Investigations in Security Challenges and Solutions for M2M Communications—A Review

Manikandan A.[1,*], Gayathri Narayanan[1], K. S. Reddy Banu Prakash[1], Yugandhar Reddy C.[1], Mahesh A. D.[1], Vavilala Sushanth[1], and Ramprasad O. G.[2]

[1] Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, Kerala, India

[2] Solutions Architect, Cloudera Inc. 513 Conservatory Ln Aurora Illinois, USA

Email: mani_ac18@yahoo.co.in (M.A.), gayathrin@am.amrita.edu (G.N.), amenu4ece20028@am.students.amrita.edu (K.S.R.B.P.), amenu4ece20017@am.students.amrita.edu (Y.R.C.), amenu4ece20035@am.students.amrita.edu (M.A.D.), amenu4ece20053@am.students.amrita.edu (V.S.), ohnusaavyus@gmail.com (R.O.G.)

***Abstract*—The Internet of Things (IoT) is becoming increasingly popular, and machine-to-machine (M2M) technology is one of its major components. Reducing human interaction and tasks is one of the most important justifications for research in M2M communication. Also, M2M technology decreases network traffic, improving network effectiveness. In contrast, multiple networks are combined into M2M networks, which leads to security-related design concerns. However, a significant barrier to its growth is security. According to statistics, new gadgets may come under attack five minutes after they connect to the Internet. If these issues are resolved, it will be easier for people to trust this worldview. Security issues with possible solutions have gotten little attention despite extensive M2M studies. This article provides a comprehensive security analysis of M2M communication technologies, exploring the risks and solutions to better comprehend M2M communication and its security implications.**

***Index Terms*—M2M communication, security attacks, solutions**

I. Introduction

The direct communication between two or more systems or devices using communication channel, which includes wired or wireless without human interaction is machine-to-machine (M2M) communication. It involves the capacity for machines or devices to exchange information with one another and collaborate, coordinate, and carry out tasks independently. According to industry predictions by Ericsson [1, 2] there are already five billion M2M devices connected to wireless networks, and within ten years, this number will rise to fifty billion. This includes a wide array of devices, ranging from high-end smartphones to resource-efficient wireless sensors. These gadgets can interface with the server to keep track of various events and manage certain server operations. Observed events are transmitted through wired or wireless channels to a server or wherever they occur [3]. M2M offers a new method for connecting devices and exchanging data, enabling remote monitoring and control for diverse M2M applications, thereby ensuring efficient and automated functionality.

Security is a critical obstacle that could stymie the growth and broad adoption of machine-to-machine (M2M) technologies. M2M networks are subject to a variety of threats, including network assaults as well as hardware and software attacks, due to the nature of M2M settings and the sensitivity of the data shared. M2M devices are also more common than personal communication devices, raising concerns about the potential collection of personal information. Inadequate security measures may result in concerns about confidentiality and privacy. While many studies on M2M security systems and architectures have been published, these frequently focus on specific M2M use cases without addressing the overall security issue. In this work, we seek to present a comprehensive assessment of M2M security, considering the problems that must be solved to ensure the security of M2M communications and protect against various attacks. The extent of our survey is summarized in Table I. Our survey not only analyses the challenges and issues in security areas, but it also looks into viable solutions. We analyse existing solutions, define the security services they provide, and compare them based on a variety of criteria, including scalability and applicability, while keeping resource constraints in mind.

The papers described in Table I provides a comprehensive overview of the state-of-the-art in M2M and Internet of Things (IoT) research and development. They cover a wide range of topics, including M2M communication architectures and protocols, IoT applications in smart cities, transportation, healthcare, and other industries. Security and privacy are major challenges in M2M and IoT systems. M2M and IoT systems are often vulnerable to cyberattacks, which could have serious consequences for individuals and businesses. The authors highlighted few opportunities and challenges. M2M and IoT technologies have the potential to transform many aspects of our lives. For example, M2M and IoT-enabled smart cities can improve traffic management, reduce energy consumption, and enhance

Manuscript received August 23, 2023; revised November 2, 2023; accepted November 10, 2023; published January 2, 2024.

*Corresponding author

public safety. In healthcare, M2M and IoT devices can be used to monitor patients remotely and to provide personalized care. And in agriculture, M2M and IoT technologies can be used to improve crop yields and reduce environmental impact. However, there are also some challenges that need to be addressed before M2M and IoT can reach their full potential. One key challenge is security. M2M and IoT systems are often vulnerable to cyberattacks, which could have serious consequences for individuals and businesses. As the number of M2M and IoT devices continues to grow, it will be important to develop new technologies and architectures that can support this growth. In addition, there is a need to integrate M2M and IoT systems with existing systems in order to be widely adopted. This will require the development of new standards and interfaces. Also, M2M and IoT systems need to be easy to use and manage. This will require the development of new user interfaces and tools. Finally, it is important to consider the ethical implications of M2M and IoT technologies. For example, we need to ensure that M2M and IoT systems are used in a way that respects privacy and security.

TABLE I: COMPARISON OF RELATED SURVEY PAPERS.

Reference	Vulnerabilities	Security Issues	Passive Attacks	Active Attacks	M2M Security Solutions
[4], 2011	✔	✔	x	x	✔
[5], 2015	x	✔	x	x	x
[6], 2015	x	✔	x	x	x
[7], 2016	x	x	x	x	x
[8], 2018	x	✔	x	x	x
[9], 2006	✔	✔	✔	✔	✔
[10], 2021	x	✔	x	x	✔
[11], 2012	x	✔	x	x	✔
[12], 2016	✔	✔	x	x	x
[13], 2016	✔	✔	x	✔	✔
[14], 2019	x	✔	✔	x	✔
[15], 2021	x	✔	✔	x	✔
[16], 2020	✔	✔	x	x	x
[17], 2020	x	✔	✔	✔	✔
[18], 2016	✔	✔	x	x	✔
[19], 2021	x	✔	x	x	x
[20], 2019	x	✔	✔	x	✔
[21], 2019	✔	✔	x	x	x
[22], 2011	✔	✔	✔	✔	✔
[23], 2018	✔	✔	x	x	x
[24], 2018	✔	✔	x	x	x
[25], 2022	✔	✔	x	x	x
[26], 2012	✔	✔	x	x	x
[27], 2016	✔	✔	✔	✔	✔
[28], 2021	✔	✔	x	x	x
[29], 2022	✔	✔	x	x	x
[30], 2020	✔	✔	x	x	x
[31], 2015	✔	✔	x	✔	✔
[32], 2013	✔	✔	x	x	x
[33]. 2018	✔	✔	x	x	x
[34], 2019	✔	✔	x	x	x
[35], 2019	✔	✔	x	x	x
[36]. 2015	x	✔	✔	✔	✔
[37], 2018	✔	x	x	✔	✔
[38], 2012	✔	✔	x	x	x
[39], 2014	✔	✔	✔	✔	✔
[40]. 2011	✔	✔	x	x	x
[41], 2014	x	✔	x	x	✔
[42], 2019	✔	✔	✔	✔	✔
[43], 2012	x	✔	✔	✔	✔
[44], 2021	✔	✔	✔	x	x
[45], 2017	x	✔	✔	✔	✔
[46], 2017	✔	✔	✔	✔	x

II. SECURITY ISSUES AT THE ARCHITECTURE LEVEL IN M2M COMMUNICATIONS

M2M communication systems are typically composed of three main layers: the device layer, the network layer, and the application layer. Each layer presents its own unique security challenges at the architecture level.

1) Device layer

Physical access: M2M devices are often deployed in remote and unattended locations, making them vulnerable to physical tampering by attackers. Attackers may steal or damage devices, or they may attempt to modify the devices' software or hardware.

Resource constraints: M2M devices often have limited resources, such as processing power and battery life. This can make it difficult to implement security measures without sacrificing performance.

Heterogeneity: M2M devices can come from a variety of vendors and use different technologies. This heterogeneity can make it difficult to implement consistent security measures across all devices.

2) Network layer

Scalability: M2M networks can be very large, with millions or even billions of devices. This can make it difficult to implement security measures that are scalable and performant.

Visibility: It can be difficult to gain visibility into M2M traffic, making it difficult to detect and respond to attacks.

Interoperability: M2M networks may use different technologies and protocols. This can make it difficult to implement security measures that are interoperable across different networks.

3) Application layer

Data integrity: M2M applications often collect and process sensitive data. Attackers may attempt to modify or delete this data to disrupt the application's operation or to steal sensitive information.

Authorization: It can be difficult to ensure that only authorized users and devices have access to M2M applications and data.

Audit: It can be difficult to audit M2M activity to detect and investigate suspicious behaviour.

III. M2M Applications

M2M technology is expanding and encompassing an increasing number of applications [47, 48]. The proposed applications can be divided into five groups based on their intended use: automotive, eHealth, smart metering, city automation, and home automation. The automobile industry has garnered most of the attention, which has resulted in the development of numerous automotive applications. As the technologies are unavailable and we need to prepare for their implementation, some of the applications we are discussing are very simple or like how we live [49]. However, some applications may be so far in the future that we can only imagine them now. All the applications are discussed in detail in the preceding sections.

A. Automotive

All applications involving an automobile, or transit system fall under this category. Each car requires a communication module for its operation, which typically consists of a GPS and a Universal Integrated Circuit Card (UICC) that enables bidirectional communication with the remote servers. Telematics and various forms of vehicle-to-vehicle, vehicle-to-citizen/authority, and vehicle-to-fixed-site communications are all included in M2M-enabled transportation systems [49]. As a result, automotive applications not only enhance safety and resource and traffic management but also provide users with added convenience.

Vehicle Telematics: Using M2M, real-time data from moving cars may be collected and transmitted to a central server or cloud platform [50–52]. This information covers engine performance, fuel consumption, GPS position, and car diagnostics. Telematics systems make fleet management, remote vehicle monitoring, and preventative maintenance possible [53].

Connected entertainment: M2M connectivity enables automobiles to connect to the Internet and provide passengers with various entertainment options [54]. This includes real-time news, weather updates, social media integration, streaming music, internet radio, and personalized content. M2M allows a car to link seamlessly to external networks or gadgets [55].

Usage-Based Insurance (UBI): Thanks to M2M technologies, insurance providers may now provide usage-based insurance plans [56]. Insurance companies can customize premiums based on real usage patterns by gathering information about driving behavior, such as speed, acceleration, braking, and distance. This encourages defensive driving and may result in savings for policyholders [57].

Vehicle Remote Diagnostics: Automakers and service providers can remotely diagnose and correct vehicle software problems [58]. As a result, fewer physical inspections are necessary, and preventive maintenance is made possible, reducing vehicle downtime, and raising customer satisfaction.

Roadside assistance and emergency assistance: M2M-enabled emergency response systems instantly notify emergency services in the case of an accident or other life-threatening circumstances [59]. Emergency personnel receive location information and vehicle details, enabling quicker help. Roadside assistance services like remote vehicle unlocking, battery jump-starting, and tire pressure monitoring are also made possible via M2M.

Autonomous Vehicle Communication: M2M technology enables communication between autonomous vehicles and other vehicles and infrastructure, such as traffic lights and road signs [60, 61]. In Connected and Autonomous Vehicle (CAV) environments, this enables coordinated mobility, better traffic flow, and increased safety.

Intelligent Transport Systems (ITS): M2M communication helps the growth of ITS, which include a variety of applications like traffic management, smart parking, dynamic routing, and congestion control [62–66]. M2M improves overall transportation efficiency by sharing real-time data between infrastructure and vehicles to optimize traffic flow, lower accidents, and reduce congestion.

B. E-Health

Wearable sensors are used in e-health applications to remotely monitor people's health and fitness data, such as blood pressure, heart rate, and temperature. This data is transmitted to a distant server for visualization and analysis. Wearable sensor data has the potential to improve the monitoring and management of people's health and well-being, such as by detecting and monitoring a variety of health conditions. However, it is important to note that the correlation between wearable sensor data and health is not always perfect. There may be other factors that can affect the sensor data, such as the environment or the person's individual physiology. It is also important to use wearable sensor data in conjunction with other methods, such as clinical assessments, to make accurate diagnoses and treatment decisions [67–72].

Remote patient monitoring: Remote patient monitoring is possible because M2M connectivity enables ongoing patient health status monitoring outside conventional healthcare settings [73, 74]. Patients connected to medical devices can gather and send important health information to healthcare professionals, allowing for remote monitoring and prompt action [75]. Early health issue detection, individualized treatment strategies, and better patient outcomes are all made possible by this component of eHealth [76].

Telemedicine: M2M communication enables telemedicine services, allowing medical professionals to remotely diagnose, treat, and monitor patients. This feature of eHealth makes healthcare services more accessible, especially for people who live in rural areas or have limited mobility [77, 78]. Video conferencing and real-time data transmission allow doctors to assess patients' illnesses, provide medical advice, and prescribe medications without seeing them in person [79]. This makes telemedicine a valuable tool for improving access to healthcare and reducing the burden on traditional healthcare systems.

For example, telemedicine can be used to provide remote care to patients with chronic conditions such as diabetes or heart disease [80, 81]. It can also be used to provide care to patients in rural areas who may not have easy access to a doctor. Telemedicine can also be used to provide care to patients who have difficulty traveling to see a doctor, such as elderly patients or patients with disabilities.

Data management and analysis: The gathering, transmission, and analysis of enormous amounts of medical data are all made possible by M2M technology [82]. Electronic Health Records (EHRs) or cloud-based systems can securely receive continuous streams of data from connected healthcare devices and wearables [83, 84]. To personalize care, make educated decisions, and undertake data-driven research to improve healthcare outcomes, healthcare practitioners need real-time access to this data [85].

Self-care and patient engagement: M2M-enabled eHealth solutions enable patients to participate actively in their healthcare and engage in self-care. Individuals can measure their health-related indicators, create goals, get personalized advice, and make wise lifestyle decisions with connected gadgets like wearables and smartphone apps [86]. This element of eHealth fosters healthy behavior's, increases overall wellness, and promotes patient participation.

Enhanced communication and collaboration: M2M communication encourages fluid communication and collaboration between medical professionals, patients, and carers [87]. Real-time data interchange improves cooperation between healthcare stakeholders and facilitates effective communication and distant consultations [88, 89]. This element of eHealth promotes patient experience, lowers healthcare costs, and improves care coordination.

C. City Automation

This includes green applications for city automation in M2M; multiple gateways are deployed across the city to collect and transmit data from various sensors [90–92]. These gateways act as intermediaries, receiving data from sensors in different areas and forwarding it to the central server. Distributing the gateways strategically makes the data collection process more efficient and cost-effective. The gateways aggregate data from multiple sensors, reducing the need for direct connections to the central server. This approach optimizes energy usage, reduces costs, and improves scalability and reliability for green applications in the city.

Smart traffic management: M2M allows it to manage traffic congestion, optimize traffic signals, and monitor and control traffic flow in real-time [93]. It comprises programs like adaptive signal control systems, intelligent traffic lights, and smart parking systems.

Smart energy management: M2M makes it easier to monitor and manage energy use in infrastructure such as buildings, streetlights, and public spaces [94, 95]. It makes it possible to implement automated energy management systems, smart meters, and demand response systems, which results in optimized energy use, financial savings, and a smaller carbon footprint [96].

Environmental monitoring: M2M allows for gathering and analyzing information about environmental factors like noise levels, air quality, and waste management [97]. Environmental sustainability is improved by monitoring waste collection routes, identifying pollution hotspots, and implementing preventive measures.

Public safety and security: M2M applications like video surveillance, emergency response systems, and accident management are vital to improving public safety and security. It allows for quick communication, real-time monitoring, and coordination among public safety authorities.

Smart infrastructure management: M2M makes monitoring and maintaining vital infrastructure easier, such as highways, bridges, water supplies, and waste disposal systems. It makes early defect detection, effective resource allocation, and predictive maintenance possible, ensuring the dependability and lifespan of infrastructure assets.

Intelligent Waste Management (IWM): M2M enables IWM solutions, such as smart bins and waste collection optimization [98, 99]. It aids in streamlining waste collection routes, lower overhead expenses, and enhances overall waste management process efficiency [100].

Citizen engagement and services: M2M communication makes it possible to provide personalized services and platforms for citizen involvement [101–103]. Citizens may access information, offer input, and take part in civic events thanks to technologies like smart city apps, digital signs, and interactive kiosks.

D. Home Automation

By enabling users to detect and control operations remotely, smart home apps, or home automation, provide convenience and enhance quality of life. Homeowners can access and prevent numerous systems and gadgets in their houses from anywhere using these programs [104]. This involves tracking energy use, automating appliances, adjusting temperatures, watching security cameras, and controlling lighting. Smart home applications increase homeowners comfort, convenience, and efficiency by enabling remote task execution, eventually enhancing their overall quality of life.

Smart lighting control: The automation and remote control of lighting systems are made possible by M2M technology [105]. Through voice commands or smartphone apps, users can change the brightness, color, and timing of lights. Interaction between lighting fixtures, sensors, and control devices is possible through M2M connectivity.

Management of HVAC (Heating, Ventilation, and Air Conditioning) systems: M2M offers remote HVAC system monitoring and control [106, 107]. The temperature, humidity, and energy usage can be optimized based on occupancy, weather, and user preferences. Real-time communication between thermostats, sensors, and centralized control systems is possible via M2M.

Advanced security and monitoring: Unauthorized access, motion, or strange behaviors can all be found using integrated sensors, cameras, and alarms. Homeowners may act immediately and access real-time video feeds from their mobile devices thanks to M2M communication's quick notifications and remote monitoring capabilities.

Energy management: M2M technology allows households to regulate their energy usage effectively [108]. Smart meters and sensors can gather real-time energy consumption data, which can then be analyzed to find trends and maximize energy use [109, 110]. To cut down on waste, homeowners can set energy-saving preferences, receive information on their home's energy usage, and remotely operate appliances and other devices.

Smart home appliances: M2M allows numerous home appliances and gadgets to link to one another and communicate. For instance, an intelligent fridge may place a grocery order automatically when supplies are running short, or a smart oven can be remotely prepared using a smartphone app. M2M communication allows these products to be seamlessly integrated and controlled, increasing convenience.

Home entertainment: Users may manage audio/video equipment, streaming services, and media collections from a single interface. M2M allows for device synchronization and offers tailored content recommendations based on user preferences.

Water management: M2M technology may be used in residential settings to monitor water usage. Water resources can be conserved using intelligent irrigation systems that change watering schedules based on the weather and soil moisture levels. M2M communication enables remote monitoring and managing taps, sprinklers, and water usage, encouraging effective water management [100].

E. Smart Grid

By incorporating sophisticated automation and communication capabilities, the smart grid transforms electrical grid systems using M2M communication [111]. M2M applications allow real-time data transmission and seamless interaction between devices, sensors, and utility providers. This encourages wise choices, effective energy management, and increased grid dependability. Demand response, the integration of renewable energy sources, and consumer empowerment are made possible by innovative grid applications in M2M, which improve energy efficiency, sustainability, and system resilience.

Advanced Metering Infrastructure (AMI): M2M supports the implementation of advanced metering equipment (AMI), which includes the deployment of smart meters and communication equipment [112]. Accurate billing, load management, and demand response programs are made possible by smart meters, which gather real-time data on energy consumption and relay it back to utility companies.

Demand response: During moments of high demand, M2M connectivity enables real-time engagement between utility providers and customers. The utility may send signals to linked devices and smart meters to change or reduce energy consumption. M2M enables automatic response mechanisms that are based on demand response signals, such as altering thermostats or cycling appliances [113].

Grid monitoring and control: Real-time grid infrastructure monitoring and control are made possible via M2M connectivity [114]. Sensors and devices gather information on voltage, current, equipment performance, and grid conditions throughout the grid. Through seamless communication with control centers made possible by M2M, grid operators are better equipped to spot problems early, distribute energy more efficiently, and maintain grid stability [115].

Integration of Distributed Energy Resources (DER): M2M communication makes it easier to integrate DERs into the smart grid, including energy storage units, wind turbines, and solar panels [116]. Utility providers can use M2M communication to monitor and control the production and consumption of energy from these decentralized sources, ensuring optimal utilization and system stability.

Fault detection and self-healing: M2M technology gives the smart grid self-healing capabilities [117]. Intelligent gadgets and connected sensors communicate to find problems, such as equipment breakdowns or power outages. M2M allows the grid to automatically reconfigure, isolate, and restore electricity while minimizing outages.

Infrastructure for charging Electric Vehicles (EVs): M2M connectivity enables the integration of EV charging infrastructure into the smart grid. M2M-enabled charging stations can connect with utility companies to manage load balancing, optimize charging schedules, and facilitate demand response for EV charging during grid stress [118].

IV. Vulnerabilities, Security Issues, and Attack Scenarios of M2M Communications

A. Vulnerabilities

To guarantee safety and information integrity, security vulnerabilities, especially in M2M interactions, must play a significant role. The following guidelines are crucial for ensuring data security in M2M communication:

1) Privacy

Confidentiality will guard against unauthorized access to information transmission, ensuring that only authorized sites can access and read data in M2M communication [119]. Privacy protection is crucial to safeguarding user privacy, particularly while sending personal data. People may suffer severe repercussions if sensitive information, such as health information, is disclosed without authorization.

2) Integrity

Keeping data integrity is crucial for restricting and stopping unauthorized alterations. Unauthorized alterations may involve deliberate or accidental alteration, erasure, delay, or repetition of words [120].

3) Availability

Availability is a critical aspect when addressing vulnerabilities, security issues, and potential attack scenarios in M2M communications [121]. Ensuring that network services and the application itself remain accessible to authorized users is essential. It not only safeguards against denial-of-service attacks but also contributes to energy conservation and extends the network's lifespan [122]. Several measures must be implemented to maintain the availability of M2M systems in the face of potential security threats and vulnerabilities [123].

4) Authentication

Authentication focuses on controlling device access to applications and network domains, ensuring that only authorized users can access paper-sensitive data [124]. The security system must verify the parties identity and verify they are who they claim to be [125]. These security rules are the basis for generating security information in M2M communication. Prevent unauthorized access and data falsification and ensure authorized users can access services when needed [126]. Creating M2M applications with security in mind is paramount to ensure their robust protection. Secure M2M communications rely on early threat detection and vulnerability remediation [127]. Nonetheless, M2M communication faces several challenges and security concerns, including:

Physical security: M2M devices are not physically secure—self-chosen danger. Attackers gaining physical access to a device can compromise data security [128]. It is imperative to implement physical security measures, including secure installations and tamper-evident hardware.

Limited resources: Many M2M devices are created to reduce manufacturing and development expenses [129]. Limitations on power, bandwidth, memory, computing power, etc., may be among them. These limitations can impede the implementation of robust security solutions.

Wireless communication: The prevalence of wireless communication exposes M2M networks to potential attacks, as wireless signals are susceptible to interception, increasing security risks and the potential for unauthorized access [130].

Heterogeneity: M2M networks often involve integration of different products and networks from various vendors [131]. Each product has its security challenges, and when combined, these vulnerabilities can accumulate and grow to give you a powerful cybersecurity solution.

Global connectivity: Open networks and universal access to Internet communications are frequently used by M2M networks [132]. M2M devices are more susceptible to attacks due to their widespread communication, which attracts attackers as a target [133].

Software vulnerabilities: Any software, including software used for M2M applications, can contain security vulnerabilities affecting the entire network. Most software vulnerabilities, such as SQL injection, can be exploited by unauthorized users to access sensitive information [134].

Open standards: Open protocols like TCP/IP and ICCP are the foundation of M2M communication [135]. These regulations provide coordination, but security may have been a minor concern when they were developed. Applications for M2M may become vulnerable due to flaws in this process [136].

Latency Constraints: Restrictions on delays. Some M2M applications, like eHealth, have strict time and latency requirements. Denial of service (DoS) attacks and other stalling attacks can have dire repercussions [137]. These circumstances preclude deploying security solutions that cause delays, necessitating precise security measures to reduce any adverse effects on business.

Scalability: M2M networks often contain millions of devices. The scale of these networks creates security risks, challenges the effectiveness of existing security measures, and requires new measures to ensure the security of M2M transmissions [138].

Resource-constrained devices: M2M devices are often resource-constrained, with limited processing power, memory, and battery life [139]. This makes it difficult to implement traditional security solutions on these devices.

All these concerns makes M2M networks less vulnerable to attack. This complicates the security mechanisms of M2M networks. Vulnerabilities and challenges in M2M communication. These challenges and vulnerabilities complicate the security landscape of M2M communication. Addressing these issues is essential for a comprehensive understanding of the associated risks. Developing custom security solutions with unique features and rules tailored to M2M communication is a necessary step in mitigating these challenges and ensuring robust security.

B. Attack Scenarios

Securing M2M communications is of paramount importance, yet ongoing research is required to further clarify the landscape. M2M networks support range of technologies, including LTE, Wi-Fi, ZigBee, Bluetooth, and more. Therefore, any cyberattack applied to these networks will also affect M2M networks. Thus, the M2M network must address security threats in the underlying communication network. Security Understanding the risks M2M networks must deal with is one of several difficulties they must overcome. To overcome this problem, we are looking for potential dangers to M2M communications.

1) Physical attacks

Physical attacks are designed to destroy the hardware or software of an M2M device. Physical attacks in the M2M network environment can be classified as follows:

Side channel attacks: M2M access point devices can be implanted in human bodies to launch side-channel attacks. A side-channel attack exploits physical properties of a device, such as power consumption or electromagnetic radiation, to extract sensitive data. A thorough study [140] has shown how effective side-channel attacks can be in influencing different industries. For example, a hacker can use a side-channel attack to obtain an encryption key from a client device. In another example, a hacker can activate a manufacturing process to alter a product without having access to the design.

Node tampering: In a node tampering attack, the attacker gains physical access to a device and then takes control of it [141]. By physically tampering with the device, the attacker can access the data in its memory and erase any desired data.

Software modification: This kind of attack involves tampering with the software of the target device to prevent it from performing as it should [142]. Wireless control is an option for this. By producing incorrect or invalid data, the afflicted node jeopardizes the integrity of the data. Nodes can be sabotaged using this attack technique. Attackers may use this method to manipulate payments, as demonstrated by electronic toll booths and smart meters.

Hardware Trojan: A hardware Trojan is a malicious modification of a hardware link during manufacturing. These changes may contain malicious hardware or monitor operating systems. Hardware Trojans usually occur when a device is received from an untrusted source [143].

Damage to M2M equipment: Since M2M equipment is often used in easily accessible areas, these will be vulnerable to theft or physical damage [144, 145]. For example, an attacker could modify the central control of the network to control the location of the sensor network configuration [146]. It is essential to recognize that this physical attack poses a severe risk to the security and integrity of M2M networks and their connected devices: physical access and compromise-related risks.

2) Logic-based attacks

Logical attacks aim to disrupt the functionality of the M2M network without necessitating physical access to the target device [147]. In addition to the physical harm that can result from cyberattacks, these attacks can severely impact network operations. These attacks on M2M networks can be categorized as follows:

Spoofing: In spoofing attacks, the attacker impersonates a network user by focusing on typical network procedures [148]. For instance, if the adversary has verified the smart meter, it can compel the owner to pay rivals [149]. Things get more severe if the attacker launches an attack by pretending to be the server. During the attack, the attacker connects an unauthorized M2M device to the server. Replay attacks also fall under this category because they involve data capture and retransmission [150].

Denial of Service (DoS): In a denial-of-service attack, a rogue user prevents authorized users from accessing a machine or network resource. Continuous transmission of pointless packets may lead to the draining of the battery first and implementation failure because it utilizes less power than many M2M devices. The mixer continuously broadcasts, obstructing legitimate stations. This exploit, for instance, may stop someone from reporting an attack in the remote monitoring application. A DoS attack can target any M2M network location, including devices, gateways, underpinning infrastructure, or remote management [151].

Relay attack: In a relay attack, an attacker sends a message multiple times to make the intended recipient think the message was nearly received. This attack, for instance, can be used against access control systems that employ smart tokens. When the door reader opens the door to the attacker while pretending to have a valid token, the attacker launches a counterattack [152]. The M2M domain or network domain is the attack’s intended target.

Attacks on the protocols for routing: Attacks may impact numerous popular routing systems on routing protocols, which aim to manipulate routing decisions along communication routes. Attacks include Byzantine, Wormhole, and Sybil attacks, as examples. Malware exposes numerous unauthorized identities on the network during Sybil attacks [153]. Wormhole attacks involve collecting, tunneling, and relaying packets from one source to another. A collection of nodes sending and storing packets together is a Byzantine attack.

To maintain the integrity and security of M2M networks, it is essential to combat these threats. Implementing robust authentication mechanisms, secure communication protocols, access detection, and encryption technologies help reduce the hazards related to these diseases.

3) Data breaches

Data attacks, which are typically carried out through eavesdropping technology, obliterate the information shared in M2M conversations [154]. The following groups of data attacks in M2M networks can be identified:

Eavesdropping: Attackers target M2M communication to intercept data transmissions, gaining insights into the network [155]. Criminals can access sensitive data, including user behavior, health information, and more. For instance, a burglar planning a theft might eavesdrop on a conversation between a smart meter and the fire department to gather information about the presence of people in a structure.

Man-in-the-Middle (MitM) attack: In this form of attack, the perpetrator places himself in the center of the back-end server and the front-end sensor while hiding and possibly switching the languages of the two [156]. They depend on parties talking to each other face to face.

Traffic studies: Attackers use traffic sniffing to examine transmissions to identify participants, languages, and connection patterns passively. A targeted differentiation attack, for instance, aims to distinguish devices (sensors, actuators, and performers) by looking at the vehicle model [157]. The growing wireless and Internet technology usage has increased these attacks' potency. M2M network communications.

Integrity Attack: When data is transmitted, kept on a device's memory, or hosted on an application server, integrity attacks can jeopardize its integrity [158]. The attacker introduces false information during an integrity attack. The manipulation of sensed data or location information may sometimes endanger lives. For instance, an attacker tricked GPS receivers into believing they were in a different location at an additional time, which put lives in jeopardy and cost money.

Selective forwarding: Selective forwarding attacks are a type of cyberattack in which an adversary arbitrarily drops or delays packets that have been received. Black hole and grey hole attacks are two types of selective forwarding attacks [159]. In a black hole attack, malicious nodes reject all packets rather than forwarding them. In a grey hole attack, malicious nodes randomly drop certain packets while forwarding others. Selective forwarding attacks can be used to disrupt M2M communication and compromise data confidentiality, integrity, and availability [160]. For example, an attacker could use a black hole attack to prevent sensor data from being transmitted to a central server, or a grey hole attack to corrupt data packets in transit. To mitigate the risks of selective forwarding attacks, it is important to implement security measures such as encryption, secure communication protocols, intrusion detection systems, and anomaly detection tools. Additionally, authentication and access control mechanisms can help to prevent unauthorized access to M2M devices and data.

V. M2M Security Solutions

To improve the security of M2M communications, several proposals have been made by academia, industry, and standards bodies such as One M2M and ETSI.

A. Key Management Solution

Key management is essential for M2M security and reliability. Keys are the basis for authentication, confidentiality, and integrity in M2M systems. Current M2M key management strategies often use Public Key Encryption (PKC) to generate keys securely between devices. These two solutions include:

Public Key Infrastructure (PKI): For authenticated M2M devices to receive and transmit encrypted data, this solution depends on a Certificate Authority (CA), a dependable third party.

Symmetric key management: This solution uses a shared key between the two communication systems to secure data transmission. Keys are usually generated using secure key exchange systems such as Diffie-Hellman cryptography or elliptic curves.

Key Distribution Center (KDC): This solution includes a solution that uses a central server or KDC to distribute and manage keys among M2M devices. The KDC generates and distributes keys and manages key revocation and renewal. This scenario includes restricted M2M devices that allow less restricted users to perform complex asymmetric tasks. The secure agent transfers the secret between the restricted and remote servers and extracts the equivalent key for subsequent secure communication. This method separates devices by function and responsibility in low-power wireless personal area networks (6LoW PANs), which are designed for IPv6.This includes an authentication step where the edge router authenticates other devices and a key generation step where a symmetric key is generated with the edge device on a remote server. However, this plan has limitations. Limited M2M nodes are required to manage multiple keys and trusts. If an agent joins the primary plan and 6LR and 6LBR join the secondary plan, the generated keys can be destroyed. Addressing these issues is critical to protecting M2M key management and overall security.

B. Authentication Solutions

Authentication is required in M2M communication to authenticate the site and ensure data integrity. Source authentication and data source authentication are the two basic types of authentication services. In an M2M network, authentication focuses on the authentication of the communication target. This can be done using a secret or Pre-Shared Key (PSK) shared on the device or a digital certificate issued by an authority, Certificate Authority (CA). An authentication code is used to verify that a message or data packet comes from a source. This is frequently accomplished using digital signatures, in which the sender signs a document using a private number, and the recipient verifies the signature using the sender's public key. Information can be verified using other techniques like message authentication codes (MACs) and hash algorithms. In general, authentication plays an important role in M2M security by preventing unauthorized access, maintaining data integrity, and authenticating communications. The required level of security and throughput in an M2M environment are just two factors influencing authentication technology choices.

Secure authentication and authorization protocols: these are essential for protecting M2M communications from unauthorized access and data theft. These protocols allow M2M devices to prove their identity and to obtain permission to access resources. This helps to prevent attackers from gaining access to sensitive data or disrupting M2M operations. Two common secure authentication and authorization protocols for M2M communications are OAuth 2.0 and DTLS. These protocols can be used in a variety of M2M applications to improve the security and reliability of M2M communications.

C. Privacy Solutions

Privacy is important for M2M security solutions as it safeguards sensitive information from unauthorized disclosure. There are various methods which privacy can be effectively maintained within M2M systems:

Data encryption: It serves as a robust safeguard, rendering sensitive information inaccessible to unauthorized parties by transforming it into an indecipherable format. This process involves the utilization of encryption techniques and cryptographic keys for both encryption and decryption.

Anonymization: Anonymization technology replaces or removes personal identifiers from data to prevent a specific individual from being identified. This allows information to be shared while maintaining confidentiality.

Access control: Access control systems restrict access to files to authorized users only. This is done by implementing user authentication and authorization mechanisms, which ensure that only authorized individuals or devices can access sensitive information.

Multilateral Computing (MC): MC offers a significant balance between privacy and security, enabling data analysis while preserving personal privacy. This approach ensures the collection of aggregate information without revealing details about specific individuals. In general, privacy plays a crucial role in M2M security, with technologies such as data encryption, anonymization, access restriction, and data storage being employed to safeguard sensitive data and prevent unauthorized use.

D. Confidentiality Solutions

In M2M security, confidentiality solutions are employed to safeguard private information from unauthorized access or interception during transmission. Various methods, including access control, encryption, and decryption, are utilized for this purpose. The encryption process encodes the plaintext information so only authorized parties with the corresponding decryption key can decrypt it. M2M communications can be secured through a range of encryption algorithms, including symmetric encryption (utilizing a shared key) and asymmetric encryption (using a public and private key pair). Additionally, data integrity is verified to ensure it has not been tampered with, often through the use of hash methods. Decrypting with the correct decryption key is essential for reverting the encrypted data to its original state, and protected data can only be processed and accessed by authorized individuals equipped with the appropriate decryption key. Privacy management in M2M security relies on various access control techniques, including Role-based Access Control (RBAC), Virtual Private Networks (VPN), and firewalls. These controls serve to restrict access to M2M communications, ensuring that sensitive data is only accessible to parties with proper authorization. For effective implementation of security solutions in M2M, organizations must first identify sensitive data that requires protection, such as personal customer information or confidential data. They can then employ suitable encryption methods and access control mechanisms to secure this information during both transmission and storage. Regular reviews and updates of these solutions are essential to address evolving security concerns and maintain a high level of privacy.

Lightweight encryption algorithms: These are essential for M2M security. They are designed to be efficient and lightweight, while still providing strong security. This makes them suitable for resource constrained M2M devices. Examples of lightweight encryption algorithms include AES-GCM and ChaCha20. These algorithms can be used to protect a variety of M2M communications, such as data transmission between M2M devices and cloud servers, communication between M2M devices and other devices on the network, and software updates for M2M devices. By using lightweight encryption algorithms, M2M organizations can help to protect their devices and networks from unauthorized access, data theft, and other security threats.

E. Integrity Solutions

Integrity solutions are paramount in M2M security as they ensure that data transmitted between devices remains unaltered. This is essential for upholding the accuracy and trustworthiness of the conveyed data. To assure the integrity of M2M security, cryptographic techniques such as digital signatures and message authentication codes (MACs) are commonly employed. A digital signature links the communication to the sender's identity, allowing anyone with access to the sender's public key to verify the sender's authenticity. On the other hand, a MAC is a small piece of data used to identify a message and protect its integrity from tampering.

In M2M security, maintaining data integrity relies on the use of digital signatures and MACs. Prior to sending a communication to another device, a digital signature or MAC can be appended to it to ensure its integrity. The recipient can then use the sender's public key or shared secret to confirm that the message remains untampered after the signature or MAC has been validated.

Integrity solutions are pivotal in M2M security to ensure the accuracy and reliability of data transmission between devices. By employing encryption techniques such as digital signatures and MACs, M2M devices can safeguard data integrity and establish the authenticity and dependability of communication.

F. Intrusion Detection and Prevention Systems (IDS/IPS)

These are essential for protecting M2M communications from attacks. IDS/IPS systems monitor network traffic for suspicious activity and can block attacks in real time. There are a number of different types of IDS/IPS systems, but they all work in a similar way. IDS/IPS systems typically use a combination of signature-based detection and anomaly-based detection. Signature-based detection looks for known attack patterns, while anomaly-based detection looks for unusual or suspicious activity.

IDS/IPS systems can be deployed in a variety of ways. They can be deployed as standalone devices, or they can be integrated into routers, firewalls, and other network security devices. Here are some of the solutions of IDS/IPS that are relevant for M2M security:

Network-based IDS/IPS: Network-based IDS/IPS systems monitor network traffic for suspicious activity. They can be deployed at various points in a network, such as at the perimeter of the network, at the edge of a data center, or between different segments of a network.

Host-based IDS/IPS: Host-based IDS/IPS systems monitor the activity of a single device, such as a server or a workstation. They can be used to detect attacks that are targeting the device itself, or attacks that are using the device as a launchpad for attacks against other devices on the network.

Cloud-based IDS/IPS: Cloud-based IDS/IPS systems are deployed in the cloud and can be used to protect M2M devices and networks that are distributed across multiple locations. Cloud-based IDS/IPS systems can be particularly useful for protecting M2M devices and networks that are in remote or hard-to-reach locations.

Recent developments in IDS/IPS for M2M security:

Use of machine learning and artificial intelligence: IDS/IPS systems are increasingly using machine learning and artificial intelligence to improve their detection capabilities. Machine learning and artificial intelligence can be used to develop more sophisticated attack signatures and to detect anomalies that would be difficult to detect with traditional methods.

Support for heterogeneous networks: IDS/IPS systems are also being developed to support heterogeneous networks. Heterogeneous networks are networks that consist of devices from different manufacturers and using different communication protocols. IDS/IPS systems that support heterogeneous networks can be used to protect M2M networks that are becoming increasingly complex and diverse.

Lightweight IDS/IPS solutions: Lightweight IDS/IPS solutions are being developed for resource-constrained M2M devices. Lightweight IDS/IPS solutions can be deployed on M2M devices to provide real-time protection without sacrificing performance or battery life.

G. Security Information and Event Management (SIEM) Systems

SIEM systems typically have a number of different solutions, including:

Log collection: SIEM systems collect security logs from a variety of sources, including M2M devices, networks, and applications.

Log normalization: SIEM systems normalize security logs from different sources into a common format. This makes it easier to analyze the logs and to identify patterns.

Log analysis: SIEM systems analyze security logs for suspicious activity. SIEM systems use a variety of techniques to analyze logs, including signature-based detection, anomaly-based detection, and machine learning.

Alerting: SIEM systems generate alerts when they detect suspicious activity. Alerts can be sent to security personnel via email, SMS, or other notification channels.

Reporting: SIEM systems generate reports on security incidents. These reports can help organizations to understand the threats they face and to improve their security posture.

Recent developments in SIEM for M2M security:

Use of machine learning and artificial intelligence: SIEM systems are increasingly using machine learning and artificial intelligence to improve their detection capabilities. Machine learning and artificial intelligence can be used to develop more sophisticated attack signatures and to detect anomalies that would be difficult to detect with traditional methods.

Support for heterogeneous networks: SIEM systems are also being developed to support heterogeneous networks. Heterogeneous networks are networks that consist of devices from different manufacturers and using different communication protocols. SIEM systems that support heterogeneous networks can be used to protect M2M networks that are becoming increasingly complex and diverse.

Lightweight SIEM solutions: Lightweight SIEM solutions are being developed for resource-constrained M2M devices. Lightweight SIEM solutions can be deployed on M2M devices to provide real-time protection without sacrificing performance or battery life.

VI. Future Work Prospect

M2M communications are becoming increasingly widespread, but they also pose new security challenges. Emerging M2M applications, such as autonomous vehicles and smart cities, pose new security challenges that need to be addressed. Additionally, quantum computers could pose a threat to existing security solutions, so quantum-resistant security solutions need to be developed for M2M communications. Finally, AI could be used to develop more effective security solutions for M2M communications, so this area needs to be explored further. Future work should also focus on developing security solutions that are lightweight, efficient, and interoperable. Security solutions for M2M communications must also be able to support heterogeneous networks and devices with limited resources.

VII. Conclusion

The discussion of M2M Security Solutions focuses on identifying potential risks and vulnerabilities associated with M2M communications and developing mitigation strategies. It is necessary to evaluate the security of various M2M ecosystem elements such as servers, networks, and devices. The use of encryption and authentication mechanisms to protect the confidentiality and integrity of data during transmission is an important topic discussed in M2M security. Consider Symmetric or asymmetric encryption methods and use digital signatures and certificates to confirm the authenticity of devices and servers, which must be done to achieve this. Implementing regulatory measures to prevent illegal access to M2M and data is also an important topic of discussion. To effectively monitor and manage network connections, this requires role-based access control, firewall, access control, and protection mechanisms. The main purpose of the M2M Network Security Conference is to find and resolve threats and vulnerabilities in M2M systems. It offers best practices and implementation instructions to guarantee the security and integrity of M2M conversations and data. These discussions usually center on evaluating the efficacy of current security procedures, looking into emerging dangers, and outlining future security modifications. Before concentrating on the challenges and risks of M2M communications, the section provides an overview of the ETSI M2M architecture and several M2M applications. The sensitivity of the information shared in M2M systems must be emphasized because attacks can lead to significant financial losses, endanger lives, and impact utilities and customers. The topic of existing M2M communication security solutions is explored, emphasizing key management, entity authentication, and privacy issues. However, open research areas include availability, group key management for secure multicast communications, and the development of effective and lightweight cryptographic algorithms for devices with limited resources.

Additionally, it is recognized that M2M systems can acquire enormous volumes of user data. Utilizing data mining techniques, useful information can be gleaned, including user behaviors and health issues. Even though many businesses would be interested in this data, it creates privacy issues that might prevent M2M applications from being widely used. Therefore, it is important to emphasize the need for new policies that safeguard acquired data and maintain user privacy.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Literature Review in M2M and concluding by Manikandan A, Literature review in IoT by Gayathri Narayanan, Literature review in Vulnerabilities by Yugandhar Reddy C, Literature review in active attacks by Mahesh AD, Literature review in passive attacks Vavilala Sushanth, Security solutions by K S Reddy Banu Prakash, Proof reading, complete review and recent challenges and issues by Ramprasad O. G.

ACKNOWLEDGMENT

The authors would like to thank the management of Amrita Vishwa Vidyapeetham for their moral support.

REFERENCES

[1] D. Evans, *The Internet of Things: How the Next Evolutions of the Internet Is Changing Everything*,”*Connections*, vol. 1, pp. 1–11, 2011.

[2] R. Nabati and S. Taheri, “The internet of things (IOT): A survey,” *Turkish Online Journal of Design, Art and Communication*, vol. 6, 2016. doi: 10.7456/1060jse/041

[3] K. G. Shanthi and A. Manikandan, “An improved adaptive modulation and coding for cross layer design in wireless networks,” *Wirel. Pers. Commun*., vol. 108, no. 2, 2019. doi: 10.1007/s11277-019-06448-1

[4] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, “GRS: The green, reliability, and security of emerging machine to machine communications,” *IEEE Communications Magazine*, vol. 49, no. 4, 2011. doi: 10.1109/MCOM.2011.5741143

[5] Rajandekar and B. Sikdar, “A survey of MAC layer issues and protocols for machine-to-machine communications,” *IEEE Internet of Things Journal*, vol. 2, no. 2, 2015. doi: 10.1109/JIOT.2015.2394438

[6] F. Ghavimi and H. H. Chen, “M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications,” *IEEE Communications Surveys and Tutorials*, vol. 17, 2015. doi: 10.1109/COMST.2014.2361626

[7] Y. Cao, T. Jiang, and Z. Han, “A survey of emerging M2M Systems: Context, task, and objective,” *IEEE Internet of Things Journal*, vol. 3, no. 6. 2016. doi: 10.1109/JIOT.2016.2582540

[8] T. S. J. Darwish and K. Abu Bakar, “Fog based intelligent transportation big data analytics in the internet of vehicles environment: Motivations, architecture, challenges, and critical issues,” *IEEE Access*, vol. 6, 2018. doi: 10.1109/ACCESS.2018.2815989

[9] K. Y. Cho, C. H. Bae, Y. Chu, and M. W. Suh, “Overview of telematics: A system architecture approach,” *International Journal of Automotive Technology*, vol. 7, no. 4. pp. 509–517, 2006,

[10] S. Hussain, U. Mahmud, and S. Yang, “Car e-talk: An IoT-enabled cloud-assisted smart fleet maintenance system,” *IEEE Internet of Things Journal*, vol. 8, no. 12, 2021. doi: 10.1109/JIOT.2020.2986342

[11] M. J. Booysen, J. S. Gilmore, S. Zeadally, and G. J. Rooyen, “Machine-to-machine (M2M) communications in vehicular networks,” *KSII Trans. on Internet and Information Systems*, vol. 6, no. 2, 2012. doi: 10.3837/tiis.2012.02.005

[12] R. Coppola and M. Morisio, “Connected car: Technologies, issues, future trends,” *ACM Comput. Surv*., vol. 49, no. 3, 2016. doi: 10.1145/2971482

[13] D. I. Tselentis, G. Yannis, and E. I. Vlahogianni, “Innovative motor insurance schemes: A review of current practices and emerging challenges,” *Accid. Anal. Prev*., vol. 98, 2017. doi: 10.1016/j.aap.2016.10.006

[14] P. Fraga-Lamas and T. M. Fernández-Caramés, “A review on blockchain technologies for an advanced and cyber-resilient automotive industry,” *IEEE Access*, vol. 7, 2019. doi: 10.1109/ACCESS.2019.2895302

[15] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, “Evolution of IoT-enabled connectivity and applications in automotive industry: A review,” *Vehicular Communications*, vol. 27. 2021. doi: 10.1016/j.vehcom.2020.100285

[16] L. Yaqoob, L. U. Khan, S. M. A. Kazmi *et al.*, “Autonomous driving cars in smart cities: Recent advances, requirements, and challenges,” *IEEE Netw*., vol. 34, no. 1, 2020. doi: 10.1109/MNET.2019.1900120

[17] L. Guevara and F. A. Cheein, “The role of 5G technologies: Challenges in smart cities and intelligent transportation systems,” *Sustainability*, vol. 12, no. 16, 2020. doi: 10.3390/su12166469

[18] S. H. Almotiri, M. A. Khan, and M. A. Alghamdi, “Mobile health (m-Health) system in the context of IoT,” in *Proc. 2016 4th Int. Conf. on Future Internet of Things and Cloud Workshops*, 2016. doi: 10.1109/W-FiCloud.2016.24

[19] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang *et al.*, “Internet of things for in-home health monitoring systems: Current advances, challenges and future directions,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, 2021. doi: 10.1109/JSAC.2020.3042421

[20] R. Abdolkhani, K. Gray, A. Borda, and R. DeSouza, “Patient-generated health data management and quality challenges in remote patient monitoring,” *JAMIA Open*, vol. 2, no. 4, 2019. doi: 10.1093/jamiaopen/ooz036

[21] R. M. J. J. van der Kleij, M. J. Kasteleyn, E. Meijer *et al.*, “SERIES: eHealth in primary care. Part 1: Concepts, conditions and challenges,” *European Journal of General Practice*, vol. 25, no. 4, 2019. doi: 10.1080/13814788.2019.1658190

[22] S. McLean, D. Protti, and A. Sheikh, “Telehealthcare for long term conditions,” *BMJ*, vol. 342, 2011. doi: 10.1136/bmj.d120

[23] G. Aceto, V. Persico, and A. Pescapé, “The role of information and communication technologies in healthcare: taxonomies, perspectives, and challenges,” *Journal of Network and Computer*

Applications, vol. 107, 2018. doi: 10.1016/j.jnca.2018.02.008

[24] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput*., vol. 22, no. 2, 2018. doi: 10.1109/MIC.2018.112102519

[25] Batani and M. S. Maharaj, "Towards data-driven models for diverging emerging technologies for maternal, neonatal and child health services in Sub-Saharan Africa: A systematic review," *Global Health Journal*, vol. 6, no. 4. 2022. doi: 10.1016/j.glohj.2022.11.003

[26] M. Swan, "Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0," *Journal of Sensor and Actuator Networks*, vol. 1, no. 3. 2012. doi: 10.3390/jsan1030217

[27] N. D. Schüll, "Data for life: Wearable technology and the design of self-care," *Biosocieties*, vol. 11, no. 3, 2016. doi: 10.1057/biosoc.2015.47

[28] Ocloo, S. Garfield, B. D. Franklin, and S. Dawson, "Exploring the theory, barriers and enablers for patient and public involvement across health, social care and patient safety: a systematic review of reviews," *Health Res. Policy Syst*., vol. 19, no. 1, 2021. doi: 10.1186/s12961-020-00644-3

[29] T. F. Tan, Y. Li, L. S., Lim *et al.*, "Metaverse and virtual health care in ophthalmology: Opportunities and challenges," *Asia-Pacific Journal of Ophthalmology*, vol. 11, no. 3, 2022. doi: 10.1097/APO.0000000000000537

[30] I. Marcu, G. Suciu, C. Bălăceanu *et al.*, "Arrowhead technology for digitalization and automation solution: Smart cities and smart agriculture," *Sensors* (Switzerland), vol. 20, no. 5. 2020. doi: 10.3390/s20051464

[31] Y. Mehmood, C. Görg, M. Muehleisen, and A. Timm-Giel, "Mobile M2M communication architectures, upcoming challenges, applications, and future directions," *Eurasip Journal on Wireless Communications and Networking*, vol. 2015, no. 1. 2015. doi: 10.1186/s13638-015-0479-y

[32] G. P. Hancke, B. de C. de Silva, and G. P. Hancke, "The role of advanced sensing in smart cities," *Sensors* (Switzerland), vol. 13, no. 1. 2013. doi: 10.3390/s130100393

[33] Corbett, K. Wardle, and C. Chen, "Toward a sustainable modern electricity grid: The effects of smart metering and program investments on demand-side management performance in the US electricity sector 2009-2012," *IEEE Trans. Eng. Manag.*, vol. 65, no. 2, 2018. doi: 10.1109/TEM.2017.2785315

[34] E. S. A. Ahmed and M. E. Yousef, "Internet of things in smart environment: Concept, applications, challenges, and future directions article contents," *World Scientific News*, vol. 134, no. 1, pp. 1–51, 2019.

[35] H. Hildmann and E. Kovacs, "Review: Using unmanned aerial vehicles (UAVS) as mobile sensing platforms (MSPS) for disaster response, civil security and public safety," *Drones*, vol. 3, no. 3. 2019. doi: 10.3390/drones3030059

[36] A. Picon, *Smart Cities: A Spatialised Intelligence*, 2015. doi: 10.1002/9781119075615

[37] S. K. Rao and R. Prasad, "Impact of 5G technologies on smart city implementation," *Wirel. Pers. Commun*., vol. 100, no. 1, 2018. doi: 10.1007/s11277-018-5618-4

[38] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. on Frontiers of Information Technology*, 2012. doi: 10.1109/FIT.2012.53

[39] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54. 2014. doi: 10.1016/j.comcom.2014.09.008

[40] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, 2011. doi: 10.1109/MCOM.2011.5741146

[41] Robles T, Alcarria R, Martín D, Navarro M, Calero R, Iglesias S, and López M, "An IoT based reference architecture for smart water management processes," presented at the 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014.

[42] Imani, A. Keshavarz-Haddad, M. Eslami, and J. Haghighat, "Security challenges and attacks in M2M communications," in *Proc. of 9th Int. Symp. on Telecommunication: with Emphasis on Information and Communication Technology*, 2018. doi: 10.1109/ISTEL.2018.8661044

[43] Y. Cheng, M. Naslund, G. Selander, and E. Fogelström, "Privacy in machine-to-machine communications: A state-of-the-art survey," in *Proc. 2012 IEEE Int. Conf. on Communication Systems*, 2012. doi: 10.1109/ICCS.2012.6406112

[44] P. K. R. Maddikunta, S. Hakak, M. Alazab *et al.*, "Unmanned aerial vehicles in smart agriculture: applications, requirements, and challenges," *IEEE Sens. J*., vol. 21, 2021. doi: 10.1109/JSEN.2021.3049471

[45] M. Qabulio, Y. A. Malkani, and A. Keerio, "A framework for securing mobile wireless sensor networks against physical attacks," in *Proc. 2016 Int. Conf. on Emerging Technologies*, 2016. doi: 10.1109/ICET.2016.7813265

[46] C. Zhao, L. Huang, Y. Zhao, and X. Du, "Secure machine-type communications toward LTE heterogeneous networks," *IEEE Wirel. Commun*., vol. 24, no. 1, 2017. doi: 10.1109/MWC.2017.1600141WC

[47] A. Talaminos-Barroso, M. A. Estudillo-Valderrama, L. M. Roa *et al.*, "A machine-to-machine protocol benchmark for eHealth applications - Use case: Respiratory rehabilitation," *Comput. Methods Programs Biomed*., vol. 129, 2016. doi: 10.1016/j.cmpb.2016.03.004

[48] F. Montori, L. Bedogni, M. Felice, and L. Bononi, "Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues," *Pervasive and Mobile Computing*, vol. 50. 2018. doi: 10.1016/j.pmcj.2018.08.002

[49] O. Ghaffarpasand, M. Burke, L. K. Osei *et al.*, "Vehicle telematics for safer, cleaner and more sustainable urban transport: A review," *Sustainability*, vol. 14, no. 24. 2022. doi: 10.3390/su142416386

[50] D. Oladimeji, K. Gupta, N. A. Kose *et al.*, "Smart transportation: An overview of technologies and applications," *Sensors*, vol. 23, no. 8. 2023. doi: 10.3390/s23083880

[51] Md. J. N. Mahi, S. Chaki, S. Ahmed *et al.*, "A review on VANET research: Perspective of recent emerging technologies," *IEEE Access*, vol. 10. 2022. doi: 10.1109/ACCESS.2022.3183605

[52] A. P. John, S. N. Anand, S. Verma, S. Shukla, A. Chalil, and K. N. Sreehari, "IoT based system to enhance agricultural practices," in *Proc. the 2nd Int. Conf. on Electronics and Sustainable Communication Systems*, 2021. doi: 10.1109/ICESC51422.2021.9532804

[53] M. Naik and R. Sikka, "Self-actuated telematics implementation aimed at insurance covers of fleets," *Mater. Today Proc*., vol. 81, 2023. doi: 10.1016/j.matpr.2021.03.201

[54] T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, *Automotive Internetworking*, 2012. doi: 10.1002/9781119944737

[55] D. Boswarthick, O. Elloumi, and O. Hersent, *M2M Communications: A Systems Approach*, 2011. doi: 10.1002/9781119974031

[56] I. Stankevich, K. Korishchenko, N. Pilnik, and D. Petrova, "Usage-based vehicle insurance: Driving style factors of accident probability and severity," *Journal of Transportation Safety and Security*, vol. 14, 2022. doi: 10.1080/19439962.2021.1941459

[57] W. Nai, Z. Yang, Y. Wei *et al.*, "A comprehensive review of driving style evaluation approaches and product designs applied to vehicle usage-based insurance," *Sustainability* (Switzerland), vol. 14, no. 13. 2022. doi: 10.3390/su14137705

[58] M. Kaur, S. Kaur, and Varsha, "Internet of things in the smart automotive sector: A review," in *Proc. the 2022 11th Int. Conf. on System Modeling and Advancement in Research Trends*, 2022. doi: 10.1109/SMART55829.2022.10047604

[59] F. Salahdine, T. Han, and N. Zhang, "5G, 6G, and beyond: Recent advances and future challenges," in *Proc. Annales des Telecommunications/Annals of Telecommunications*, 2023. doi: 10.1007/s12243-022-00938-3

[60] B. N. Kumar, V. M. Pranavan, B. S. L. Pragathi, M. Arunachalam, and C. Chin, "Emergency message dissemination through MQTT over the internet of vehicles - A layered approach," in *Proc. 2022 IEEE 19th India Council Int. Conf.*, 2022. doi: 10.1109/INDICON56171.2022.10039736

[61] J. He, K. Yang, and H. H. Chen, "6G cellular networks and connected autonomous vehicles," *IEEE Netw*., vol. 35, no. 4, 2021. doi: 10.1109/MNET.011.2000541

[62] D. Oladimeji, K. Gupta, N. A. Kose *et al.*, "Smart transportation: An overview of technologies and applications," *Sensors*, vol. 23, no. 8. 2023. doi: 10.3390/s23083880

[63] A. Rehman, K. Haseeb, T. Saba, J. Lloret, and Z. Ahmed, "Towards resilient and secure cooperative behavior of intelligent transportation system using sensor technologies," *IEEE Sens. J.*, vol. 22, no. 7, 2022. doi: 10.1109/JSEN.2022.3152808
[64] M. Aljohani, S. Olariu, A. Alali, and S. Jain, "A survey of parking solutions for smart cities," *IEEE Trans. on Intelligent Transportation Systems*, vol. 23, no. 8, 2022. doi: 10.1109/TITS.2021.3112825
[65] N. Singh, S. P. Sasirekha, A. Dhakne, B. V. S. Thrinath, D. Ramya, and R. Thiagarajan, "IOT enabled hybrid model with learning ability for E-health care systems," *Measurement: Sensors*, vol. 24, 2022. doi: 10.1016/j.measen.2022.100567
[66] G. Pinheiro, R. Miranda, B. Praciano *et al.*, "Multi-sensor wearable health device framework for real-time monitoring of elderly patients using a mobile application and high-resolution parameter estimation," *Front Hum. Neurosci.*, vol. 15, 2022. doi: 10.3389/fnhum.2021.750591
[67] K. O. Asare, I. Moshe, Y. Terhorst *et al.*, "Mood ratings and digital biomarkers from smartphone and wearable data differentiates and predicts depression status: A longitudinal data analysis," *Pervasive Mob. Comput.*, vol. 83, 2022. doi: 10.1016/j.pmcj.2022.101621
[68] C. V. Anikwe, H. F. Nweke, A. C. Ikegwu *et al.*, "Mobile and wearable sensors for data-driven health monitoring system: State-of-the-art and future prospect," *Expert Systems with Applications*, vol. 202. 2022. doi: 10.1016/j.eswa.2022.117362
[69] A. O. Perez, B. Bierer, L. Scholz, J. Wöllenstein, and S. Palzer, "A wireless gas sensor network to monitor indoor environmental quality in schools," *Sensors* (Switzerland), vol. 18, no. 12, 2018. doi: 10.3390/s18124345
[70] J. Kassirer, C. Lefebvre., W. Morgan *et al.*, "Social marketing comes of age: A brief history of the community of practice, profession, and related associations, with recommendations for future growth," *Social Marketing Quarterly*, vol. 25, no. 3, pp. 209–225, 2017.
[71] E. Sadeghi, C. Kappers, A. Chiumento *et al.*, "Improving piglets health and well-being: A review of piglets health indicators and related sensing technologies," *Smart Agricultural Technology*, vol. 5. 2023. doi: 10.1016/j.atech.2023.100246
[72] J. Tu, "Application of wireless sensor network model based on big data ecosystem in intelligent health monitoring system," *Journal of Function Spaces*, vol. 2022, 2022. doi: 10.1155/2022/3179915
[73] J. Gómez, B. Oviedo, and E. Zhuma, "Patient monitoring system based on internet of things," *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.04.103
[74] O. Taiwo and A. E. Ezugwu, "Smart healthcare support for remote patient monitoring during covid-19 quarantine," *Inform. Med. Unlocked*, vol. 20, 2020. doi: 10.1016/j.imu.2020.100428
[75] D. J. Porche, *Health Policy: Application for Nurses and Other Healthcare Professionals*, Jones & Bartlett Learning, 2021, Ch. 6, pp. 81–92.
[76] C. Widberg, B. Wiklund, and A. Klarare, "Patients' experiences of eHealth in palliative care: an integrative review," *BMC Palliat. Care*, vol. 19, no. 1, 2020. doi: 10.1186/s12904-020-00667-1
[77] V. Jones, V. Gay, and P. Leijdekkers, "Body sensor networks for mobile health monitoring: Experience in Europe and Australia," in *Proc. 4th Int. Conf. on Digital Society*, 2010. doi: 10.1109/ICDS.2010.41
[78] R. Negra, I. Jemili, and A. Belghith, "Wireless body area networks: Applications and technologies," *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.04.266
[79] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Telemedicine for healthcare: Capabilities, features, barriers, and applications," *Sensors International*, vol. 2. 2021. doi: 10.1016/j.sintl.2021.100117
[80] E. Hage, J. P. Roo, M. A. G. Offenbeek, and A. Boonstra, "Implementation factors and their effect on e-Health service adoption in rural communities: A systematic literature review," *BMC Health Services Research*, vol. 13, no. 1. 2013. doi: 10.1186/1472-6963-13-19
[81] M. Currie, L. J. Philip, and A. Roberts, "Attitudes towards the use and acceptance of eHealth technologies: A case study of older adults living with chronic pain and implications for rural healthcare Organization, structure and delivery of healthcare," *BMC Health Services Research*, vol. 15, no. 1, 2015. doi: 10.1186/s12913-015-0825-0
[82] J. A. Laub, "From paternalism to the servant organization: Expanding the organizational leadership assessment (OLA) model", *The International Journal of Servant-Leadership*, vol. 1, no. 1, pp. 155–186, 2005.
[83] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet Things J.*, vol. 8, no. 13, 2021. doi: 10.1109/JIOT.2021.3050703
[84] M. A. Uddin, A. Stranier, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Studies in Health Technology and Informatics*, 2018. doi: 10.3233/978-1-61499-914-0-105
[85] K. Shameer, M. A. Badgeley, R. Miotto, B. S. Glicksberg, J. W. Morgan, and J. T. Dudley, "Translational bioinformatics in the era of real-time biomedical, health care and wellness data streams," *Brief Bioinform.*, vol. 18, no. 1, 2017. doi: 10.1093/bib/bbv118
[86] Ben Dhaou, M. Ebrahimi, M. Ben Ammar *et al.*, "Edge devices for internet of medical things: Technologies, techniques, and implementation," *Electronics* (Switzerland), vol. 10, no. 17, 2021. doi: 10.3390/electronics10172104
[87] L. Shang, M. Zuo, D. Ma, and Q. Yu, "The antecedents and consequences of health care professional-patient online interactions: Systematic review," *Journal of Medical Internet Research*, vol. 21, no. 9, 2019. doi: 10.2196/13940
[88] J. M. Grossman, T. S. Bodenheimer, and K. McKenzie, "Marketwatch: Hospital-physician portals: The role of competition in driving clinical data exchange," *Health Aff.*, vol. 25, no. 6, 2006. doi: 10.1377/hlthaff.25.6.1629
[89] Y. Zhai, Y. Wang, M. Zhang *et al.*, "From isolation to coordination: how can telemedicine help combat the COVID-19 outbreak?" *Digital Health and Medical Analytics: Second Int. Conf., DHA 2020*, Beijing, China, 2020, pp. 127–132.
[90] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-enabled smart cities: A review of concepts, frameworks and key technologies," Applied *Sciences* (Switzerland), vol. 12, no. 3. 2022. doi: 10.3390/app12031607
[91] A. Abeera *et al.*, "Exploring multi-hop LoRa for green smart cities," *IEEE Netw.*, vol. 34, no. 2, 2020. doi: 10.1109/MNET.001.1900269
[92] C. Gomez and J. Paradells, "Urban automation networks: Current and emerging solutions for sensed data collection and actuation in smart cities," *Sensors* (Switzerland), vol. 15, no. 9, 2015. doi: 10.3390/s150922874
[93] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of things and its applications: A comprehensive survey," *Symmetry*, vol. 12, no. 10. 2020. doi: 10.3390/sym12101674
[94] S. Talari, M. Shafie-Khah, P. Siano *et al.*, "A review of smart cities based on the internet of things concept," *Energies*, vol. 10, no. 4. 2017. doi: 10.3390/en10040421
[95] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings-energy optimization and next-generation building management systems," *IEEE Internet Things J.*, vol. 4, no. 1, 2017. doi: 10.1109/JIOT.2017.2647881
[96] X. Yan, Y. Ozturk, Z. Hu, and Y. Song, "A review on price-driven residential demand response," *Renewable and Sustainable Energy Reviews*, vol. 96. 2018. doi: 10.1016/j.rser.2018.08.003
[97] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Big data toward green applications," *IEEE Syst. J.*, vol. 10, no. 3, 2016. doi: 10.1109/JSYST.2016.2550530
[98] V. Lampkin, W. T. Leong, L. Olivera *et al.*, *Building Smarter Planet Solutions with MQTT and IBM WebSphere MQ Telemetry*, IBM Redbooks, 2012.
[99] N. B. Chang, A. Pires, and G. Martinho, "Empowering systems analysis for solid waste management: Challenges, trends, and perspectives," *Crit. Rev. Environ. Sci. Technol.*, vol. 41, no. 16, 2011. doi: 10.1080/10643381003608326
[100] S. Nižetić, N. Djilali, A. Papadopoulos, and J. J. P. C. Rodrigues, "Smart technologies for promotion of energy efficiency, utilization of sustainable resources and waste management," *Journal of Cleaner Production*, vol. 231. 2019. doi: 10.1016/j.jclepro.2019.04.397
[101] M. Kassen, "Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation," *Technol. Soc.*, vol. 66, 2021. doi:

10.1016/j.techsoc.2021.101650
[102] H. Rheingold, "Using participatory media and public voice to encourage civic engagement," *Civic Life Online: Learning How Digital Media Can Engage Youth*, W. L. Bennett Ed., pp. 97–118, MIT Press, 2018. doi: 10.7551/mitpress/7893.003.0006
[103] V. Lowndes and H. Sullivan, "Like a horse and carriage or a fish on a bicycle: How well do local partnerships and public participatiion go together?" *Local Government Studies*, vol. 30, no. 1, 2004. doi: 10.1080/0300393042000230920
[104] W. A. Jabbar, T. K. Kian, R. M. Ramli *et al*., "Design and fabrication of smart home with internet of things enabled automation system," *IEEE Access*, vol. 7, 2019. doi: 10.1109/ACCESS.2019.2942846
[105] M. Tastan and H. Gokozan, "An internet of things based air conditioning and lighting control system for smart home," *American Scientific Research Journal for Engineering, Technology, and Sciences*, vol. 50, no. 1, pp. 181–189, 2018.
[106] C. C. Cheng and D. Lee, "Artificial intelligence-assisted heating ventilation and air conditioning control and the unmet demand for sensors, Part 1: problem formulation and the hypothesis," *Sensors* (Switzerland), vol. 19, no. 5, 2019. doi: 10.3390/s19051131
[107] B. E. Medina and L. T. Manera, "Retrofit of air conditioning systems through a wireless sensor and actuator network: An IoT-based application for smart buildings," in *Proc. the 2017 IEEE 14th Int. Conf. on Networking, Sensing and Control*, 2017. doi: 10.1109/ICNSC.2017.8000066
[108] M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. C. M. Leung, "A survey of recent developments in home M2M networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, 2014. doi: 10.1109/SURV.2013.110113.00249
[109] A. Sial, A. Singh, and A. Mahanti, "Detecting anomalous energy consumption using contextual analysis of smart meter data," *Wireless Networks*, vol. 27, no. 6, 2021. doi: 10.1007/s11276-019-02074-8
[110] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings*, 2010. doi: 10.1145/1878431.1878446
[111] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw*., vol. 26, no. 3, 2012. doi: 10.1109/MNET.2012.6201210
[112] Z. Popovic and V. Cackovic, "Advanced metering infrastructure in the context of smart grids," in *Proc. IEEE Int. Energy Conf.*, 2014. doi: 10.1109/ENERGYCON.2014.6850622
[113] P. Siano, "Demand response and smart grids—A survey," *Renewable and Sustainable Energy Reviews*, vol. 30. 2014. doi: 10.1016/j.rser.2013.10.022
[114] J. J. Nielsen, H. Ganem, L. Jorguseski *et al*., "Secure real-time monitoring and management of smart distribution grid using shared cellular networks," *IEEE Wirel. Commun*., vol. 24, no. 2, 2017. doi: 10.1109/MWC.2017.1600252
[115] R. Ma, H. H. Chen, Y. R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Trans Smart Grid*, vol. 4, no. 1, 2013. doi: 10.1109/TSG.2012.2225851
[116] N. M. Kumar, A. A. Chand, M. Malvoni *et al*., "Distributed energy resources and the application of ai, iot, and blockchain in smart grids," *Energies*, vol. 13, no. 21. 2020. doi: 10.3390/en13215739
[117] M. S. Aktas and M. Astekin, "Provenance aware run-time verification of things for self-healing Internet of Things applications," *Concurrency and Computation: Practice and Experience*, 2019. doi: 10.1002/cpe.4263
[118] S. Morsalin, A. Haque, and A. Mahmud, "Machine to machine performance evaluation of grid-integrated electric vehicles by using various scheduling algorithms," *eTransportation*, vol. 3, 2020. doi: 10.1016/j.etran.2020.100044
[119] Y. Cheng, M. Naslund, G. Selander, and E. Fogelström, "Privacy in machine-to-machine communications A state-of-the-art survey," in *Proc. 2012 IEEE Int. Conf. on Communication Systems*, 2012. doi: 10.1109/ICCS.2012.6406112
[120] J. Gaspar, T. Cruz, C. T. Lam, and P. Simoes, "Smart substation communications and cybersecurity: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, 2023. doi: 10.1109/COMST.2023.3305468
[121] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications," *Sustainability* (Switzerland), vol. 14, no. 23, 2022. doi: 10.3390/su142315900
[122] K. Kalaivani and M. Chinnadurai, "A hybrid deep learning intrusion detection model for fog computing environment," *Intelligent Automation and Soft Computing*, vol. 30, no. 1, 2021. doi: 10.32604/iasc.2021.017515
[123] S. Zahid, M. S. Mazhar, S. G. Abbas, Z. Hanif, S. Hina, and G. A. Shah, "Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls," *Internet of Things*, vol. 22, 2023. doi: 10.1016/j.iot.2023.100766
[124] D. Pradhan and H. M. Tun, "Security challenges: M2M communication in IoT," *Journal of Electrical Engineering and Automation*, vol. 4, no. 3, 2022. doi: 10.36548/jeea.2022.3.006
[125] R. T. Moreno, J. B. Bernabe, J. G. Rodríguez *et al*., "The OLYMPUS architecture—Oblivious identity management for private user-friendly services," *Sensors* (Switzerland), vol. 20, no. 3, 2020. doi: 10.3390/s20030945
[126] G. Heo, D. Yang, I. Doh, and K. Chae, "Efficient and secure blockchain system for digital content trading," *IEEE Access*, vol. 9, 2021. doi: 10.1109/ACCESS.2021.3082215
[127] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *Journal of Network and Computer Applications*, vol. 168. 2020. doi: 10.1016/j.jnca.2020.102761.
[128] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on IoT and IIoT devices," in 2020 *Proc. 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, 2020. doi: 10.1109/UEMCON51285.2020.9298138
[129] S. Kahveci, B. Alkan, M. H. Ahmad, B. Ahmad, and R. Harrison, "An end-to-end big data analytics platform for IoT-enabled smart factories: A case study of battery module assembly system for electric vehicles," *J. Manuf. Syst.*, vol. 63, 2022. doi: 10.1016/j.jmsy.2022.03.010
[130] I. Ahmad, T. Rahman, A. Zeb *et al*., "Analysis of security attacks and taxonomy in underwater wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2021. 2021. doi: 10.1155/2021/1444024
[131] V. Ovidiu, B. Roy, O. Marco *et al*., "Internet of robotic things intelligent connectivity and platforms," *Frontiers in Robotics and AI*, vol. 7. 2020. doi: 10.3389/frobt.2020.00104
[132] H. Verma, N. Chauhan, and L. K. Awasthi, "A comprehensive review of 'internet of healthcare things': Networking aspects, technologies, services, applications, challenges, and security concerns," *Comput. Sci. Rev.*, vol. 50, 2023. doi: 10.1016/j.cosrev.2023.100591
[133] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, 2011. doi: 10.1109/MCOM.2011.5741144
[134] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. 2011 IEEE Int. Conf. on Internet of Things and Cyber, Physical and Social Computing*, 2011. doi: 10.1109/iThings/CPSCom.2011.34
[135] M. M. Mogadem, Y. Li, and D. L. Meheretie, "A survey on internet of energy security: related fields, challenges, threats and emerging technologies," *Cluster Comput*., vol. 25, no. 4, 2022. doi: 10.1007/s10586-021-03423-z
[136] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of things and blockchain integration: security, privacy, technical, and design challenges," *Future Internet*, vol. 14, no. 7, 2022. doi: 10.3390/fi14070216
[137] U. Singh, A. Dua, N. Kumar *et al*., "Scalable priority-based resource allocation scheme for M2M communication in LTE/LTE-A network," *Computers and Electrical Engineering*, vol. 103, 2022. doi: 10.1016/j.compeleceng.2022.108321
[138] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, "SoftCell: Scalable and flexible cellular core network architecture," in *Proc. the 2013 ACM Int. Conf. on Emerging Networking Experiments and Technologies*, 2013. doi: 10.1145/2535372.2535377
[139] A. Shalaginov and M. A. Azad, "Securing resource-constrained iot nodes: Towards intelligent microcontroller-based attack

detection in distributed smart applications," *Future Internet*, vol. 13, no. 11, 2021. doi: 10.3390/fi13110272

[140] G. Agosta, A. Barenghi, and G. Pelosi, "Securing software cryptographic primitives for embedded systems against side channel attacks," in *Proc. International Carnahan Conference on Security Technology*, 2014. doi: 10.1109/CCST.2014.6987032

[141] Y. K. Saheed, A. I. Abiodun, S. Misra *et al.*, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, 2022. doi: 10.1016/j.aej.2022.02.063

[142] R. K. Shrivastava, S. P. Singh, M. K.l Hasan *et al.*, "Securing internet of things devices against code tampering attacks using Return Oriented Programming," *Comput. Commun.*, vol. 193, 2022. doi: 10.1016/j.comcom.2022.06.033

[143] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer* (Long Beach Calif), vol. 43, no. 10, 2010. doi: 10.1109/MC.2010.299

[144] C. Hongsong, F. Zhongchuan, and Z. Dongyan, "Security and trust research in M2M system," in *Proc. 2011 IEEE Int. Conf. on Vehicular Electronics and Safety*, 2011. doi: 10.1109/ICVES.2011.5983830

[145] M. Ndiaye, G. P. Hancke, and A. M. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors* (Switzerland), vol. 17, no. 5. 2017. doi: 10.3390/s17051031

[146] M. Waqas, S. Tu, Z. Halim *et al.*, "The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges," *Artif. Intell. Rev*., vol. 55, no. 7, 2022. doi: 10.1007/s10462-022-10143-2

[147] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Security and Privacy*, vol. 6, no. 1, 2023. doi: 10.1002/spy2.271

[148] M. Shafiq, Z. Gu, O. Cheikhrouhou *et al.*, "The rise of 'internet of things': Review and open research issues related to detection and prevention of IoT-based security attacks," *Wireless Communications and Mobile Computing*, vol. 2022, 2022. doi: 10.1155/2022/8669348

[149] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, 2017. doi: 10.1109/JIOT.2017.2749883

[150] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 2. 2011. doi: 10.1109/SURV.2011.041110.00022

[151] G. P. Hancke, K. E. Mayes, and K. Markantonakis, "Confidence in smart token proximity: Relay attacks revisited," *Computers and Security*, vol. 28, no. 7. 2009. doi: 10.1016/j.cose.2009.06.001

[152] W. Dong and X. Liu, "Robust and secure time-synchronization against Sybil attacks for sensor networks," *IEEE Trans. Industr. Inform.*, vol. 11, no. 6, 2015. doi: 10.1109/TII.2015.2495147

[153] R. Sujatha, G. Prakash, and N. Z. Jhanjhi, *Cyber Security Applications for Industry 4.0*. 2022. doi: 10.1201/9781003203087

[154] R. Pothumarti, K. Jain, and P. Krishnan, "A lightweight authentication scheme for 5G mobile communications: a dynamic key approach," *J. Ambient Intell. Humaniz. Comput.*, 2021. doi: 10.1007/s12652-020-02857-4

[155] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Electronics* (Switzerland), vol. 11, no. 20. 2022. doi: 10.3390/electronics11203330

[156] T. Ma, C. Xu, S. Yang *et al.*, "A mutation-enabled proactive defense against service-oriented man-in-the-middle attack in kubernetes," *IEEE Trans. on Computers*, vol. 72, no. 7, 2023. doi: 10.1109/TC.2023.3238125

[157] A. Angelopoulos, E. T. Michailidis, N. Nomikos *et al.*, "Tackling faults in the industry 4.0 era—A survey of machine-learning solutions and key aspects," *Sensors* (Switzerland), vol. 20, no. 1. 2020. doi: 10.3390/s20010109

[158] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications," *Sensors*, vol. 21, no. 11. 2021. doi: 10.3390/s21113654

[159] L. Raja and P. S. Periasamy, "A trusted distributed routing scheme for wireless sensor networks using block chain and jelly fish search optimizer based deep generative adversarial neural network (Deep-GANN) technique," *Wirel. Pers. Commun*., vol. 126, no. 2, 2022. doi: 10.1007/s11277-022-09784-x

[160] M. P. Lokhande, D. D. Patil, L. V. Patil, and M. Shabaz, "Machine-to-machine communication for device identification and classification in secure telerobotics surgery," *Security and Communication Networks*, vol. 2021, 2021. doi: 10.1155/2021/5287514

A. Manikandan completed his B.E in electronics and communication engineering from Madurai Kamaraj University in 2004, master of engineering in communication systems from Anna University in 2006. He received his Ph.D from Anna University at 2018. He is having 16 years of teaching experience and guided many UG & PG Projects. He is a life member of IETE & ISTE. He has published papers in 11 International Journals, 6 International conferences and 6 National Conferences. Currently he is working in M2M communication. He is currently associated with Amrita School of Engineering, Amrita Vishwa Vidhyapeetham, Amritapuri, Kollam, Kerala, India.

Gayathri Narayanan is currently with the Department of Electronics and Communication Engineering at Amrita Vishwa Vidyapeetham Amritapuri Campus. She completed her Bachelors in Engineering from Amrita Institute of Technology and Science, Anna University, India in 2006 and M.Tech in Telecommunications from National Institute of Technology Calicut, India in 2011. She is currently pursuing her PhD in the signal processing domain. Her research interests include real time frequency estimation, systems modelling and signal processing for communication networks.

K. S. Reddy Banu Prakash is currently pursuing bachelor's degree in electronics and communication at Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam, Kerala. He has also participated in Smart City hackathon where he stood as finalist in one of the hackathons held by top companies. He has also published a research paper which was based on recommendation systems in an IIIT Conference and one more paper in an International Journal. His research interest includes Computer Networking, Communication.

Yugandhar Reddy is currently Pursuing a bachelor's degree in Electronics and Communication at Amrita Vishwa Vidyapeetham, Amritapuri Campus. He possesses a profound fascination for technology and exhibits strong technical skills, which have driven him to do many electronics-related projects in the field of microcontrollers, radio frequency, and micro-electro-mechanical systems and He has also done several projects in the field of communication as well. His enthusiasm for technology serves as a driving force, with a particular interest in computer networking and communication. Yugandhar research pursuits revolve around comprehending and enhancing the functionalities of networks and communication systems.

Mahesh A. D. is currently Pursuing a bachelor's degree in Electronics and Communication at Amrita Vishwa Vidyapeetham, Amritapuri Campus. He is an enthusiastic and driven individual with a keen interest in technology. He has a strong grasp of technical skills, which motivated him to take part in renowned hackathons like the Smart City hackathon and earned a spot as a finalist in one of the hackathons organized by leading companies. In addition to his hackathon success, he has published a research paper in an IIIT Conference, focusing on recommendation systems. His research interests lie in understanding and improving the ways networks and communication systems functions.

Vavilala Sushanth is currently pursuing a bachelor's degree in Electronics and Communication at Amrita Vishwa Vidyapeetham, Amritapuri Campus. He is an enthusiastic and driven individual with a keen interest in technology. His strong grasp of technical skills and passion with VLSI. He is particularly intrigued by the realms of computer networking, communication systems, and VLSI. Sushanth's research interests lie in understanding and improving the ways networks and communication systems function, as well as exploring VLSI design and implementation.

Ramprasad Ohnu has completed his bachelor's degree in Electronics and Communication Engineering from Anna University in the year 2011. Currently he is working as Solutions Architect in Cloudera Inc at USA. He has wide experience in design and implementation of technology solutions for an organization. He is responsible for ensuring that the solutions align with the organization's overall business goals and objectives. He has a strong background in technology and a deep understanding of various software and hardware systems. This may include experience with programming languages, databases, cloud computing, and networking. In addition, he can understand how technology solutions can support and drive business goals.