moved and pumped by actuators like hydraulics, pneumatics, and motors.

**3.2.5 Softwarization:** Software capabilities are crucial to the IoT's growth in a variety of ways, including self-describing data structures and distributed execution.

**3.2.6 Location Identification:** Dead reckoning uses sensors, but it doesn't meet the real-world need for geo-location. As a result, wireless methods like GPS, which is often augmented by other signals, and cellular towers have grown in popularity. The locations of fixed or orbiting transmitters are known.

## 4. M2M Communication

M2M can be simply defined as the automated transmission of data between devices. To put it in another way, once the system is set up, M2M communication should not require human interaction. Through M2M, a temperature sensor hundreds of feet below the ocean's surface can collect data and transmit it to a central system without the need for human intervention. Similarly, M2M Serial, Powerline (PLC), and wireless connections are all parts of M2M. With the help of M2M, communication of embedded devices is similar to cellular communication. M2M and IoT are almost the same thing. Ethernet and cellular networks and other public networking technologies helps IoT to enable M2M exchange of information. One of M2M's applications is sensor telemetry, which allows businesses to remotely monitor

things like temperature, energy consumption, moisture, and pressure. For end-to-end communications between sensors in modern M2M communications networks, as well as in traditional WSNs, there is a need for assurance regarding the confidentiality, identity, integrity, authentication, access control, and non-repudiation of the transmitted data.

### 4.1 Standard

There is no standardized platform for devices in machine-to-machine technology, and many M2M systems are designed to be task- or device-specific.

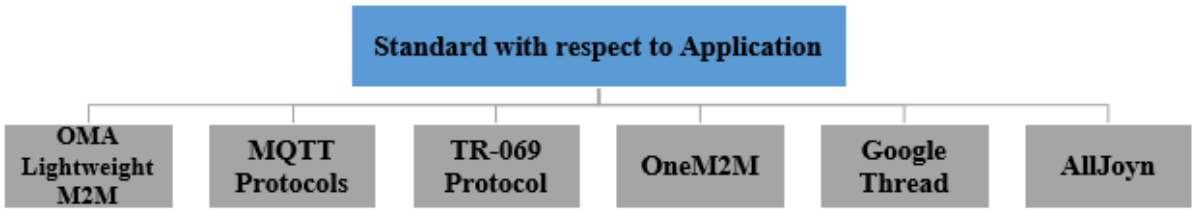


**Figure 3.** Types of Standards with respect to Application -M2M

### 4.2 Benefits

- Reduced expenses by minimizing downtime and equipment maintenance.
- Uncovered new business opportunities for servicing products in the field, which increase revenue.
- Enhanced customer service by monitoring and servicing equipment on an ongoing basis, either before it fails or only when it is required.

### 4.3 Requirement

- **Principles of M2M Application:** Communication M2M systems ought to make it possible to communicate with the M2M device or gateway by means of exchanging information or data through SMS or IP based connected services between the gadgets. The mechanism of transfer and reception of information is done in an efficient manner between the connected devices with the usage of network in IoT, whereas in M2M, network may not be used.
- **Scalability:** The identification and authentication of large number of connected gadgets in accordance with the regulatory bodies are monitored by the service provider. Whenever the requirement of identification of device is asked, M2M system may give a certain identification of the connected devices or gadgets.

- **Logging:** During the stagnant condition of network service, M2M systems with the help of IoT, can save all the important information while attempting the re-installation. Request for log should be accepted by the server connected to the devices.
- **Message Transmission Scheduling:** M2M systems should be aware of the tolerance for M2M application scheduling delay, able to schedule delivery of information and manage the accessible of network used while exchanging information between M2M.
- **Channel Selection:** The optimization of the usage of channel in M2M system depends on various factors such as cost effectiveness of network, propagation delay and false alarm.
- **Delivery Mechanism:** In order to reduce network load, the various broadcast mode has been used by M2M system. There is a flexibility in the mode of broadcast while exchanging information whenever it is required for a specific duration.

### 4.4 Important Features

- With the help of M2M, a low power consumption service is provided effectively to a provider of packet-switched service on the network with monitoring capabilities that enable event detection.
- Time tolerance allows for delays in data transfers.
- Control over time of transmission and reception of data.
- Triggers are specific to a specific location and notify the users.
- The capacity to exchange information in a regular basis between devices for a small amount of period.

The available IoT applications inclined to the features are discussed in Table 1.

**Table 1.** Application of IoT with the amalgam of M2M Communication

| S.No. | Area of Application | Remarks |
|---|---|---|
| 1 | Smart Grid | ● Through a variety of methods, energy can be used efficiently.<br>● These methods include tracking energy utilization, anticipating power breakage and efficient usage, and collecting information on how energy can be harvested in smart cities. |
| 2 | Retail IoT | Customer satisfaction with their usage of devices, e-monitoring the |

| | | |
|---|---|---|
| | | activities of staff and customer with an efficient management system. |
| 3 | Hospitality & Tourism | The IoT has enormous potential to improve tourism and hospitality operations. In the hospitality sector, staffing is a significant expense, but IoT can automate specific interactions to reduce staffing requirements. |
| 4 | Smart factories | • IoT technology is used by smart factories to collect data about mechanism of work and gadgets in order to make strategic plans and increase efficiency.<br>• To enhance analytics, sensors are connected to factory and machine tools. |
| 5 | Fitness Tracking System | • A person can track his/her progress and optimize fitness goals with IoT- connected devices.<br>• Daily activities such as, body posture while sleeping, heartbeat, patterns of activity, workout statistics, and calories burned, are all tracked by fitness trackers. |
| 6 | Smart Agriculture | • Intelligent IoT farming applications offer opportunities to revolutionize the farming industry by optimizing numerous time-consuming farm operations.<br>• The IoT can assist a farmer in determining the ideal time to harvest crops, creating fertilizer profiles based on soil chemistry, and detecting the concentrations of soil nutrients and moisture. |
| 7 | Health Industry | Connecting sensors to patients at home is made possible by IoT. Doctors can keep track of a patient's progress using these sensors and alerts. |
| 8 | Smart Home | The most popular IoT application on this list is smart homes. |
| 9 | Self-Automated Vehicles | In order to determine the level of engine oil, the temperature of the radiator water, etc. |

## 5. Relationship between M2M and IoT

The components of a Web of Things (WoT) system are considered. The architecture of an IoT or WoT system begins with IoT devices, which include a variety of sensors for data collection. M2M communication is the method by which this IoT device transmits data to other devices or a central system; in particular, the internet. That's why it's called the Internet

of Things. Data transmission is a component of both M2M and IoT. However, while M2M can use wired, wireless, or cellular communication, IoT typically relies on communication through a central server and uses wireless internet. Peer-to-Peer (P2P) communication, on the other hand, is just one option for the IoT, despite the fact that P2P communication is an essential component of the original definition of M2M. Between a smart device and an end-user device, many IoT systems require a server or a data analysis tool. Smart weather monitoring, for instance, relies on a vast network of hundreds of sensors. The information from all these sensors is gathered and analyzed by a centralized system, resulting in the weather forecast. Table 2 discusses the basic difference between M2M and IoT. The connection is where IoT and M2M really differ. The IoT usually refers to any device that uses the internet to perform better. In contrast, M2M typically consists of two or more internet-connected devices for data sharing and analytics.

**Table 2.** Difference between IoT and M2M Communication

| S.No. | Features | IoT | M2M Communication |
|---|---|---|---|
| **1** | Internet | Need to be connected to the internet | The internet connection is not necessary for devices |
| **2** | Data Sharing | Sharing data with other applications to make the user experience better | Sharing of data only between communicating parties |
| **3** | Technology | Software- and hardware-based | Hardware-based |
| **4** | Intelligence | Decision-making is the responsibility of objects | Observing intelligence to some degree |
| **5** | Protocols | Protocols for the Internet, like Telnet, FTP, and HTTP | Techniques of communication technology and conventional protocols |
| **6** | Communication | Automation for IoT sensors | Direct communication between machines |
| **7** | Connectivity | IP networks are how devices communicate | Simple communication between devices typically occurs within embedded software at the client site |

## 6. Security & Privacy Issues

- **Variability and Dynamism:** The main challenge for IoT is providing the privacy and security of information due to the diversified heterogeneous network. In the diversified network, any number of gadgets can join or leave at any time as per the usage of the users.
- **Digital and integrated operational world security**: Security measures have not been taken into account when designing control plans until now. However, internetwork connectivity necessitates security for the integration of the physical and digital worlds.
- **Device Security and Data Security:** Device security has been the subject of a great deal of research. Device security and data security should be implemented now. The IoT and M2M aim for object-to-object communication, which necessitates data security.
- **Information on the Data Source**: It is of the utmost importance to know where the data came from. Control, audit, management, and ultimately security of IoT and M2M communication all depend on having a solid understanding of the data source [27].
- **Confidentiality of the Data:** In IoT scenarios, data confidentiality is a crucial issue because it ensures that only authorized parties can access and modify data. This is especially true in the business world, where data may be an asset that needs to be protected to maintain market values and competitiveness. Data can be accessed by authorized objects and users in the IoT context. This necessitates dealing with two crucial aspects: "access control mechanism" and "object authentication process" (along with "identity management system").
- **Data Transmission:** The attacker is able to obtain user data, signaling data, or control data through physical theft or online listening in order to achieve the goal of unauthorized access because data transmission is prevented from reaching the end of service.

## 7. Conclusion

One of the most vulnerable components of the Internet of Things ecosystem is Machine-to-Machine (M2M) communication system. Any abnormalities in the behavior of the network are likely to go unnoticed because communication between connected machines typically occurs without much human oversight. In addition, compromised M2M may put physical infrastructure and safety at risk due to the influence of machines on the physical

world. Because it has affected virtually every area of communication, IoT and M2M account for the majority. Despite the existence of security protocols for IoT and M2M communication, new cyberattacks emerge every day. The above discussed issues are the challenges faced by IoT inclined with M2M Communication. In addition, the M2M standard, one of the most well-known standard initiatives for making M2M networks safer and to run more smoothly has been briefed, as well as the IoTs has been elaborated.

## References

[1] Zeinab, Kamal Aldein Mohammed, and Sayed Ali Ahmed Elmustafa. "Internet of things applications, challenges and related future technologies." World Scientific News 67, no. 2 (2017): 126-148.

[2] Yugha, R., and S. Chithra. "A survey on technologies and security protocols: Reference for future generation IoT." Journal of Network and Computer Applications 169 (2020): 102763.

[3] Parne, Balu L., Shubham Gupta, and Narendra S. Chaudhari. "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network." IEEE Access 6 (2018): 3668-3684.

[4] Chen, Hsing-Chung, Ilsun You, Chien-Erh Weng, Chia-Hsin Cheng, and Yung-Fa Huang. "A security gateway application for End-to-End M2M communications." Computer Standards & Interfaces 44 (2016): 85-93.

[5] Pradhan, Devasis, Hla Myo Tun, and Ajit Kumar Dash. "IoT: Security & Challenges of 5G Network in Smart Cities." Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146 8, no. 2 (2022): 45-50.

[6] Mohanty, Jayashree, Sushree Mishra, Sibani Patra, Bibudhendu Pati, and Chhabi Rani Panigrahi. "IoT security, challenges, and solutions: a review." Progress in Advanced Computing and Intelligent Engineering (2021): 493-504.

[7] Varga, Pal, Sandor Plosz, Gabor Soos, and Csaba Hegedus. "Security threats and issues in automation IoT." In 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), pp. 1-6. IEEE, 2017.

[8] Weber, Mario, and Marija Boban. "Security challenges of the internet of things." In 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 638-643. IEEE, 2016.

[9] Castilho, Sergio D., Eduardo P. Godoy, and Fadir Salmen. "Implementing security and trust in iot/m2m using middleware." In 2020 International Conference on Information Networking (ICOIN), pp. 726-731. Ieee, 2020.

[10] Imani, Amirhosein, Alireza Keshavarz-Haddad, Mohsen Eslami, and Javad Haghighat. "Security challenges and attacks in m2m communications." In 2018 9th International Symposium on Telecommunications (IST), pp. 264-269. IEEE, 2018.

[11] Hameed, Sufian, Faraz Idris Khan, and Bilal Hameed. "Understanding security requirements and challenges in Internet of Things (IoT): A review." Journal of Computer Networks and Communications 2019 (2019).

[12] Shabandri, Bilal, and Piyush Maheshwari. "Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle." In 2019 6th International conference on signal processing and integrated networks (SPIN), pp. 1069-1075. IEEE, 2019.

[13] Pradhan, Devasis, Hla Myo Tun, Naw Khu Say Wah, Thandar Oo, K. C. Priyanka, and Ajit Dash. "Efficient Usage of Energy in 5G toward Sustainable Development inclined to Industry 4.0 Connectivity." In 2022 IEEE Region 10 Symposium (TENSYMP), pp. 1-6. IEEE, 2022.

[14] Pramanik, Sabyasachi. "An Effective Secured Privacy-Protecting Data Aggregation Method in IoT." In Achieving Full Realization and Mitigating the Challenges of the Internet of Things, pp. 186-217. IGI Global, 2022.

[15] Pradhan, Devasis, Prasanna Kumar Sahu, Mangesh M. Ghonge, and Hla Myo Tun. "Security Approaches to SDN-Based Ad hoc Wireless Network Toward 5G Communication." In Software Defined Networking for Ad Hoc Networks, pp. 141-156. Springer, Cham, 2022.

[16] Pradhan, Devasis, Prasanna Kumar Sahu, A. Dash, and Hla Myo Tun. "Sustainability of 5G green network toward D2D communication with RF-energy techniques." In 2021 International Conference on Intelligent Technologies (CONIT), pp. 1-10. IEEE, 2021.

[17] Pradhan, Devasis, and K. C. Priyanka. "A comprehensive study of renewable energy management for 5G green communications: Energy saving techniques and its optimization." Journal of Seybold Report ISSN NO 1533 (2020): 9211.

[18] Dash, A., Devasis Pradhan, Hla Myo Tun, and Zaw Min Naing. "M-MTC for Optimized Communication in 5G." Journal of Network Security Computer Networks 8, no. 3 (September 28, 2022): 1–8. https://doi.org/10.46610/jonscn.2022.v08i03.001.

[19] Devasis Pradhan et al.;Critical Security & Privacy Issue in Blockchain Technology Intended to Industry 4.0. Middle East Res J. Eng. Technol, 2022 Jan-Feb 2(1): 1-7.

[20] Devasis Pradhan et al.; Green WPC: Energy Harvesting in Smart Cities‖. Middle East Res J. Eng. Technol, 2022 Jan-Feb 2(1): 8-12

## Author's biography

**Devasis Pradhan** is currently working as an Assistant Professor / Research Coordinator in the Department of Electronics & Communication Engineering at Acharya Institute of Technology, Bengaluru, Karnataka since 2017. His current research includes the effectiveness of 5G-Green Communications, mmWave antenna design, UWB antennas, and its implementation. He has published 50 research papers in eminent international journals & conferences, 4 books and 3 edited books with a reputed publishing house. He is a co-editor in Editorial Board & peer-reviewed 8 international journals and a committee member in a reputed organization. He has authored and co-authored 10 book chapters. He has been a technical committee member and reviewer for a reputed internal conference such as IEEE, Grenz Society, IFERP, etc. He has received 6 national awards in the field of academic and research work from various governing bodies associated with the government of India. He is also an active member of ISTE, IEEE, ATMS, and other professional associations toward professional growth.

**Hla Myo Tun** currently works at the Department of Electronic Engineering, Yangon Technological University. Hla does research in Communication Engineering, Control Systems Engineering and Electronic Engineering. His current project is Biomedical Signal Processing and Semiconductor Electronics Measurement System. He is an active senior member of IEEE as well as other professional bodies. He has published more than 100 research papers in eminent international journals & conferences, 4 books and 3 edited books with a reputed publishing house. He is co-editor in Editorial Board & peer-reviewed more than 10 international journals and a committee member in a reputed organization.