# A Mobile and Web-Based Security Guard Patrolling, Monitoring and Reporting System to Maintain Safe and Secure Environment at Premises

https://doi.org/10.3991/ijim.v17i11.35483

Vigneswara Rao Gannapathy[1](✉), Vigneswaran Narayanamurthy[1,2], Siva Kumar Subramaniam[3,4], Ahamed Fayeez Bin Tuani Ibrahim[3], Ida Syafiza Md Isa[1], Sujatha Rajkumar[5]

[1] Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

[2] Department of Biotechnology, Saveetha Institute of Medical and Technical Sciences, Chennai, India

[3] Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

[4] Technical and Project Manager, IIOTSME Sdn. Bhd., Melaka, Malaysia

[5] Department of Embedded Technology, Vellore Institute of Technology, Vellore, India

vigneswara@utem.edu.my

**Abstract—**The guard tour system helps companies and organizations to monitor their security activities such as protecting people, buildings, assets, or equipment. According to the existing system, the patrolling at each checkpoint is being executed by using RFID-based digital data loggers that records and save all patrolling entries internally. The data will be transferred manually by the guard once the patrolling is completed. In some cases, when there is a problem with the device, the system unable to retrieve the patrolling data that has been already stored in the device. In addition, the current system also not be able to track the guard's movement, patrolling information, and incidents in real-time basis. The main aim of this work is to develop a Security Guard Patrolling, Monitoring and Reporting (eSmartGuard) system that able incorporates many unique and intelligent technologies such as NFC, GPS and IoT to records and save the patrolling data automatically on the cloud/server in real-time basis. An important value-added feature of the system is real-time incidents notification that able to notify any risk of the guards instantly to the security officers. Furthermore, through the eSmartGuard, the patrolling information such as date, time, GPS coordinate, guard ID can be monitored and retrieved remotely via proposed Mobile Apps and Web at a convenient time. The eSmartGuard patrolling system is proposed to improve the safety of the people and assets by assisting the security guards to perform their patrolling duty efficiently.

**Keywords—**guard patrolling, Global Positioning System (GPS), Internet-of-Things (IoT), Near Field Communication (NFC), smartphones

# 1 Introduction

A guard patrolling system is used in universities, companies, or any organization to improve the safety level of the people and assets by assisting the security personnel to patrol and performs their duty efficiently. The patrolling tags will be installed at multiple points along the patrolling routes with unique Identification (ID) which identify different locations/points or routes. The guards will patrol according to their planned routes and records their arrival by scanning the tags with the reader device. The guard patrolling system helps the organization to provide excellent and efficient implementation of standard operating procedure (SOP) and improve the security of the assets and premises.

A Watchclock is one of the oldest guard tour systems, but it is a mechanical clock still used by some of the security guard all over the world. It is using mechanical algorithms that required a several key and a paper tape. The keys are the same as the one commonly used by peoples to rotate the lock. But for watchclock, the keys will be inserted into the box and rotate, now the key is rotated, checkpoints and current time will be numerically stamped on the paper tape. The keys will be placed at several checkpoints or locations. The security guards need to go from one checkpoint to another to stamp the date and checkpoints number onto the paper during their patrolling session. The authorized administrator can only check the status of patrol after the security guard completed all the checkpoints. Therefore, this antique system does not provide real time arrival checking and has no ability to generate patrolling reports based on weekly, monthly, or yearly. Besides that, the watchman's clock is bulky to carry around and paper tape inside the box needs to be changed regularly after the patrolling is done. Thus, this is involving high maintenance fee.

Hicham El Mrabet [2] has presented advance monitoring and reporting system using connected objects and RFID technology. Digital based RFID data loggers are the most used technologies by the security guard now. Even though it has same functionality with the watchman's clock, but it uses electronic rather than mechanical components. Since it is using electronic component, the patrolling records will be in the term of digital form. Therefore, the size of the data is smaller compared to Watchclock's paper tape. An electronic wand that security guards always carry during patrol called RFID readers. The physical size of the RFID reader depending on the manufacturer, but usually a small device with the size of a stick or pen. The 'RFID chips' are passive tags that are placed in locations that security guards must go through. When security guards scan the chip, the wave will be reflected to the RFID reader, therefore the chip will be activated, and the data will be sent to the reader during reflection.

During patrols, security guards will stop at each checkpoint and scan with RFID reader. The location of the checkpoints and the current time will be recorded in the RFID reader. Once rounds completed, the patrolling data will be downloaded manually into a computer via USB. The data need to be downloaded before the sensor threshold is exceeded, otherwise the data may lose. Since records are saved internally on the device, therefore the security officer is not able to monitor patrolling activities in real-time basis. One of the main drawbacks of digital based data logger system is the cost to replace or repair the machine is expensive when it damaged. In addition to

that, the digital data logger needs to be charged regularly and changed when battery's health is significantly degraded. This eventually leads to higher maintenance cost to maintain this device. Besides, it also does not provide a real-time reporting system to monitor guard's activity instantaneously. All the records in the digital data logger will be lost permanently and unable to retrieve if the device is stop functioning. Lastly, all reports from the system need to be downloaded manually via USB connection by the guard security officers or administrator which might not be practical to obtain the reports instantly or remotely.

## 2 Background study

A guard patrolling system is used to ensure the safety and security of premises such as university. In general, security guards assigned to visit pre-determined checkpoints at regular intervals and perform safety checks. Karakaya [3] has proposed a wireless control system based on smart Bluetooth and IBeacon technology for auditing the patrols. He proposed the used of smartphone with IBeacon in their security systems and developed a Web-Based application to generate and retrieve the patrolling reports that have been scanned by the guards. If patrol is completed, all data patrolling will be saved in the database. However, the scope of this patrol is a lengthy process depending on the size of the area. The larger the area, the more checkpoints need to be scanned, and more risk involves to the guards while they perform their patrolling.

Faizul [4] has proposed GuardExpert PRO: Application-centric IoT solution for Guard Touring System (GTS). The GTS is developed to records and manages guard patrolling tasks and activities in an efficient way. The system is also used to ensure that the guards complete their daily patrols without missed. The author used IoT technology in their guard touring system to connect to internet through cellular network. The data collected by the NFC reader will subsequently be transferred to a cloud server through the internet, where the administrator is able to retrieve them at their convenient time. However, the GuardExpert PRO only focused on improving their patrolling management system while the safety of guards while on patrol was neglected.

Mobile devices that are incorporated with GPS and NFC have been used widely in most of the works related to security and management system. Asadullah Shaikh [5] has presented some of mobile app-based applications that incorporate with GPS in his work. Alexopoulou [6] has also presented the approach towards cognitive flexibility and the ways it is affected by mobile and advanced information and communication technologies. Keau [7] has proposed a Smart-Hadir system to record student attendance digitally during a class session. He has developed a system that able scan the available beacons that incorporated using NFC or QR code. Through the system, the student's attendance will be immediately captured and saved in database.

Saare [8] has provided a systematic review on the usability evaluation of mobile tracking applications namely information tracking, location tracking, information, and location tracking. He concluded that effectiveness, efficiency, usefulness, and accura-

cy are the most important characteristics of the usability of mobile tracking application. In addition to that, Ching [9] in his work has discussed on the acceptability and usability of an android-based measurement mobile-app.

Ali [10] had presented a comprehensive literature review on the use of IoT, big data analytics and mobile application in facility management processes. In his work, he concluded the incorporation between IoT, big data analytics and mobile application significantly reducing management costs and improving facilities performance and service quality. Similar work reported by Fan [11] by incorporating hybrid wearable sensor network system with IoT for safety and health monitoring applications.

Several recent studies [12, 13, 14, 15] has suggested some NFC-enabled systems such as Incentive Lynx Security, inViu NFC-tracker, and NFC Patrol to improve security patrolling and management. Basically, the checkpoints will be mounted with NFC tags in a building. Once the NFC tags were scanned with NFC-enabled device, the tags UID will be sent to server over the Internet instantly. By using this system, a security guard can prove their presence at the checkpoint to their security officers in real time basis. Some of the system such as Incentive Lynx Security uses the Global Positioning System (GPS) in the phone to detect the position of the security guards.

The use of NFC technology is still relatively low. NFC is a short-range advanced wireless technology that makes consumers' life more convenient and easier. Most of NFCs just require a read-only device to operate Singh [14] has given an exposure of NFC technology to security attacks. According to his study, the NFC provides numerous benefits as it can be used for data transfer, connecting to other devices, performing cashless payments, and making simple transfers with only one touch. However, without preceding technologies like RFID, advancements in NFC technology would not have been possible [15]. Noor Cholis Basjaruddin [16] has described the use of NFC technology that enables mobile phones to store important data safely and reliably in his work. He has proposed a special application to allow NFC off-line data transfer between mobile phones and modify the NFC data by using special authentication system.

Devices that fulfil the ISO/IEC18092 and ISO/IEC14443 standards are also required to utilize NFC technology as stated in [15]. NFC is divided into three categories which is Peer-to-Peer mode, Card Emulation mode, and Reader/Writer mode [15].

Peer-to-peer mode as shown in Figure 1, allows users to connect with other devices to exchange data, social networking, and transfer money [15].

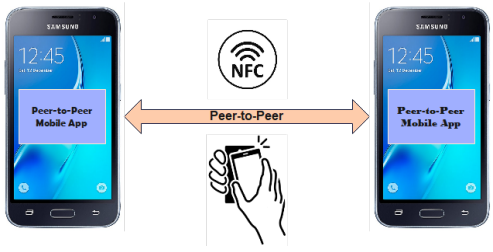


**Fig. 1.** Peer-to-Peer Mode NFC Connectivity

Card emulator mode as shown in Figure 2, allows devices to create contactless smart cards. This mode is used by loyalty cards, identity or access cards, credit cards, and debit cards.

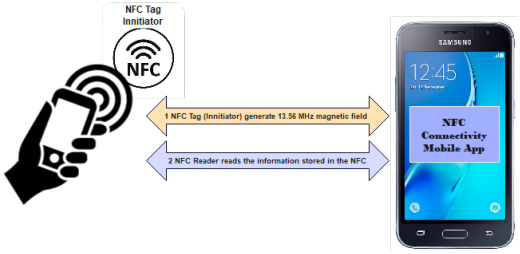


**Fig. 2.** Card Emulator Mode

Reader/Writer mode as shown in Figure 3, able to read data or information from and to NFC tag. Mostly this mode is used for social networking and location-based services as stated in [15]. Where the NFC tag has been program for a specific point and after it scanned, it will be read and store the information to the database.

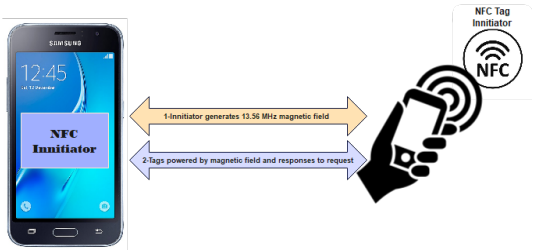


**Fig. 3.** Reader/Writer mode

## 3 eSmartGuard system design

Figure 4 and 5 depicted the system architecture and flowchart of eSmartGuard system respectively. Based on system architecture diagram shown in Figure 4, the eSmartGuard consists of guard mobile app, superior mobile app and the admin room which is known as eSmartGuard web dashboard app. Both mobile and web apps will be connected to cloud server (remote storage) via WiFi or cellular networks. The number of NFC tags also will be installed around the premises (known as checkpoints) to assist patrolling process.

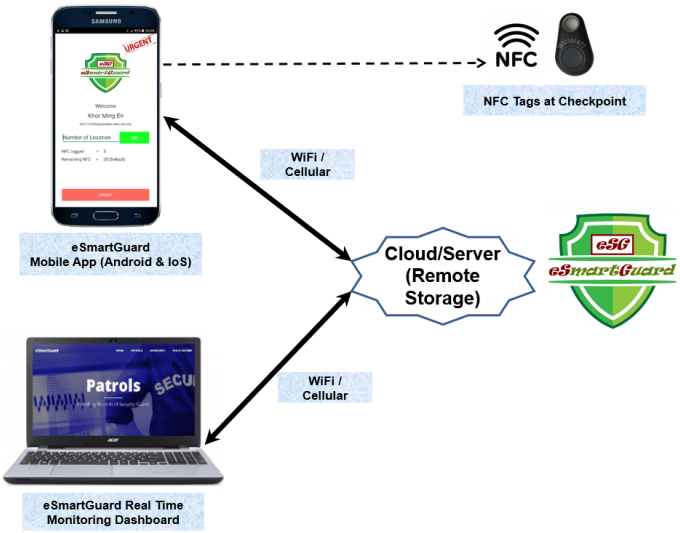


**Fig. 4.** eSmartGuard System Architecture

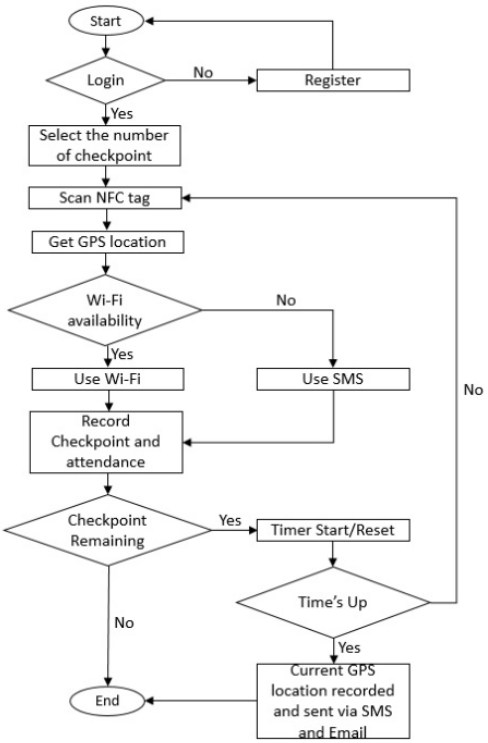


**Fig. 5.** eSmartGuard System Flowchart

At the beginning of the eSmartGuard process, the security guards will be directed to the login page. This interface is developed to obtain username and e-mail before allowing guards to enter the main App interface. These credentials are required to ensure the safety and prevent any possible hacking to the system. Based on this authentication, only the pre-registered guards can login and access to eSmartGuard system application. New users are required to register and sign up with authorized superior at the main control center by using eSmartGuard web dashboard system.

The guards are required to switch on GPS and NFC features before the proceed to login page. If the guard access the interface without these features enabled, a reminder message will be popped by the system to remind the user. Next, the main interface of the system will prompt the user to enter the number of checkpoints that requires to be patrolled. If the user chooses not to enter the number of checkpoints before start patrolling, then the application will automatically choose it based on previous entries. However, the user still can choose to enter the number of locations or checkpoints that need to be patrolled based on the instruction received from patrolling manager.

The NFC tags will be installed at multiple checkpoints at any premises. The guard will carry NFC reader (NFC enabled smartphone) to patrol according to their planned routes and records their arrival by scanning the NFC tagged at checkpoints. Security guards can access a detail list of existing as well as upcoming checkpoints at the premises. This information is processed in real-time and helps to keep a check on all the checkpoints of the premises. Once the NFC tag is scanned, patrolling information such as checkpoint names, coordinate, scan timings and guard ID will be sent automatically to the cloud server via cellular or WiFi network. If the checkpoint doesn't have any internet connection or connection lost, the application will switch to cellular network and send the data by using SMS service. Received SMS containing user information will be recorded before duplicating them into the cloud database.

When guard start scanning the first NFC tags, the timer will be activated. The layout will display the time left on the bottom part of the interface. The countdown timer will be set by the administrator cannot be modified by the guards or client. After the timer starts, the guard must scan the next NFC tag within predefine time. The countdown timer will be reset for each successful scan until the guard passes all the checkpoints. If the countdown timer is expired before the guard reaches next checkpoint, the application will detect the guard's current location via GPS and send this information to cloud database for emergency recording purpose. In addition, the application will send an alert message directly to the superior via WhatsApp, SMS and e-mail. After the guard scanned all the checkpoints, the application will end the patrolling process and a "Successfully Done!" message will be appeared on the screen to indicate that the guard has successfully patrolled all the given checkpoints. All scanned information can be monitored and retrieved remotely by using eSmartGuard web monitoring dashboard. The eSmartGuard patrolling reports can be downloaded in customize format (i.e., hourly, daily, weekly, monthly or yearly) as per needed. Therefore, the developed eSmartGuard also offers dedicated assistance to report any untoward incident immediately.

The eSmartGuard system also helps to report any risk and incidents that the guards encounter during patrolling automatically. This is to ensure the safety of guards while

they are patrolling at any premises. This information is processed in real-time basis and helps to keep a check on all the checkpoints during patrolling.

## 4 Conclusion

The eSmartGuard system records the patrol activities of guards according to the patrol plan and ensure the guards accomplish their tasks at specified point and within the predefined time interval. The guards will patrol according to their planned routes and records their arrival by scanning the NFC tagged checkpoints with smartphone. The system is connected wirelessly to its cloud database on the internet. The database of the system has been successfully completed as it is able to receive the information sent by the mobile application through internet or SMS. Besides, the superior can monitor the progress of their planned guard tour by retrieving the information from the database remotely via their personal computer or smartphones. The system also designed to automatically notify any incidents during the patrolling via WhatsApp, SMS and email to authorized personnel. This can be done by pressing the emergency call manually or automatic time-out by eSmartGuard patrolling system. This system can help the organization to provide excellent and efficient implementation of Standard Operating Procedure (SOP) and improve the security of the assets and premises.

## 5 Acknowledgment

The authors would like to thank the Centre for Research and Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM) which has provided funds through the Short-Term Grant Scheme (PJP/2022/FTKEE/S01884).

## 6 References

[1] R. Chuymurkar, V. Bhagdi, "Smart Surveillance Security and Monitoring System Using Raspberry PI and PIR Sensor", International Journal of Scientific Engineering and Applied Science (IJSEAC), vol.2, issue 1, January 2016.

[2] H. El Mrabet and A. Ait Moussa, "IoT-School Attendance System Using RFID Technology", International Journal of Interactive Mobile Technologies (iJIM), vol. 14, no. 14, pp. pp. 95–108, Aug. 2020. https://doi.org/10.3991/ijim.v14i14.14625

[3] M. Karakaya, G. Şengül, and A. Bostan, "A Wireless Control System Based on Smart Bluetooth and I-Beacon Technology for Auditing the Patrols," International Journal of Scientific Research in Information Systems and Engineering, vol. 2, no. 3, 2016, [Online]. Available: http://www.ijsrise.compg.8

[4] H. Faizul and R. A. Rashid, "GuardExpert PRO: Application-Centric IoT solution for Guard Touring System," Journal of Electrical Engineering, vol. 16, no. 2, pp. 39–43, 2017, [Online]. Available: www.fke.utm.my/elektrika

[5] A. Shaikh, "Advances in Deep Learning in Mobile Interactive Algorithms and Learning Technologies", International Journal of Interactive Mobile Technologies (iJIM), vol. 14, no. 10, pp. pp. 4–6, Jun. 2020. https://doi.org/10.3991/ijim.v14i10.15369

[6] A. Alexopoulou, A. Batsou, and A. Drigas, "Mobiles and Cognition: The Associations Between Mobile Technology and Cognitive Flexibility", International Journal of Interactive Mobile Technologies (iJIM), vol. 14, no. 03, pp. pp. 146–156, Feb. 2020. https://doi.org/10.3991/ijim.v14i03.11233

[7] C. Seng Keau, C. Kim On, M. H. Ahmad Hijazi, and M. Mahinderjit Singh, "Smart-Hadir – Mobile Based Attendance Management System", International Journal of Interactive Mobile Technologies (iJIM)., vol. 15, no. 14, pp. pp. 4–16, Jul. 2021. https://doi.org/10.3991/ijim.v15i14.22677

[8] M. Ali Saare, A. B. Hussain, O. M. Jasim, and A. A. Mahdi, "Usability Evaluation of Mobile Tracking Applications: A Systematic Review", International Journal of Interactive Mobile Technologies (iJIM)., vol. 14, no. 05, pp. pp. 119–128, Apr. 2020. https://doi.org/10.3991/ijim.v14i05.13353

[9] E. Tsen Yi Ching, C. Kim on, R. Alfred, M. H. Ahmad Hijazi, and T. Tse Guan, "An Android Mobile-based Measurement Application – Object and Interior Room Measurement App", International Journal of Interactive Mobile Technologies (iJIM)., vol. 14, no. 20, pp. pp. 135–152, Dec. 2020. https://doi.org/10.3991/ijim.v14i20.15415

[10] I. M. Ali, M. N. Mohd Nawi, M. Y. Hamid, F. I. A Jalil, and B. Hussain, "Integration of IoT, Data Analytics and Mobile Application towards Digitisation Facilities Management: A Case Study", International Journal of Interactive Mobile Technologies (iJIM)., vol. 15, no. 22, pp. pp. 154–164, Nov. 2021. https://doi.org/10.3991/ijim.v15i22.24115

[11] W. Fan, W. Taiyang, & R. Y. Mehmet, "An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications", Sensors Journal, vol.9, issue 1, pp. 1-21, 2018. https://doi.org/10.3390/s19010021

[12] H. Jiang, "Application and Research of Intelligent Security System Based on NFC and Cloud Computing Technology," 20th International Symposium on Distributed Computing and Applications for Business Engineering and Science, DCABES 2021, 2021, pp. 200–202. https://doi.org/10.1109/DCABES52998.2021.00057

[13] K. Mansur, Z. B. Hasanuddin, and M. Wardi, "Implementation of NFC for Smart Gate Access Control in Campus Area," presented at International Conference on Science and Technology, published by Atlantis Press, Ancol, 2018. https://doi.org/10.2991/icosat-17.2018.37

[14] M. M. Singh, K. Aina, A. Ku Adzman, and R. Hassan, "Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures", International Journal of Engineering and Technology, 2018. [Online]. Available: www.sciencepubco.com/index.php/IJET

[15] V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication (NFC) technology," Wireless Personal Communications, published by Springer Nature, vol. 71, no. 3. pp. 2259–2294, Aug. 2013. https://doi.org/10.1007/s11277-012-0935-5

[16] N. C. Basjaruddin, E. Rakhman, K. Kuspriyanto, and M. B. Renardi, "NFC Based Electronic Medical Record", International Journal of Interactive Mobile Technologies (iJIM), vol. 13, no. 03, pp. pp. 4–12, Mar. 2019. https://doi.org/10.3991/ijim.v13i03.8047

## 7 Authors

**Vigneswara Rao Gannapathy** C.Eng., MIET currently serving as a Senior Lecturer at Department of Electronics and Computer Engineering Technology, Faculty of Electrical and Electronic Engineering Technology (FTKEE), Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. In 2002, he received his certificate in Electron-

ics Engineering (Telecommunication) from Politeknik Shah Alam. Vignes pursued BEng in Electronics Engineering (Telecommunication) from Universiti Teknikal Malaysia Melaka (UTeM), Malaysia in 2007 and he then pursued and graduated a MSc in Electronics Engineering from the same institution in the year of 2011. He has 13 years' experience in research, teaching and consultancy in the field of Electronics and Wireless Networking. His research direction has focused on 5G technology which emerged as a key technology for next-generation Mobile Communication. He is an active Member of various technical societies such as IET (UK), BEM (Malaysia) and IEEE. Vigneswara Rao has headed more than 10 projects on research and development, written several research papers and won innovation awards in national and international innovation competitions (email: vigneswara@utem.edu.my).

**Dr. Vigneswaran Narayanamurthy** C.Eng., MIE., is a Senior Lecturer at Department of Electronics and Computer Engineering Technology, Faculty of Electrical and Electronic Engineering Technology, Universiti Teknikal Malaysia Melaka, Malaysia. Has more than 9 years of experience in research, teaching, and consultancy in the field of Electronics and Biomedical Engineering. He has published 40 indexed international journals and hold two patents. He is a Life Member of various technical societies such as IET (UK), IEI (India), IEEE, IAEng. Products developed through his past research includes passive lab on chip applications, expert systems, and agriculture technologies. His research interests include MEMS/NEMS, biosensors, medical devices, precision farming, biomedical engineering, signal and image processing, single cell analysis, lab on chip and soft lithography (email: vigneswaran@utem.edu.my).

**Eur. Ing. Dr. Siva Kumar Subramaniam** has been a Senior Lecturer at Universiti Teknologi Malaysia Melaka since 2012. He also co-founded a spin-off company from UTeM, IIOTSME Sdn. Bhd in 2021, a private limited company that drives customised IoT-based engineering innovation and solutions, where he is appointed as the Technical and Project Manager. Siva earned a B.Eng in Electronics Engineering (Industrial Electronics) from Kolej Universiti Teknikal Kebangsaan Malaysia in 2006 and a M.Sc in Electronics Engineering from the same institution, which is now known as Universiti Teknikal Malaysia Melaka (UTeM), in 2009. In 2017, he received his Ph.D. in Electrical Engineering and Electronic Research from Brunel University London, United Kingdom. Dr Siva has spearheaded more than ten projects involving research and development of innovative products, written more than 70 technical papers, more than 15 innovative products and 25 intellectual property rights. His research interests include wireless sensor networks, particularly on IEEE 802.11 and IEEE 802.15.4 standards. He specialises in wireless sensor networks, IoT systems, system integration, and consumer electronics system and has a successful track record of industrial collaboration in the last 15 years (email: siva@utem.edu.my / siva@iiotsme.com.my).

**Dr. Ahamed Fayeez Tuani** is a senior lecturer at Electronics & Computer Engineering Faculty, Technical University of Malaysia Melaka (UTeM). He received a Diploma in Electronics Eng from in 2005 followed by a bachelor's degree in Electronics Eng (Computer Eng) in 2008 from the same university. Having worked as software test engineer upon graduation, he joined UTeM as a tutor in 2009 before

graduating in M.Eng (Electronics & Telecommunication) from Universiti Teknologi Malaysia (UTM) in 2012 and continued to serve UTeM until 2015. He then pursued and graduated with a Ph.D. in Computer Science from University of Exeter, UK in the field of Swarm Intelligence specifically Ant Colony Optimization (ACO). His research interest includes but not limited to: ACO, Swarm Intelligence, Bio-inspired optimization, wireless sensor network, internet of things (IoT) to name a few. He has authored several research papers and also won research awards for his outstanding research in the field mentioned above (email: fayeez@utem.edu.my).

**Dr. Ida Syafiza Binti Md Isa** has received the Ph.D. degree from the University of Leeds, U.K., in 2020, worked on energy efficient access networks design for healthcare applications. She is currently a Senior Lecturer with Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. She has published several articles in this area. Her research interests include network architecture design, energy efficiency, network optimization, mixed integer linear programming, and patient healthcare systems (email: idasyafiza@utem.edu.my).

**Dr. Sujatha Rajkumar** is a Senior Associate Professor in the Department of Embedded Technology, School of Electronics Engineering, Vellore Institute of Technology, India. Received her Ph.D. in the field of information security. Having 23 years of teaching and research experience in reputed Institutions. Her research interests include Industrial Internet of Things, Data Engineering in cloud and Information security in cloud platform. Received speaker award at the UK Cloud Asia Summit-2019, Cambridge University, UK. Published research articles in peer-reviewed national, international journals and conferences. Received DST SERB grant for IoT-LoRa enabled detection and prediction of pollutants in ground water in an open dumping yard. Received Seed Grant for LoRa enabled water pipeline monitoring and green house management. Dr. Sujatha is an AWS certified cloud computing practitioner and trainer. She has completed a consultancy project in "Audio Captioning" for Samsung Bangalore, India with a Certificate of Excellence and "Industry automation through cloud-based environmental factor monitoring" for Transcend Solar Systems, India. Dr. Sujatha is the In-charge and active member of "Intelligent Industrial IoT and computing lab" at the School of Electronics Engineering, Vellore Institute of Technology, India (email: sujatha.r@vit.ac.in).

Article submitted 2022-09-21. Resubmitted 2023-01-26. Final acceptance 2023-01-30. Final version published as submitted by the authors.