International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

An Empirical Analysis of Smart City Vulnerabilities and Exploits through Real-World Case Studies

Durga Prasad Palla[1], Sabout Nagaraju[2]
[1]PhD Scholar, Department of Computer Science, School of Engineering & Technology, Pondicherry University.
[2]Associate Professor, Department of Computer Science, PUCC, Pondicherry University.
Email ID: durgaprasadpalla96@pondiuni.ac.in[1]

Abstract

The growth in the human population brings new socioeconomic and environmental hazards. In modern times, the world is heading toward smart city advancement to overcome the present and future challenges of urban crowding. Millions of intelligent devices communicate with each other to provide more innovative services ranging from smart health to smart grids. Smart city services endeavor the urban socioeconomic development with the most significant opportunities to improve the quality and ease of life. Smart cities' key enablers and drivers are IoT cloud-based technologies and artificial intelligence solutions. Inevitably, these imperatives promote smart cities for urban socioeconomic and the caliber of life enrichment. Security and privacy threats must be considered when any mechanism is developed and implemented in smart cities. Considering smart cities, security, privacy, and trust are prominent issues which may hamper the adoption and growth of smart city services. This paper narrowed down and examined the security and privacy threats associated with each layer of smart city services, the exploitation of vulnerabilities in each layer, and the communication technologies to be adapted in a few smart city services are discussed. The review of this study may provide helpful research frameworks and serve as a guide for the security and privacy standards in smart city services.
Keywords: *Smart city,Internet of Things,Security,Privacy,Threats.*

1. Introduction

Individuals relocate to cities primarily for work. To back their comfortable living, individuals also need great quality lodging and cost-effective physical and social infrastructure, such as water, sanitation, power, healthcare, transportation, amusement, etc. [1]. The term smart city employs data and communication innovations (ICTs) and other practices to enhance the quality of life, effectiveness of urban operations and administrations, and competitiveness. It is anticipated that around 70% of the world population will live in urban regions by 2050 [2]. This rapid growth in the urban population will lead to financial and infrastructural complications, inadequate natural resources, environmental hazards, poverty, and health problems. Hence, making a city more innovative is the solution to add intelligence to urban socio-economical advancement. Smart cities should be able to create employment opportunities, attract investments, and make it easy to do business. Smart cities should ensure the quality of life, including safety, security of smart home end devices, the privacy of user data collected through various sensors, and ease of accessing the smart city resources [3]. In this paper, we concentrated on five critical smart city services smart hospital, smart home, smart grid, smart dustbin, and smart transport. Fig. 1 shows the structure of some of the smart city services. Smart hospitals deploy IoT end devices, 5G networks, and other technologies like cloud, and artificial intelligence (AI) techniques for secure data transfer, improve the patient experience, streamline the workflow, etc. [4] Traffic congestion caused by vehicles is a problematic issue, and it rises exponentially yearly. Searching for a parking space in a city burns one million barrels per day. On account of that, smart parking is deployed in smart cities to ease residents' movement so that traffic congestion is reduced [5]. Smart Grid allows two-way communications between the service providers and the users. The decentralized energy

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

system is implemented with the help of the smart grid; so that power restoration can be provided quickly in case of any natural calamities occur. Smart Grid also includes integrating renewable energy systems that help to reduce fuel costs and burning fossil fuels. The smart home has the potential to improve home comfort by controlling all the smart devices in one touch and saving the electricity bill by turning off the lights and other electrical appliances when you sleep. The Smart home, which is equipped with a surveillance camera, can make people aware of the events like fire or theft and notify them immediately through alert messages. All the smart devices deployed in the home continuously send the data to a server which causes the battery to drain very fast. So a Low power vast area network is needed to send the data to highly long distances, and it should be less costly. The most prominent network choices are available for LPWAN: LoRa WAN (Long Range) and NB-IoT (Narrow Band). NB-IoT is preferred because of its low cost, improvement in the coverage area, low power consumption, and low latency [6].LoRa WAN is an open-source technology, and it is a low-cost one [7]. LoRa networking provides lightweight encryption and authentication mechanisms that can be configured during activation [8]. Elvira et al. [9] provide a detailed review of threats related to security and privacy in smart city services like smart health care and smart grid. The author also suggests algorithms and protocols need to be implemented in the smart city to avoid security and privacy breach. Shachar et al. [10] reviewed and analyzed IoT devices' possible network layer security attacks. The major cyber attacks identified are spoofing, unauthorized access, man-in-the-middle, DoS (Denial of Service), and Sybil. Andrea et al. [11] analyzed some well-known physical layer attacks: malicious code injection, sleep deprivation, node tampering, and jamming. Jamming. Brittany et al. [12] presented security and vulnerability issues in some of the smart home vendors like Leeo smart alert, Google Home mini, Philips Hue smart lightning, etc. Le costa et al. [13] investigated the various encryption attacks on intelligent devices: side-channel attack, MITM (man-in-the-middle), and cryptanalysis. We concentrated on the following smart city services which was shown in Figure 1 Structure of smart city services.

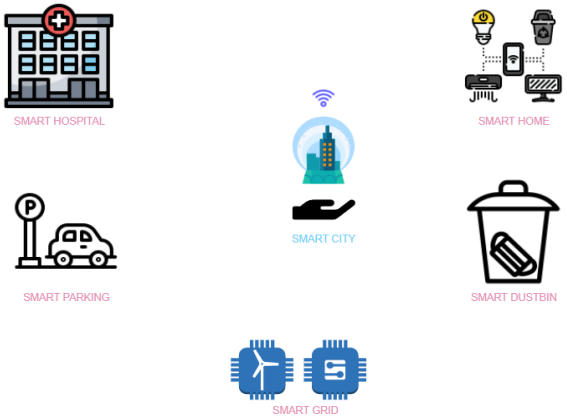

Figure 1 Structure of smart city services

1.1.Contribution

- We presented our real-time configuration of smart city use cases which was shown in Fig. 2
- We explored various vulnerabilities and their associated threats in critical smart services like smart homes, hospitals, parking, dustbin, and grid.
- Reviewed the security techniques and other characteristics of long-range and low-power IoT communication technologies like NB-IoT (Narrow band) and LoRa (Long Range).
- We reviewed centralized learning approaches related to security, privacy, and trust in critical smart city services like smart homes, hospitals, parking, dustbin, and grid.
- Explained the need for federated learning that helps to solve privacy issues and its implementation in smart city services.
- Elucidated the important features of blockchain, such as transparency, trust, and its implementation in smart city services.

1.2.Organization of the paper

The rest of this paper is summarized as follows. Section 2 discusses the smart city experimental setup. The attacks and vulnerabilities in smart city

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

service are discussed in Section 4. Section 3 reviews and analyzes the communication technologies deployed in a smart city and its performance metrics. Section 5 discusses existing research on various attacks related to each IoT layer in smart city services. In section 6 conclusion and future research directions are addressed to safeguard the IoT network.Shown as Figure 2 Overall laboratory setup

2. Experimental Setup

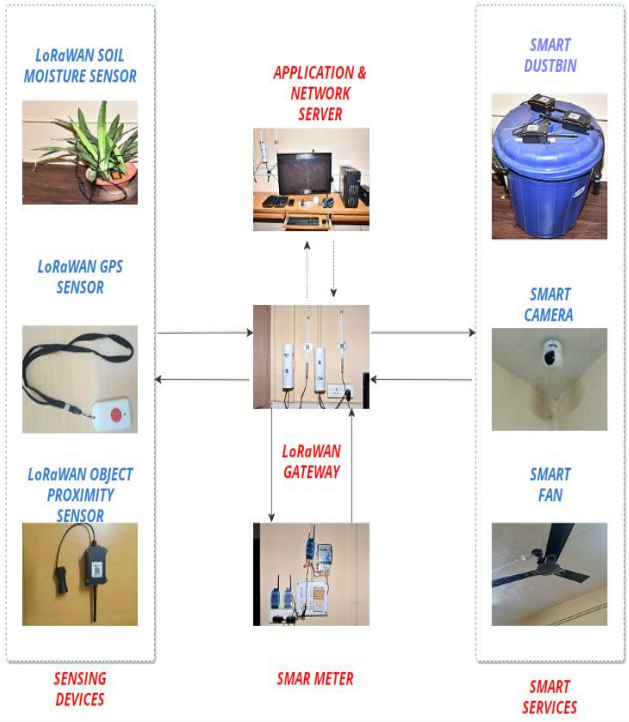

Figure 2 Overall laboratory setup

LoRa WAN GPU server provides effective parallel computing capabilities with a capacity of four dual-slot GPU cords and 64 cores [14]. It supports 5G networking infrastructure, 1 Gb/s Ethernet ports, secure encryption, and virtualization.GPU servers can withstand 10 – 20 minutes to prevent data loss due to power failure. GPU server is equipped with an automatic fan speed controller to reduce heat dissipation. GPU servers have a storage capacity of 4TB, and a 2*L3 cache is available for fast access to data. LoRa WAN GPU server consists of 2 USB slots, 2 RJ45 slots, one serial, and VGA ports. Its operating temperature is 10 to 35 ℃ [15].

LoRa WAN gateway is an open source one that uses a Semtech packet forwarder. It allows users to send sensor data at a highly long distance at a low data rate. LoRa WAN gateway has built-in GPS, antenna, 16MB flash memory, 64MB RAM, 400Mhz ar9331 processor, support 802.11 b/g/n Wi-Fi standards, 12 - 24 V power supply, support 10/100M RJ45 ports for Ethernet connection, dynamic data rate adaptation, the frequency band of 2.4 GHz, supports second, third and fourth generation communication networks like GSM/GPRS/LTE, UMTS, EDGE, data rate speed is 150Mbps downlink and 50Mbps uplink [16]. Some of the applications of LoRa WAN gateway include Smart Buildings & Home Automation, Logistics and Supply Chain Management Smart Metering, Smart Agriculture, Smart Cities, and Smart Factory [17]. Figure 3 shows the gateway ID, gateway name, and status and in Figure 4 gateway information is described.

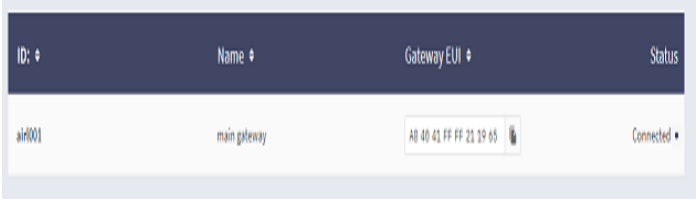

Figure 3 LoRa WAN gateway Dashboard

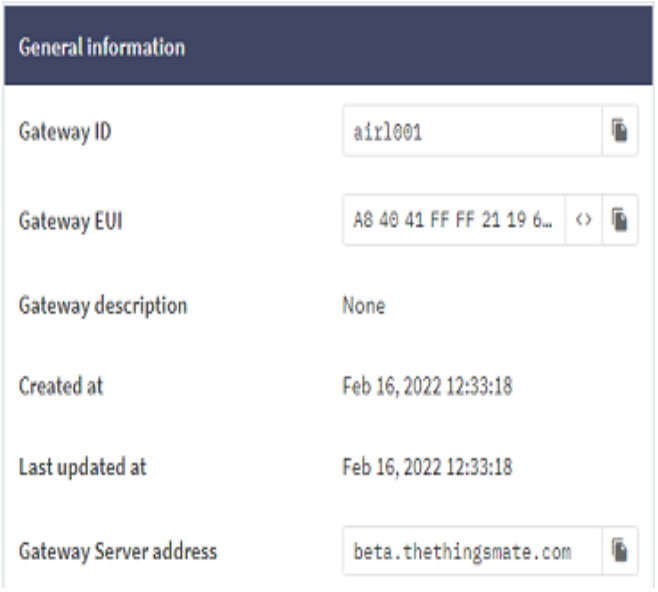

Figure 4 LoRa WAN gateway general information

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

Things Mate is a platform to manage all the LoRa WAN end devices and gateways through secure routing. Things Mate supports all kinds of LoRa WAN versions, and it's a loosely coupled architecture, whereas the user has a high degree of customization, like adding and removing the widgets and other entities [18]. It also provides data visualization features like bar charts, line charts, pie charts, etc. The sensor values are stored in relational database format like rows and columns and saved in .csv and .xlsx format for other data analytics purposes. Things Mate supports scalability so the user can create N number of applications in the platform. Dragino LSE01 is a soil moisture sensor that is used to measure the temperature of the soil, conductivity of soil, and volumetric water contents. The range of soil moisture is measured from 0-100%, and the accuracy is ±3%. If the soil moisture range is from (0-53%) else, if the soil moisture range is (>53%), then the accuracy is ±5%. The unit of soil moisture is measured in V. The soil conductivity falls from 0 – 20000 [19]. The unit of soil conductivity is measured in uS/cm, and its accuracy is ±2%. Soil conductivity high value indicates an excess of soil nutrients, and a low value indicates a deficiency of nutrients [20]. The temperature of the soil falls in the range of -40 to 85. The unit of the temperature of the soil is measured in ℃, and its accuracy is < 0.3 ℃ from -10 to 50 ℃, and if the temperature of the soil is greater than 50 ℃, the accuracy falls to< 0.6 ℃. Dragino LSE01 is powered by a battery of 4000mA Li-SOCI2 battery that can last up to 10 years. LSE01 devices can send sensor data to long distances at a low rate. It can also provide susceptibility to interference while consuming limited energy consumption. Each LES01 is pre-load with a set of unique keys for device enrollments, and registration of these keys will connect to LoRa WAN server [21]. LoRa WAN soil moisture sensor works on the following frequency band, namely CN470/ EU433/ KR920/ US915 [22]. Measuring soil moisture content is critical for farming applications to assist farmers in overseeing their water system more productively so that the farmers can able to extend their agricultural yields.

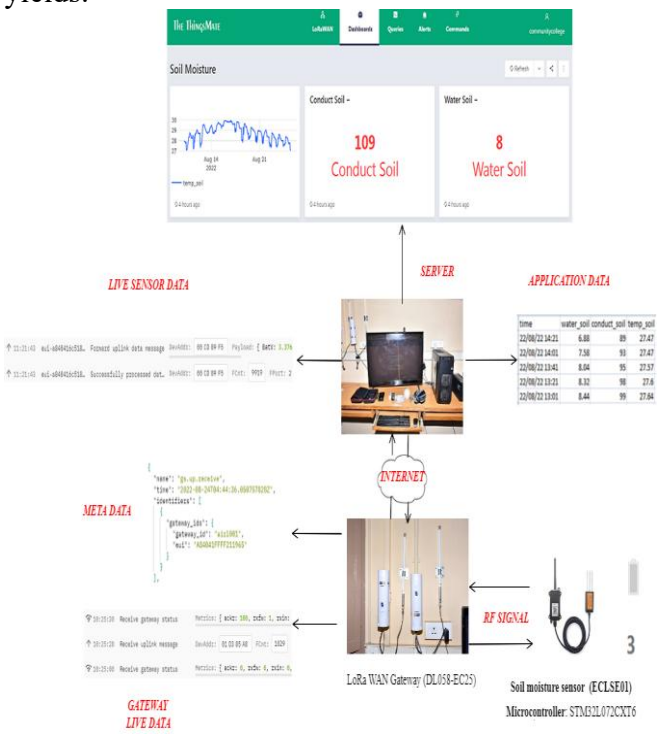

Figure 5 Experimental setup of LoRa WAN Soil moisture sensor

Soil moisture sensor data is collected from various plants such as jack fruit, and crotons will send as radio frequency packets to the nearby gateway. The gateway forwards it to the application server. The application server filters duplicate packets and necessary error checks like error correction etc. The soil conductivity, moisture content, and temperature of the soil are shown as data visualization in Fig.5. STM 32 is a family of 32-bit microcontrollers with various features like easy adaptability, low power, and low voltage design [23]. All the LoRa WAN sensors are built on top of an STM32L072CXT6 microcontroller that consists of a Digital to Analog converter, Analog Digital converter, timers, registers, and low power comparators. STM32L072CXT6 microcontroller operates at an operating voltage of 1.8 to 3.6V, and the temperature range is -40 to 125℃, 192KB flash memory for read and write operation, supportable communication protocols are I2C, SPI, DMA controllers, and USART, 20KB SRAM, 6KB EEPROM [24].

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

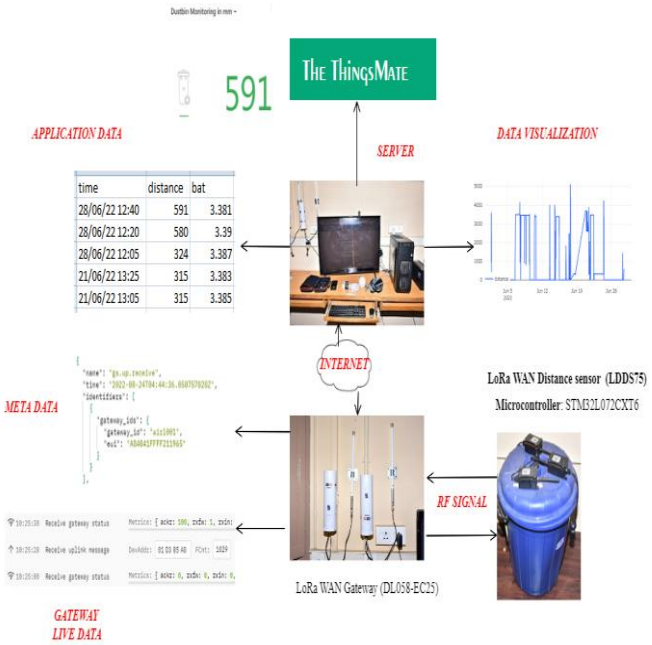

Figure 6 Experimental setup of a LoRa WAN ultrasonic sensor

Dragino LoRa WAN ultrasonic sensor (LDDS75) is used to measure the distance between the sensor and an object. It supports LoRa class A and consumes low power. LoRa WAN ultrasonic sensors calculate the distance between the objects in the range of 280mm to 7500mm [25]. As shown in the Fig. 10. Sensor measure the distance as 591 mm. The ultrasonic sensor is built on top of the STM32L072CXT6 microcontroller, which has various features like low power and low voltage design. The ultrasonic sensor is powered by a 4000mAh/8500mAh Li-SOCL2 battery and lasts up to 10 years. The ultrasonic sensor works on the following frequency band, namely AS923, EU868, KR920, AU915, AU923, EU433, CN470, and IN865. The ultrasonic sensor has a resolution of ±10 mm, and the operating temperature is -20 to 50 ℃ [26]. Some of the critical applications are liquid level measurement, smart parking, trash can monitoring system, supply chain, and sewer [27] [28]. As shown in Fig.6, the smart dustbin is kept inside a laboratory, and the cycle time to send the data to the server is set by 15 min. End devices send Radio Frequency signal as packets that are captured by the nearest gateway, which is in range. The gateway passes the sensed data to the cloud for further data exploration and visualization purposes.

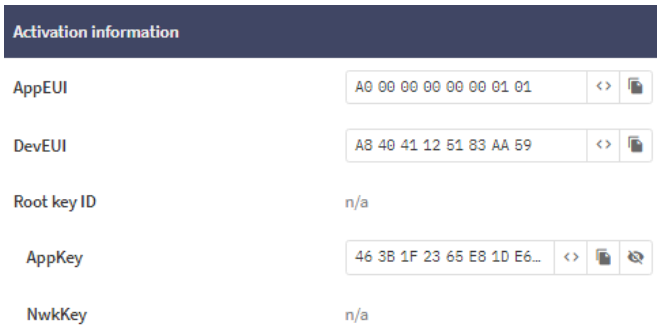

Figure 7 Security keys of LoRa WAN ultrasonic sensor

Whenever any device joins the network, Appkey (Application session key) and NwkKey (Network session key) are generated for security purposes. The NwkKey is used for interaction between the end node and the application server. The main goal of the NwkKey is to preserve the integrity of the message and to prevent message tampering. The Appkey is used for encryption and decryption of the data. Appkey and NwkKey are unique throughout the session [29].Shown as Figure 8 Session keys of LoRa WAN ultrasonic sensor

Figure 8 Session keys of LoRa WAN ultrasonic sensor

SNwkSIntKey guarantees the integrity of data for both uplink and downlink. NwkSEncKey is used to encrypt and decrypt the uplink and downlink payload [30]. Fig. 7 and Fig. 8 shows the security

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

and session keys of ultrasonic sensor. Figure 9 Experimental setup of LoRa WAN GPS sensor

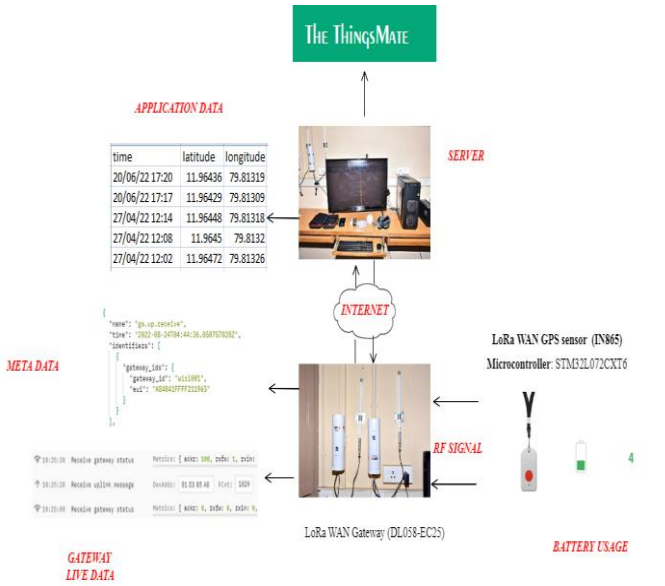

Figure 9 Experimental setup of LoRa WAN GPS sensor

Dragino LoRa WAN GPS sensor is a locationtracker that sends motion and altitude information to long distances at low data rates. It also provides interference immunity to minimize battery consumption. GPS sensor consists of a low-power GPS module and 9-axis accelerometer for detecting latitude and longitude information.GPS sensor is built on top of STM32L072CXT6 microcontroller, which has various features like low power and low voltage design. GPS sensor is powered by a 1000mA Li-on Battery power with a 2 x AA battery holder. GPS sensor works on the following frequency band, namely CN470, EU868, KR920, AU915, AU923, EU433, CN470, and IN865 [31]. GPS sensor has a flash memory of 192KB, 20KB SRAM, 6KB EEPROM, and operating temperature is -40 to 85 °C. During transmission of data, the sensor consumes 24 to 150 mA, and during sleep mode, it consumes 77 mA, and for operating, it needs 3.5 mA. Some of the well-known applications are logistics, supply chain, and human tracking [32]. As shown in Fig.9, data transmitted by the LoRa WAN GPS sensor as RF packets is captured by the LoRa WAN gateway and, in turn, forwards the packet to the application LoRa WAN server. RF packets send latitude, longitude, altitude, and timestamp information to the application server. The application server saves the location information sent by end devices, and finally, it displays the location information as a map for visualization purposes shown in Figure 10.

Figure 10 LoRa WAN GPS sensor dashboard

Figure 10 shows the LoRa WAN GPS dashboard along with Dev EUI, Join EUI, and the name of the sensor. The DevEUI is a 64-bit globally-unique Extended Unique Identifier (EUI-64) allotted by the end device's manufacturer or the proprietor. JoinEUI is also a 64-bit globally-unique Extended Unique Identifier (EUI-64) which is assigned to the application server [33]. Figure 11 Session keys of LoRa WAN GPS sensor

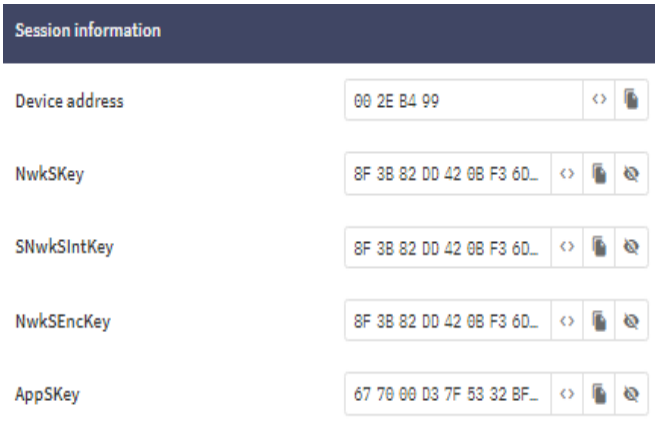

Figure 11 Session keys of LoRa WAN GPS sensor

Dev Address (Device address) is the unique address assigned to the device in the LoRa network. When data is transmitted to the device, it will send an acknowledgment specifying the Dev Address [34]. The location is tracked by using latitude and longitudinal information. Latitude is a measurement of an angle formed by the equatorial plane connecting to the earth's center [35]. Longitude is measured by imaginary lines that run

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

around the earth at the north and south poles. The latitude and longitude information of our current location obtained from the GPS sensor is 11.96 and 79.81.

3. Smart City Services

3.1.Smart Home

Smart homes offer opportunities for a pleasant and safe living environment. People monitor their homes while sitting at any place. However, this communication involves sending data using Wireless Networks like Wi-Fi, Zigbee, Bluetooth, etc., to the cloud. Alberto et al. [36] discussed the security vulnerabilities and attacks that occur while using the above mentioned technologies. Hackers gain access to the environment, and they will steal login information, passwords, etc., wherever the device is connected, either in schools or at home. Wireless Sensor Networks are popular in smart home technology, but there are still many challenges in security. Shancang Liet al. [37] reviewed the various threats that occur in the IoT Layers in Smart Homes are listed below in Table I. Fig. 1 shows the IoT Smart Home Architecture; in the Perception Layer, the devices like Smart Air conditioners, Smart Light, Smart Lock, Smart homes are equipped with sensors like Temperature and Humidity. In the Network layer, which consists of Gateways, and in the application layer, the user can control all the smart home appliances. Fig. 13 shows the layered architecture of smart home service.

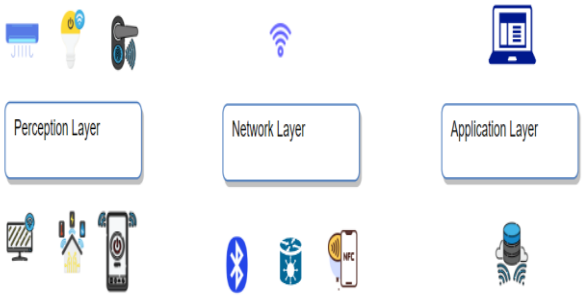

Figure 13 IoT Smart Home Architecture

It contains three layers, namely Perception Layer (Sensors, Actuators, Controllers, End Devices) connected, Network Layer (Gateways), and Application Layer (User view). Table 1 shows several threats in the IoT Layers in the Smart Home.

Table 1 Layer-wise vulnerabilities and associated threats in smart home

Layer	Attack	Description	Vulnerabilities Exploited
Perception Layer	Unauthorized access	The attacker traps the sensitive information of the IoT gadgets (or) devices.	Attempt a brute-force technique to know the shared Wi-Fi keys.
	Availability	The IoT gadgets (or) devices stop working when it is attacked.	Negligence by the manufacturer and developers of IoT devices.
	Spoofing	Attempts to generate communication on behalf of IoT devices.	Authentication weakness.
	Selfish threat	To save resources, IoT nodes stop functioning.	Unable to differentiate the legal and illegal requests.
	Malicious code	Software failure may occur because of malicious code injections like virus, worms, etc.	Weakness in access control privileges.
	DoS (Denial of Service)	A resource becomes unavailable by making a	Security weakness in the network and application layers.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

		continuous request.	
	Transmission threats	Threats such as interruption in communication and manipulating the data.	The lack of physical protection for the devices.
Network Layer	Routing Attack	Degrade the performance by changing the network topology, using exhaustive resources, etc.	Weakness in the network routing protocol.
	DoS	A resource becomes unavailable by making a continuous request.	The security weakness in the network and application layer.
	Transmission threats	Threats such as interruption in communication and manipulation of data.	The lack of physical protection for the devices.
Application Layer	Remote configuration	It allows someone to log in to the system as an authorized user without being physically present.	Because of the use of hard-coded username and password.
	Data breach	The confidential (or) sensitive information is sent to a mistrustful environment.	Insecure Application Programmable Interfaces (APIs) in web applications.
	Security management	Incorrect Access Control, Lack of Encryption, Insufficient Privacy protection.	Occur due to weak cryptographic techniques.
	Management system	All the sensors, controllers, and software patches must be updated regularly.	Weakness in application security perspective.

3.2.Smart Hospital

A Smart Hospital offers good diagnostic tools and promising treatment for patients with IoT smart devices, and it improves the quality of life in real-time monitoring and sends instant notifications in the event of any medical problems. Y. Zhang *et al.* [38] conducted a detailed analysis that the Smart Hospitals must exchange and analyze data between doctors at any time over a wireless network. This weakness can even hurt or even kill some patients if their medical data are unprotected or can be stolen by hackers. Elhoseny *et al.* [39] mentioned that the various threats in the IoT Layers in Smart Hospitals are listed below in Table 2. Fig. 14 presents the Smart Hospital Architecture, the patient is equipped with various sensors, and those sensor values are sent to a hospital server, thereby doctors and nurses can know the patient health status, and if the patient needs further hospitalization, notification is sent to Ambulance.Shown as Figure 14 Smart Hospital Architecture

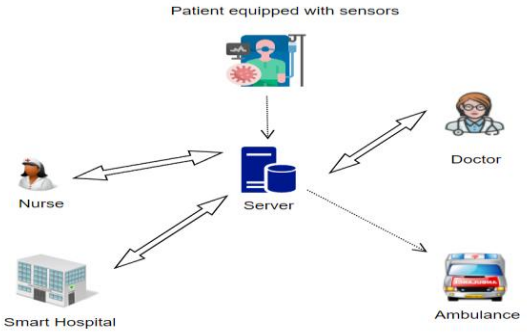

Figure 14 Smart Hospital Architecture

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

Table 2 Layer-wise vulnerabilities and associated threats

Layer	Attack	Description	Vulnerabilities Exploited
Perception Layer	DeviceTampering	Attackers manipulate IoT sensing devices, and it may impair the function or discontinue all or part of the function.	Lack of Physical protection to the IoT Device.
	Sensor tracking	The attacker tries to exploit the location of a smart device. If the patient's location is known, it is against the patient's privacy.	Occurs due to vulnerability in physical interfaces.
	Tag Cloning	The attacker tries using the data he or she has received or the data that can be acquired by a successful side-channel attack.	Occur due to insecure hardware security.
	Side-channel attacks	Reveal the sensitive data of the patient to the attackers.	The lack of a strong level of security.
Network Layer	Man in the Middle attack	The attacker tries to intervene in exchanging information between a user and an application.	Spoofing the Address Resolution Protocol (ARP).
	Sybil Attack	Attempt to create multiple accounts, nodes, or computers to hijack a network.	The deficit of device and identity management.
	Denial of Services	A resource becomes unavailable by making a continuous request.	A security weakness in Network and Application layer.
	Routing Attack	Degrade the performance by changing the network topology, consuming exhaustive resources, etc.	Weakness in the network routing protocol.
	Eavesdropping	The attacker tries to modify the data sent between the unsecured devices.	The lack of encryption and network access control.
	Replay Attack	The attacker sends a simple replay message to a channel instead of an authorized user.	Weakness in the data authentication mechanism.
Application Layer	Cross-Site Scripting	Insert malicious scripts to bypass access control privileges.	Unprotected web pages in the application.
	Data Breach	The confidential (or) sensitive information from	

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

		the patient is sent to a mistrustful environment.	Insecure Application Programming Interface and web pages.
	Phishing	Access patient personal information details which are present in the smart tag .	Occur due to degraded usage of hardware.
	SQL injection	Attacker attempts to attack a back-end database by inserting a malicious SQL statement.	Injection fault in the Database.
	Brute force	The attacker tries every possible combination to break the software.	Occurs due to poor authorization and authentication techniques.

4. Smart City Wireless Communication Technologies

The swift growth of IoT has led to the development of abundant new technologies aimed at low-power wide area networks (LPWAN) [51]. To satisfy the smart city applications, many wireless communication technologies have been developed. Wi-Fi and Bluetooth are used for short-range communications, Long Range and Narrow Band for long-range communications. Both LoRa WAN and NB-IoT are recent communication technologies, and these technologies are growing on a rapid scale in smart city deployment services because of the reduced power consumption and greater coverage area. [52].We provide a brief technical comparison between the NB-IoT (Narrow Band) and LoRa (Long Range) communication technologies. Particularly, we consider the following factors like QoS, cost, power consumption, security, etc. are discussed in table 6

Table 6 Comparison of Narrow Band (NB-IoT) and Long Range (LoRa)WAN

Feature	NB-IoT	LoRa WAN
Tolerate Buffering	Yes	No
Quality of Service (QoS)	High	Low
Data Delivery	Guaranteed Data Delivery	Depends on the network density
Deployment	Plug and Play	Deployment Infrastructure needed
Power Consumption	Compared to LoRa, more power consumption	Ten times lower power consumption than NB IoT
Licensed spectrum	Yes	No
Packet Error Rate	Robust compared to LoRa	Not so efficient as the NB IoT
Cost	Compared to LoRa, it is high	Low
Throughput	~ 40 kbps	~ 150 kbps
Encryption technique	Uses Advanced Encryption Standard (AES) of block size 16 Bytes.	Uses Advanced Encryption Standard (AES) of block size 16 Bytes.
Key Extraction	Extracting the keys is very difficult.	Extracting the keys is easy.
Standardization	3GPP	LoRa Alliance

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

Collision Avoidance	Yes	No
Battery life Peak current Sleep current	10+ years 120 mA 5 µA	15+ years 32 mA 1 µA
Type	Cellular	Non-Cellular
Modulation	QPSK, BPSK uplink, QPSK downlink	LoRa
Allow private networks	No	Yes
Allow handover	No	Yes from V1.1
Topology and Duplex	Star topology and half duplex	Star topology and half duplex
Multi-hop support	No	No
Interference immunity	Low	Very high

5. Literature Survey

Brittany *et al.* [12] presented security and vulnerability issues in some smart home vendors like Leeo smart alert, Google Home mini, intelligent Hue Philips lightning, etc. Le costa *et al.* [13] investigated the various encryption attacks that may happen on smart devices, are side-channel attacks, MITM (man-in-the-middle), and cryptanalysis. Lucas *et al.* [48] provided a brief overview of smart grid application threats and privacy issues. Y. Zhang *et al.* [38] addressed data security and privacy policies by implementing a privacy-aware s-health access control system to hide sensitive attribute values of the patient medical data. Mohamed *et al.* [39] presented a detailed overview of the security threats present in perception, network, and physical layers in smart health applications. Ruiqu *et al.* [42] focused on the smart parking facility may fail because of the following reasons as Manual Error, security threats, which happen due to weak encryption, the lapse of anti-virus software, and hardware failures may occur due to non-redundant power supply and the proper backup facility. Ali Alqazzaz *et al.* [43] discussed the various attacks such as replay attacks, MITM (Man-in-the-Middle), Phishing, and Shoulder surfing that may occur in smart parking applications. Ouidad *et al.* [46] reviewed the security threats in smart services: smart health, grid, waste and water management, surveillance, buildings, payment, learning, transport, and voting. Pardeep Kumar *et al.* [49] discussed the usage of smart meter and discussed major threats that may occur on the consumer side and on the smart grid side. Shama *et al.* [50] examined the various vulnerabilities present in the physical layer of smart grid services. Shama also suggested that when too many IoT devices are connected in smart grid, it may be vulnerable to various attacks. Lu *et al.* [54] discussed the possible security attacks and preserving the privacy of patient data in intelligent health applications. Lin *et al.* [55] used the bilinear Diffie-hellman technique to protect the privacy of smart health care data. And analyzed a secure mutual authentication system for data integrity, privacy, security, and confidentiality. Jiachun Li *et al.* [56] proposed a differential privacy (DP) policy federated learning approach to prevent the privacy leakage of patient data, which is outsourced. Su *et al.* [57] noticed a privacy violation that induces data misuse risk when an enormous amount of smart meter energy data is transmitted to the centralized AI of things for knowledge mining. Sun *et al.* [58] reviewed security and privacy issues in medical applications when the data is processed in a centralized environment.

Conclusion

A smart city ensures a comfortable life and increases the life expectancy of the people who live in urban areas. In this paper, we created an experimental test bed of smart city services like a smart dustbin, GPS tracking, measuring soil moisture, conductivity, and temperature of the soil related to agriculture. We also explored five critical smart city services like smart home, hospital, parking, dustbin, and smart grid and their

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

associated vulnerabilities, attacks (or) threats present in each layer. Moreover, we reviewed and presented important aspects of communication technologies such as LoRa WAN (Long Range) and NB-IoT (Narrow Band), which are deployed in smart cities due to their numerous advantages. Lastly, we conducted a detailed study on present IoT-cloud-enabled smart city solutions and their future requirement engineering, including deep learning, federated learning, and blockchain technologies.

Acknowledgment

This work was sponsored by Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, New Delhi, Grant No. EEQ/2020/000089.

Declarations

Conflicts of Interest:The authors declare no conflicts of interest.

References

[1]. Smart cities in India report http://terienvis.nic.in/WriteReadData/links/Smart%20Cities%20in%20India_Report_pagewise-5937837909069130880.pdf
[2]. Mohanty, Saraju.(2016). Everything You Wanted to Know About Smart Cities. IEEE Consumer Electronics Magazine. no. 5, 60 - 70.
[3]. Smart cities reference note : http://164.100.47.193/Refinput/New_Reference_Notes/English/SMART%20CITIES.pdf
[4]. Smart hospital:https://www.intel.com/content/www/us/en/healthcare-it/smart-hospital.html
[5]. Smart parking happiest minds :https://www.happiestminds.com/whitepapers/smart-parking.pdf
[6]. M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso (2016) Do LoRa lowpower wide-area networks scale?. in Proceedings of the International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 59 – 67.
[7]. Catalano J., Coupigny J-P., Kuyper. M., Sornin. N., and Yegin. A. (2019). Fuota process summary technical recommendation.
[8]. Shanmuga Sundaram J. P., Du W. and Zhao Z. (2020). A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues. IEEE Communications Surveys & Tutorials, 22(1), 371 - 388, First quarter.
[9]. Ismagilova. E., Hughes. L., Rana. N.P. et al. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Inf Syst Front, no. 24, 393 – 414.
[10]. Shachar Siboni, Vinay Sachidananda, Yair Meidan, Michael Bohadana, Yael Mathov, Suhas Bhairav, Asaf Shabtai, and Yuval Elovici. (2019). Security Testbed for Internet-of-Things Devices. IEEE Transactions on Reliability 68(1): 23 - 44.
Andrea I., Chrysostomou C., and Hadjichristofi G. (2015). Internet of Things: Security vulnerabilities and challenges. IEEE Symposium on Computers and Communication (ISCC), 180 – 187.
[11]. Brittany D. Davis, Janelle C. Mason, Mohd Anwar. (2020). Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. IEEE Internet of Things Journal, 7(10): 10102 - 10110.
[12]. Costa L., Barros J., and Tavares M. (2019). Vulnerabilities in IoT Devices for Smart Home Environment. 5thInternational Conference on Information Systems Security and Privacy (ICISSP).
[13]. GIGABYTE server datasheet: https://download.gigabyte.com/FileList/EBrochure/G191-H44_datasheet_v1.1.pdf
[14]. GIGABYTE server architecture and product overview: https://www.gigabyte.com/us/Enterprise/GPU-Server/G492-ZD0-rev-A00
LoRa WAN Gateway datasheet : https://www.dragino.com/downloads/downloads/LoRa_Gateway/DLOS8/DLOS8_Lo

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

RaWAN_Gateway_User_Manual_v1.2.pdf
[15]. LoRa WAN Gateway: https://www.dragino.com/products/lora-lorawan-gateway/item/160-dlos8.html
[16]. The Things Industries: https://www.thethingsindustries.com/stack/
[17]. LoRa WAN Soil Moisture sensor User Manual V 1.4: https://www.dragino.com/downloads/downloads/LoRa_End_Node/LSE01/LoRaWAN_Soil_Moisture_%26_EC_Sensor_UserManual_v1.4.pdf
[18]. Electrical conductivity of Soil Moisture sensor : http://traceandsave.com/what-can-electrical-conductivity-tell-us-about-our-soil/
[19]. LSE01 LoRa WAN Soil Moisture sensor: https://www.dragino.com/products/lora-lorawan-end-node/item/159-lse01.html
[20]. LSE01 LoRa WAN Soil Moisture sensor : https://www.dragino.com/downloads/downloads/LoRa_End_Node/LSE01/Datasheet_LSE01_LoRaWAN_Soil_Moisture_%26_EC_Sensor.pdf
[21]. ST Micro Reference Designs : https://ecsxtal.com/stmicro-stm32-reference-designs-32768khz
[22]. ST Micro controller Datasheet: https://www.st.com/resource/en/datasheet/stm32l072cz.pdf
[23]. LoRa WAN Ultrasonic distance sensor: https://www.dragino.com/downloads/downloads/LoRa_End_Node/LDDS75/Datasheet_LDDS75_LoRaWAN_Distance_Detection_Sensor.pdf
[24]. LoRa WAN Ultrasonic distance sensor user manual: https://www.dragino.com/downloads/downloads/LoRa_End_Node/LDDS75/LoRaWAN_LDDS75_User%20Manual_v1.6.pdf
LoRa WAN Ultrasonic distance sensor: https://www.alliot.co.uk/wp-content/uploads/2020/04/TEK-766-Fluid-Ultrasonic-LoRaWAN-datasheet.pdf
[25]. Sutjarittham T., Gharakheili H. H., Kanhere S. S. and Sivaraman V. (2022). Estimating Passenger Queue for Bus Resource Optimization Using LoRaWAN-Enabled Ultrasonic Sensors. IEEE Systems Journal, 1 – 12.
[26]. LoRa WAN security keys: https://www.thethingsnetwork.org/docs/lorawan/security/
[27]. Chen X, Lech M, Wang L.: A Complete Key Management Scheme for LoRaWAN v1.1, Sensors, (2021).
[28]. LoRa WAN GPS sensor: https://s3-us-west-2.amazonaws.com/files.seeedstudio.com/products/101990655/res/Datasheet_LGT-92.pdf
[29]. LoRa WAN GPS sensor user manual: https://www.dragino.com/downloads/downloads/LGT_92/LGT-92_LoRa_GPS_Tracker_UserManual_v1.6.8.pdf
[30]. LoRa WAN developer portal and documentation: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/the-book/deveui/
[31]. LoRa quick start guide: https://docs.rs-online.com/ae65/0900766b815bf8bf.pdf
[32]. GPS Coordinates: https://www.itilog.com/
[33]. Alberto Ernesto Coboia,Thang Tran A., Son Q. Trana, Minh Nguyen. T. (2021). Security Problems in Smart Homes. ICSES Transactions on Computer Networks and Communications. 1 - 9.
[34]. Shancang Li. (2017). Security Architecture in the Internet of Things. Elsevier Book, 27 - 48.
[35]. Zhang Y., Zheng D., Deng R. H. (2018). Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control. IEEE Internet Things Journal, 5(3) : 2130 - 2145.
[36]. Mohamed Elhoseny, Navod Neranjan Thilakarathne,Mohammed I. Alghamdi, Rakesh Kumar Mahendran, Akber Abid Gardezi, Hesiri Weerasinghe and Anuradhi Welhenge. (2021). Security and Privacy Issues in Medical Internet of Things:

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

Overview, Countermeasures, Challenges and Future Directions. MDPI Sustainability, 13(21): 1 - 31.
[37]. Can Biyik, Zaheer Allam, Gabriele Pieri, David Moroni, Muftah O'Fraifer, Eoin O'Connell, Stephan Olariu and Muhammad Khalid (2021). Smart Parking Systems: Reviewing the Literature, Architecture and Ways Forward. MDPI Smart Cities, 4(2): 623 - 642.
[38]. Andrew Mackey, Petros Spachos, Konstantinos N. Plataniotis (2020). Smart Parking System Based on Bluetooth Low Energy Beacons With Particle Filtering. IEEE Systems Journal, vol. 14(3): 3371 - 3382.
[39]. Ruiqu Ma, Patrick, Lam T. I., Chi Kin Leung (2021). Reliability Analysis of a Smart Parking Information System: The Case of Hong Kong. Wireless Personal Communications 119(2), 1681 - 1701.
[40]. Ali Alqazzaz, Ibrahim Alrashdi, Esam Aloufi, Mohamed Zohdy, Hua Ming (2018). SecSPS: A Secure and Privacy-Preserving Framework for Smart Parking Systems. Journal of Information Security, 9(4): 299 - 314.
[41]. Vairam.T & Sarathambekai S (2019). Proficient smart trash can management using internet of things and SDN architecture approach. International Journal of Enterprise Network Management, Inderscience, vol. 10(3), 241-252.
[42]. Jino Ramson S.R., Vishnu S, Alfred Kirubaraj A., Theodoros Anagnostopoulos, and Adnan M. Abu-Mahfouz (2022). A LoRaWAN IoT-Enabled Trash Bin Level Monitoring System. IEEE Transactions on Industrial Informatics, 18(2):786 - 795.
[43]. Ouidad Saber, Tomader Mazr (2021). Smart City Security Issues: The Main Attacks And Countermeasures. International Conference on Smart City Applications.
[44]. Matthew Pirretti, Sencun Zhu, Vijaykrishnan N., Patrick McDaniel, Mahmut Kandemir, (2006). The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. International Journal of distributed Systems, SAGE Journal, vol. 2(3): 267 - 287
[45]. Lucas V. Dias, and Rizzetti T. A. (2019). A Review of Privacy-Preserving Aggregation Schemes for Smart Grid. IEEE Latin America Transactions 19(7) : 1109 - 1120.
[46]. Pardeep Kumar, Yun, Guangdong Bai, Andrew Paverd, Jin Song Dong, and Andrew Martin (2019). Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. IEEE Communications Surveys & Tutorials, 21(3), 2886 - 2927.
[47]. Shama Naz Islam, Zubair Baig, and Sherali Zeadally (2019). Physical Layer Security for the Smart Grid: Vulnerabilities, Threats and Countermeasures. IEEE Transactions on Industrial Informatics, 15(15): 6522 – 6530.
[48]. Ikpehai A. et al. (2019). Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review. IEEE Internet of Things Journal, 6(2): 2225 - 2240.
[49]. LORAWAN® AND NB-IOT: COMPETITORS OR COMPLEMENTARY? (2019). ABI whitepaper.
[50]. Lu R., Lin X., and Shen X. (2013). SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-health care emergency. IEEE Trans. Parallel Distrib. Syst., vol. 24(3): 614 – 624.
[51]. Lin X., Lu R., Shen X., Nemoto Y., and N. Kato (2009). SAGE:A strong privacy preserving scheme against global eavesdropping for ehealth systems. IEEE J. Sel. Areas Commun. 27(4): 365–378.
[52].
[53]. [56] Jiachun Li, Yan Meng , Lichuan Ma, Suguo Du, Haojin Zhu, Qingqi Pei and Xuemin Shen (2022). A Federated Learning

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0325
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2254 - 2268

Based Privacy-Preserving Smart Health care System. IEEE Transactions on Industrial Informatics, 18(3): 2021 - 2031.

[54]. Su Z. et al. (2022). Secure and Efficient Federated Learning for Smart Grid With Edge-Cloud Collaboration. IEEE Transactions on Industrial Informatics, 18(2): 1333 - 1344.

[55]. Sun, Cai , Li, Liu, Fang, Wang (2018). Security and privacy in the medical internet of things: A review. Secur. Commun.Netw. 1 - 9.