Internet of Things and Cloud Computing
2024, Vol. 12, No. 2, pp. 28-39
https://doi.org/10.11648/j.iotcc.20241202.12

Review Article

Attacks, Challenges, and Countermeasures for an Integrated IoT Framework

Fadele Ayotunde Alaba[1, *], Ifeyinwa Marisa Madu[2], Haliru Musa[3]

[1]Department of Computer Science, Federal College of Education, Zaria, Nigeria
[2]Department of Mathematics, Morgan State University Baltimore, Maryland, USA
[3]Department of Chemistry, Federal College of Education, Zaria, Nigeria

Abstract

The Internet of Things (IoT) has lately attracted a lot of interest owing to the fact that it has several applications in a variety of fields and makes communication easier across a variety of levels. The IoT is made up of three unique levels, which are the physical layer, the network layer, and the application layer at the most fundamental level. The purpose of this study is to examine security threats and the responses that correspond to them for each layer of the IoT architecture. Additionally, the article investigates the implications that arise from security breaches on IoT devices. In addition to providing a detailed taxonomy of attacks, this research reveals security weaknesses that are present inside each tier of the IoT network. In addition to this, the article investigates a variety of modern security frameworks, investigates probable security flaws, and investigates remedies that correspond to those vulnerabilities. In conclusion, the article proposed the "Unified Federated Security Framework," which is an all-encompassing security architecture made specifically for IoT networks. In order to facilitate the ability of users inside the security layer to acquire access to resources situated within a separate security layer, the proposed framework is based on the building of trust across the three levels. This allows users to gain access to resources without having to utilise the account of another user.

Keywords

IoT, Security, Framework, Attacks, Network, Sensors

1. Introduction

The IoT is a rapidly growing technology that enables devices and objects to communicate with each other through powerful codes. The heterogeneity of devices, platforms, wireless technologies, communication protocols, and applications are IoT's major characteristics and building block [1]. The diversity of IoT applications and services poses a challenge that must be addressed to provide seamless operation and support a wide range and efficient deployment of IoT shortly [2]. The design of IoT systems is based on intelligent frameworks, including device autonomy, sensing capability, and contextual awareness. Embedded sensors and actuators provide IoT devices with the necessary intelligence and capability to recognize their surroundings [3]. IoT devices can make decisions autonomously based on sensed data. The increasing demand for large-scale

*Corresponding author: ayotundefadele@yahoo.com (Fadele Ayotunde Alaba)

Received: 31 May 2024; **Accepted:** 1 July 2024; **Published:** 15 August 2024

deployment of IoT devices has led to numerous service applications being proposed and developed. However, the increasing demand for large-scale deployment of IoT devices results in major security concerns [4].

Security is a critical aspect of any communication network, and attacks have targeted wired networks. Advances in technology have made wireless networks more affordable and easier to build, resulting in widespread attacks against wireless networks [5]. Securing IoT architecture/framework is a significant challenge that supports the full adoption of IoT. The lack of a unified security framework exposes IoT devices to vulnerabilities, threats, and attacks. The global interconnection of billions of highly available devices creates enormous pathways for attackers to compromise the security of IoT networks. Therefore, security challenges need to be addressed in order to encourage the full adoption of IoT [6].

This paper proposes detailed state-of-the-art security frameworks and attack countermeasures for IoT networks, discusses architectural challenges in each layer of IoT networks, develops a broad attack taxonomy and security vulnerabilities in each layer, and proposes a unified security framework based on user identification for IoT networks.

The modeling of the security attacks in IoT networks is illustrated in Figure 1.

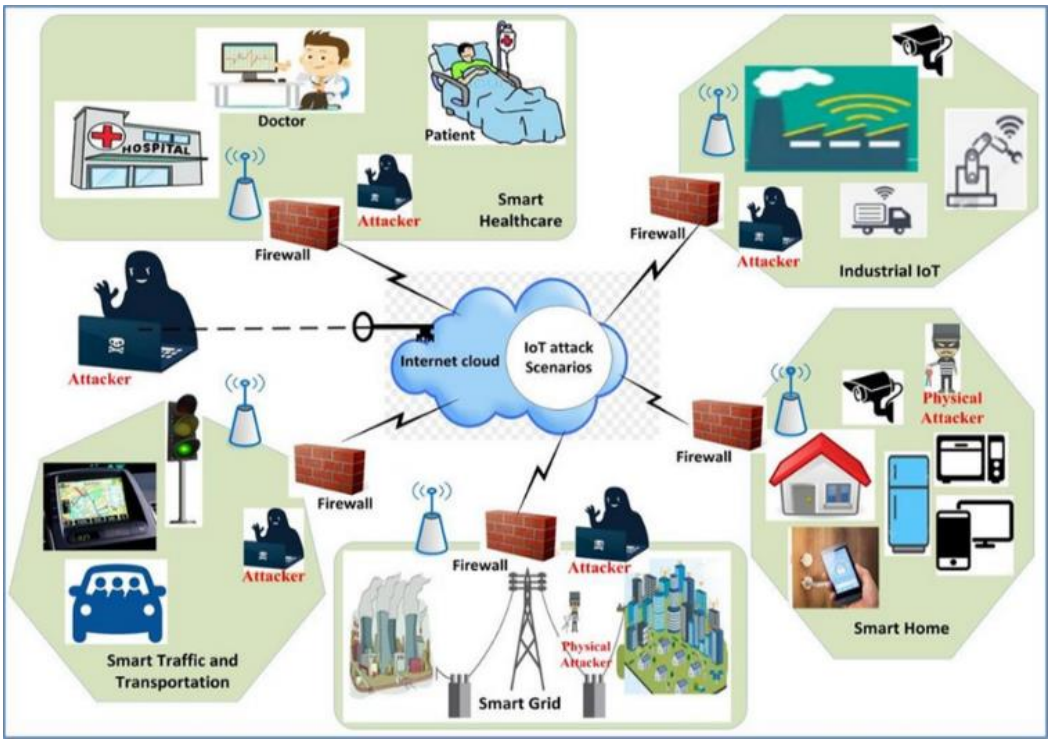

Figure 1. *Security Attacks Scenario of IoT.*

The rest of the paper is organized as follows. Section 2 discusses the state-of-the-art IoT attacks framework. The taxonomy of Attacks in IoT is discussed in section 3. The challenges in each layer of IoT is provided in Section 4. Sections 5 and 6 present the proposed unified IoT security framework and security countermeasures for each layer, respectively. Section 7 discusses future directions, while Section 8 presents the conclusions of the study.

2. State-of-the-Art IoT Attacks Framework

Different research efforts have focused on establishing attack frameworks for the IoT's physical, network, and application layers [7-10]. The security architecture for smart cities developed by J. P. S. Piest et al. incorporates Black Networks and Key Management Systems (KMS) to thwart assaults on the IoT's application layer [11]. The framework protects sensitive data, keeps private information private, and distributes keys efficiently, all while keeping the IoT's application layer as secure as possible. The framework is not reliable in protecting smart city IoT devices from threats such as side-channel attacks, cryptanalysis attacks, denial of service (DoS) attacks, and malicious scripts. Traditional security flaws in the IoT physical layer were addressed by the software-defined networking (SDN) architecture [12]. A unique SDN-based security architecture for the IoT physical layer was suggested by [12]. This framework makes use of border controllers to protect voice-over IP (VoIP) networks and to link heterogeneous IoT devices from various domains. However, securing traffic (desirable and unwanted) at the

borders is difficult, resulting in serious issues like packet delay/loss and distributed denial of service (DDoS). Service-oriented architecture (SOA)-based IoT middleware may greatly benefit from a well-defined, standardized security framework, as shown by the work of [13].

In order to provide a framework for demonstrating network layer security for IoT, the authors laid up security services that may be implemented. Such services aim to lessen network-level security risks in SOA-based IoT middleware frameworks [14].

Middleware framework Object Security Framework (OSCAR) with constrained application protocol (CoAP) was suggested by D. Muhammed, E. Ahvar, S. Ahvar, and M. Trocan for End-to-End (E2E) security at the IoT network layer [15]. Multicasting, asynchronous data transfer, and caching are all supported, and complete data integrity is provided through the straightforward Datagram Transport Layer Security (DTLS) method. Using a three-tiered system paradigm, Y. J. Lin et al. explored several vulnerabilities to the security of the IoT and proposed a method for mitigating them. Applications rely heavily on RFID, ZigBee, and other sensors, all of which may be compromised [16]. Heterogeneity presents challenges for network security, interoperability, and cooperation across sectors and settings by introducing vulnerabilities at the network layer, such as sinkhole attacks, routing information assaults, RFID unauthorized access, and DoS. To mitigate the risk of DoS and provide a signature verification service for docker images, suggested a decentralized architecture on content trust for docker images. Security risks and vulnerabilities in industrial IoT networks may be avoided with the use of a graphical security framework.

Information distribution across heterogeneous devices in IoT networks may be computed thanks to the work of [17], who created a theoretical security framework for IoBT networks. This paper by Z. Boulouard, M. Ouaissa, M. Ouaissa, and S. El Himer, titled "Security Implications of Permission Models in Smart-Home Application Frameworks," proposes a new permission model to address some of the most serious issues with the current SmartThings permission model, such as its failure to safeguard critical event data adequately [18]. The blockchain-based hybrid network architecture for the smart city developed by A. Chauhan, M. Bahadir, and B. Teichgräber provides security and anonymity using a memory-hardened Proof-of-work method but does not effectively handle edge nodes [19]. Using SDN and network function virtualization (NFV), a unique policy-based architecture was suggested to enhance IoT security [20].

This paper presents a federated unified security framework that provides complete security features for IoT networks. It also properly classifies attacks and captures all possible threats to develop and implement better security countermeasures.

3. Taxonomy of Attacks in IoT

IoT devices are vulnerable to physical, network, and application attacks because of the variety of network technologies used in their design and implementation. Therefore, it is critical to provide a comprehensive taxonomy of IoT attacks. Better security measures for IoT devices may be developed and implemented more easily, thanks to the taxonomy's cataloging of all the system's flaws and dangers. Our IoT attacks taxonomy presented in Figure 2 is unique compared to others because all attacks are categorized based on the three layers.

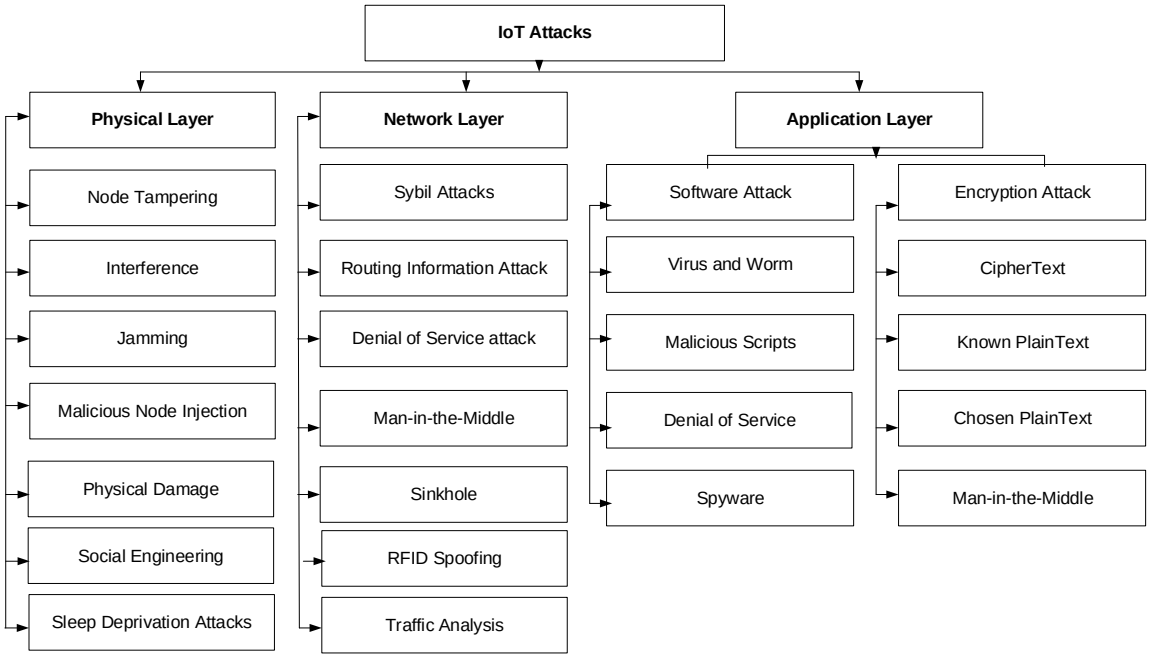

Figure 2. *IoT Attacks Taxonomy.*

3.1. Physical Layer Attacks

As stated earlier, the purpose of the physical layer is to collect data from its environment and transform it into digital form [21]. A detailed description of each attack is provided and presented as follows.

Node Tampering: When an attacker physically alters a sensor node. The attacker has full control over the seized node, wreaking havoc on the network. In order to access and manipulate sensitive information, attackers may harm sensor nodes by physically replacing them or probing them electronically [22].

Interference: At the physical layer, DoS attacks on RFID tags generate and broadcast noise signals through RFID communication channels, causing interference. Noise signals disrupt the RFID signals. ty multiple devices connect and transfer data through cloud platforms for various services, IoT communication is prone to interference [22].

Jamming: Malicious nodes intentionally interfere with valid device connections to perform a DoS attack. Jamming may damage the chronic or discontinuous network. Jamming often happens throughout operations. Fraudulent packets clash with legal ones at the link, dropping the valid ones. Jamming causes data transmission failure, which requires repeated retransmission, draining target nodes' batteries [23].

Malicious Node Injection: In this potent IoT physical layer attack, an attacker inserts a malicious node between two or more legal nodes. The rogue node controls all compromised node data flows and functions. This assault threatens the IoT physical layer. This technique is called a MitM attack because an attacker may set up additional malicious nodes between a sender and a receiver. Malicious nodes take over source-destination data flow [24].

Physical Damage: IoT system hosts are destroyed in this assault. It directly targets service availability. Physical damage to IoT devices or systems poses a severe concern. Unlike other risks, this does not change the IoT system [24].

Social Engineering: Social engineering is a key cyber security and IoT threat. Social engineering targets people's interactions. Its goal is to deceive IoT users into breaching security. An IoT system user is exploited to steal confidential data. Social engineering targets IoT users' privacy [25].

Sleep Deprivation Attack: Sleep deprivation attacks degrade a device's battery. Most gadgets enhance battery life with sleep mode. This exploit boosts power consumption by keeping the victim's node awake, which shuts down the device. It keeps sensor nodes busy by legally interacting with the target node, using more power and depleting the battery [25].

3.2. Network Layer Attacks

The network layer routes and transports data between devices within the IoT network. The most popular attacks are discussed as follows [26-30].

Sybil Attack: By fabricating network node identity, the Sybil attack subverts a genuine node. It involves an adjacent node receiving malicious information. This attacker node houses several network-layer forged/duplicated nodes and pretends to be real. Clone ID is similar to this attack when a malicious node uses many identities on the same physical node. Without installing a node, the assault may take over substantial areas of a network.

Routing Information Attacks: Spoofing or changing routing information can complicate data transmission, create routing loops, send fake error messages, drop or allow traffic, shorten or extend source routes, and partition the network. Data transmission failure might result from traffic decline. Attackers may transmit forged communications throughout the network. Hello attack and black hole attacks are routing information attacks.

Denial of Service (DoS): Malicious nodes send unsolicited messages that are replayed to produce heavy traffic. By flooding the network with fake traffic, the attacker delays service delivery. DoS attacks result from the attacker controlling data packets. DoS attacks impede network access. An IoT network may be overloaded with traffic. When an attacker floods the network with traffic, a DoS assault succeeds.

Man-in-the-Middle (MitM) Attack: This attack is comparable to node injection. The attacker talks with two nodes anonymously and maybe alters their communications. The attacker makes the nodes think they are talking directly. A third user steals a communicating party's key and sends and receives data as the genuine user. The attacker intercepts communication party communications by posing as an open node. RFID technology is at risk. MitM breaches privacy between nodes by attacking communication protocols.

Sinkhole Attack: An attacker deceives genuine nodes by providing fake routing information. User privacy and data confidentiality are affected by sinkhole attacks. It also blocks data transfer by sending packets to the attacker's system.

RFID Spoofing: Attackers intercept data by spoofing RFID reader signals. The attacker sends its data with the RFID tag's original ID to make the victim believe the recorded data is real. Pretending to be the legitimate source allows the attacker to access the IoT system. found that an attacker who spoofs RFID tags reads and captures data. Spoofing compromises integrity, confidentiality, and privacy by giving the attacker unauthorized access to other nodes.

Traffic Analysis Attack: An attacker intercepts RFID data. The attacker gathers network information before initiating this assault—traffic analysis assaults network and application levels. Network layer traffic analysis attacks change file contents, particularly in email exchanges.

RFID Cloning: Accesses critical data via impersonating RFID. RFID mimicking is copying valid RFID data to another RFID tag without requiring a physical simulation. Because the network imitates the attack via the RFID tag, it is easy to distinguish between the original and the compromised tag.

3.3. Application Layer Attacks

The application layer specifies how data is requested and delivered to individual sensor nodes. It also handles the interactions with the end users. There are two categories of application layer attacks: software and encryption.

3.3.1. Software Layer Attacks

Software attacks provide a substantial security threat to automated or computerized systems. These attacks compromise IoT security [31]. This section concerns IoT software attacks.

Worms and viruses: Two characteristics define a virus. It starts by injecting its code into another program's execution path. Second, it replaces executable files with copies of itself. It is vital to remember that not all viruses destroy programs. However, all infections cause difficulties, such as increased memory utilization, overheating, and irregular behavior that may crash computers. Without a host file, worms propagate across computers. IoT software applications cannot prevent worm assaults. Thus, they are a major security risk [32].

Malicious Scripts: Hidden code pieces on hacked websites. IoT devices' Internet security vulnerabilities may be exploited to run malicious scripts on users' apps. Since IoT is constantly linked to the Internet, this applies. The gateway's end-user may be tricked into launching malicious software. This activity may result in data theft or system shutdown [33].

Denial of Service (DoS): Affects the IoT application layer and consumers. Attackers utilize DoS to control the application layer completely and sensitive private data and databases, preventing authorized users from accessing the system. A classic DoS attack prohibits legitimate users from accessing their data while allowing unethical individuals to access it through DoS injection.

Spyware and Adware: Spyware is an attack that monitors an IoT device and Internet activity. Spyware like keyloggers delivers screenshots and keystrokes to remote attackers. This approach steals IDs, credit card numbers, passwords, and sensitive data. Conversely, Adware installs a component on an IoT device that feeds Adson sensor nodes or RFID tags by delivering pop-up adverts or installing browser toolbars [34]. Internet security vulnerabilities like these directly affect IoT security.

3.3.2. Encryption Layer Attacks

The goal of these attacks is to break encryption procedures. Encryption layer attacks include ciphertext-only attacks, known plaintext attacks, chosen plaintext or ciphertext attacks, and MitM attacks [35-37].

Ciphertext-Only Attack: An attacker can access limited encrypted communications. The attacker has no secret key or plaintext data. This attack seeks additional plaintext communications or the private key. A positive guess by an attacker reveals all communications encrypted with the same key.

Known Plaintext Attack: The attacker obtains the ciphertext and plaintext. He must guess the secret key(s) or design an algorithm to decode future communications. This approach lets him crack the cipher instead of only ciphertext assaults. The attacker cannot actively give tailored, cipher-processable secret keys.

Chosen Plaintext or Ciphertext Attack: Chosen plaintext attacks enable hackers to encrypt arbitrary plaintext data to get ciphertext. The attacker tries to get the encryption key or construct a method to decode ciphertext communications with it. The attacker compares ciphertexts with plaintexts. Cracking the secret key will provide target system information. Note that selected ciphertext attacks usually break public key encryption schemes.

Man-in-the-Middle Attack: A covert attacker "joins" IoT communication and intercepts all communications. The attacker produces two secret keys and uses the first to communicate with the path. The attacker encrypts the system response and can decode it with his secret key. The attacker sends multiple fake messages to the target and steals system data using intrusion tactics. This allows the impersonation of real users to access protected data.

4. IoT Challenges

This section discusses the current security challenges in the IoT framework, focusing on the technological and security aspects. The heterogeneous nature of IoT networks makes them vulnerable to various attacks and threats. Technical challenges arise from the ubiquitous nature of IoT networks and the interconnection of heterogeneous devices. These challenges relate to wireless technologies, scalability, energy, and network-distributed nature [38]. Functional rules and regulations are enforced to address these challenges, while security challenges can be addressed through authentication, confidentiality, end-to-end security, and data transmission integrity. Ensuring security throughout all IoT devices' development and operational lifecycle is crucial [39].

4.1. Security Challenges at the Physical Layer

B. Fu [40] identified three security challenges at the physical layer. The first challenge is the effect of attenuation on wireless signals. Unwanted signals from extraneous sources weaken the strength of the signals sent by sensor nodes. The second challenge is that IoT nodes are installed in both external and outdoor environments, making them vulnerable to devices' physical attacks. The third challenge is the regular physical movements of IoT nodes.

The physical layer handles data collection. The analysis of both technological and security attacks at the physical layer is presented in Table 1.

Table 1. *Technological and Security challenges in IoT Physical Layer.*

Components	Features	Technological Challenge	Security Challenge	Attacks Type
RFID	Unique Identification Tags	Tracking, DoS, and Repudiation	Alteration, spoofing, and deletion	Counterfeiting and Eavesdropping
Sensors	Sensors and Actuators	Exhaustion and Sybil	Routing and Flooding	Tampering and Jamming.
WSNs	Receivers, Radios, and Receivers	Misconfiguration and Access point failure	Unfairness, Hijacking (equipment), loss of signal and hacking	Malicious attacks
Near Field Communication (NFC)	Extension of RFID (NFC Tag)	Complex ecosystem, DoS	Lack of Infrastructure	Eavesdropping, collision, and MitM attacks

The table displays potential security threats in physical layer technologies. Techniques like stenography, watermarking, encryption, intellectual property, and multimedia collection can address these challenges. Attackers can also violate confidentiality through replay attacks, which involve device modification or identity theft. Confidentiality and privacy are crucial security challenges at the physical layer [39].

4.2. Security Challenges at the Network Layer

The IoT network layer faces numerous technological and security challenges due to its technical aspects, such as communication and data routing. These challenges include eavesdropping, damage, denial of service attacks, virus invasion, MitM attacks, illegal access, and confidentiality. The heterogeneous nature of IoT networks makes interoperability and network coordination critical, resulting in separate security threats. Major security issues include authenticity, confidentiality, network availability, and integrity [41]. Table 2 analyzes both technological and security attacks in the network layer.

Table 2. *Technological and Security challenges in the IoT Network Layer.*

Components	Features	Technological Challenge	Security Challenge	Attacks Type
Bluetooth	Spectrum (Frequency hopping)	Bluesnarfing, link latency, and Bluejacking	DoS, Eavesdropping	Snarf attack, backdoor attack, and bluebugging.
ZigBee	Radio and Microcontroller	Data Manipulation, Packet decoding	Traffic sniffing, data injection, eavesdropping, and hacking	Scapy, Killerbee and Killerbee stinger.
LTE	User Equipment (UE) and Evolved Packet Core (EPC)	Fake LTE station, Data caching, Framing and Clickjacking	Eavesdropping, confidentiality, and authenticity	DDoS/DoS Attacks, Phishing Attacks, and MitM attacks.
NB-IoT	Arduino footprint	The control server comprised Firmware corruption and embedded malware	Device hacking, default password hacking, and authorization	DDoS and MitM attacks.
5G	Spectrum beyond 6GHz, Advanced MIMO and Beamforming	Deployment of heterogeneous hardware and software and Misbehaving devices	Data exposure, Data inadequacy, and Unauthorized attacks	DoS, identity attacks, and phishing attacks.

The table lists the IoT network technologies, features, technological challenges, security threats, and possible exploits against IoT systems implemented using any of these technologies.

4.3. Security Challenges at the Application Layer

The application layer deals with the end users' interaction with IoT applications. The application layer consists of different applications and software, each with different security

features and mechanisms, making the unification of all IoT devices in this layer quite difficult to develop [41]. Table 3 presents the analysis of both technological and security attacks at the application layer.

Table 3. Technological and Security Challenges in IoT Application Layer.

Components	Features	Technological Challenge	Security Challenge	Attacks Type
Smart City	Street lighting, good land use, waste, and water distribution management	Organized crime, terrorist groups, commercial events, service disruption, and natural events	Cybercrime, privacy invasion, eavesdropping and website defacements	Smart city DoS and identity attacks.
Smart Healthcare	Smart Healthcare cards	Unintentional action and Insider misuse	Hacking	Cyber-attacks, Internal attacks.
Smart Transportation	Traffic Control and Parking	Privacy details	Security plagued	Cyber-attacks and Smart DoS.
Smart Government	e-government, Economic development	Physical security and Information Manipulation	Eavesdropping, privacy invasion, Cybercrime, and website defacements	DoS and Malicious attacks.
Smart Grid	Smart energy and Smart meter	Customer security and Physical security	Trust and Hacking	Malicious attacks.

The application layer faces challenges in data security, user privacy, data destruction, device protection, and software intellectual property. Challenges include interoperability, privacy protection, confidentiality, policies, and reliability. These issues stem from a lack of security policies and standards for data communication between connected devices.

5. Proposed Unified Security Framework for IoT

This section presents a unified federated security framework for IoT, focusing on user identification to prevent attacks and threats across various network layers.

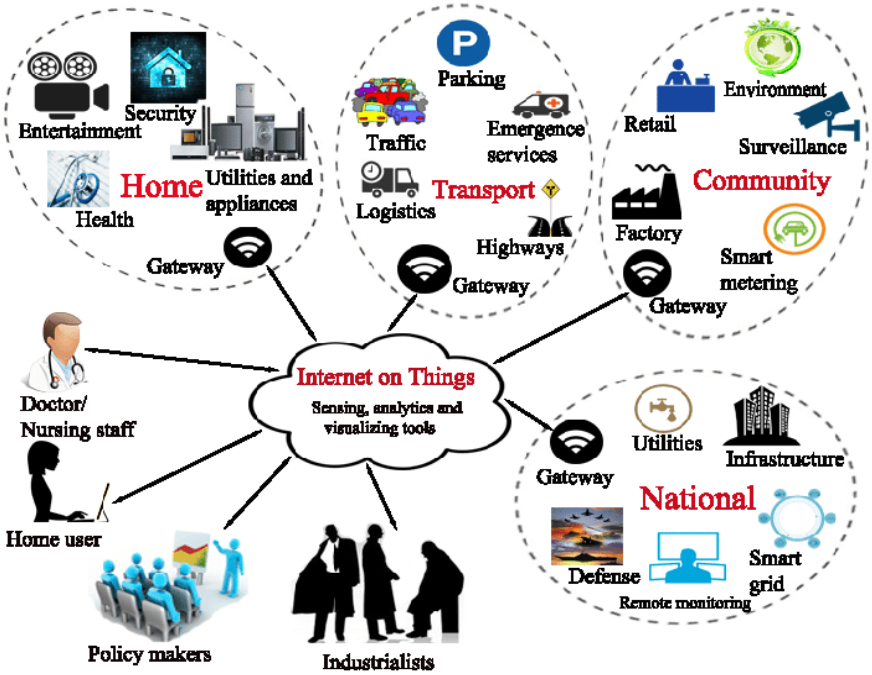

Figure 3. A Unified Federated Security Framework for IoT Network Scenario.

The proposed unified federated identity-based security architecture for the three-layer IoT network allows users from one security layer to access resources in another without another user's account. The architecture relies on trust between the three levels, with users enrolling credentials with the authentication server at the physical layer and trusting its claims. Federated identification in online security is comparable to this IoT method. The federated identity provider builds, stores, and manages device identity information by providing authentication services to dependent layers and applications. In other domains, IoT devices must be authorized.

Figure 4 depicts the proposed framework's detailed communication process.

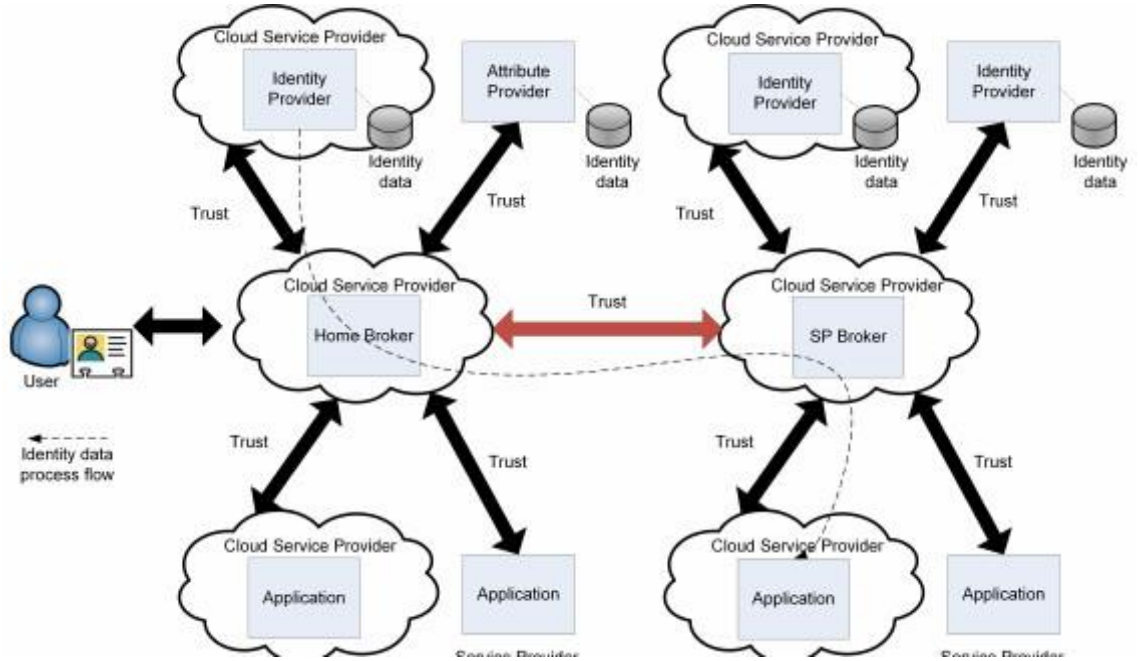

Figure 4. *Federated Identity Management Process.*

6. IoT Security Countermeasure

This section discusses the countermeasures for the attacks presented in Section 4. It highlights methods for preventing attacks at each IoT layer, which enables users to identify solutions to various security threats against IoT networks.

6.1. Countermeasures Against Physical Layer Attacks

Node tampering attacks can be mitigated by using tamper-proof hardware, designing high-quality, physically secure devices, and implementing data encryption and authentication to guarantee data confidentiality. Other solutions include hashing, message authentication codes, and cyclic redundancy checks. Interference in IoT systems can be addressed through proper installations, auditing frequency spectrums, and gaining commitment from suppliers [42]. Pilot installations are recommended to test system performance and review performance regularly. In [43] multi-hop multi-channel topology control can reduce the impacts of co-channel interference in wireless system networks. Jamming attacks at the IoT physical layer can be mitigated through game-based approaches, such as a colonel blotto game that detects jamming attacks by increasing the number of bits assigned to several nodes. The authenticity of nodes and data integrity are crucial security measures to curb malicious node injection attacks in the IoT physical layer.

Physical damage attacks aim to directly destroy or cause damage to the IoT device or system's main host. To prevent such attacks, avoiding security breaches in an IoT network and providing data confidentiality is important. Researchers have suggested good countermeasures against IoT physical level attacks, and proper risk assessment policies should be analyzed and implemented in IoT industries and services. Social engineering attacks can be mitigated by deploying robust data privacy by IoT end users [1]. Users should be cautious when sharing sensitive information in emails and avoid sending private and vital information over the Internet. Organizations should provide security training and awareness to expose personnel to the dangers of social engineering. Sleep deprivation attacks can be prevented by proper authentication of IoT devices. Devices must recognize and grant access only to authorized users with valid credentials, and

devices not authenticated should not be allowed access or connection to other nodes within the IoT system. Strong authentication protocols, such as biometrics, can be employed for better security assurance and protection against sleep deprivation attacks [10].

6.2. Countermeasures Against Network Layer Attacks

Sybil attacks are a common issue in IoT systems, which can be detected and blocked by detecting and blocking fake accounts after a user signs in. Other approaches include using behavioral thumb rules to determine who gains access to the network, monitoring accounts, frequency of posts, interactions, IP addresses, devices logging into the network, and time of activity. Routing Information Attacks can be prevented by encrypting routing tables, using strong encryption mechanisms like Advanced Encryption Standard (AES), and restricting network authorization to authorized and authenticated users [27]. Man-in-the-middle attacks can be prevented by restricting network authorization to authorized and authenticated users, using cloud-assisted security systems, and implementing Secure Sockets Layer (SSLs). Sinkhole Attacks can be prevented by security-aware ad hoc routing, using Particle Swarm Optimization to prevent insider attacks. Other countermeasures include hop count monitoring, node usage monitoring, network flow information techniques, and message digest algorithms.

Traffic Analysis Attacks can be mitigated by analyzing data in transmission before sending it for processing. Routing security is employed for data confidentiality among trusted devices or environments, and distributing pseudo-random values across the network in insecure environments can help mitigate these attacks. RFID cloning can be cured by using a proper authentication technique or mechanism that provides mutual authentication between the tag and reader during data transmission. Incorporating physically unclonable functions into the network can also help prevent RFID cloning attacks. However, it is crucial to implement these measures to protect IoT networks from potential threats such as impersonation and impersonation [42].

6.3. Countermeasures Against Application Layer Attacks

The security measures at the application layer are classified into software attack countermeasures and encryption attack countermeasures.

6.3.1. Software Attacks Countermeasures

In summary, preventing virus and worm attacks in IoT systems and applications requires using antivirus programs, sound security policies, and regular scanning of IoT applications. Malicious scripts can lead to data loss and availability, and licensed anti-malware programs can be employed to prevent damage. L. Lei et al. modeled and evaluated malicious attacks against IoT protocols, suggesting using an Intelligent Digital Network (IDN) to control connected home appliances and protect sensitive information. DoS attacks at the application layer target availability and authentication, and countermeasures include router controls, distributed packet filtering, aggregate congestion control, firewalls, resource multiplication, and dynamic en-route filtering [31]. Strong encryption mechanisms like the Advanced Encryption Standard can be used to prevent overwriting reoccurrence addresses. Spyware and Adware attacks are similar to viruses and worms but with little improvement [32]. Countermeasures include installing pop-up blockers on IoT devices, installing antispyware/anti-adware programs, implementing personal software firewalls, and using intrusion detection software. Biometric information-based secure methods are also effective for protecting smart IoT devices. Implementing these measures can help protect IoT systems and applications from potential threats.

6.3.2. Encryption Attacks

During encryption algorithm design, protecting against ciphertext-only attacks, known plaintext attacks, and chosen plaintext or ciphertext attacks is crucial. Well-prepared and reviewed ciphers are less vulnerable to these attacks. Techniques like an attack on two-time pads, thorough encoding, and frequency analysis can be effective against modern ciphers. Countermeasures can be applied to all types of cryptanalysis attacks. Strong mutual authentication techniques before secret data transmission can help defend against man-in-the-middle attacks. Public keys from known databases can be used instead of encryption keys from one side of communication, possibly from the attacker [14].

7. Future Direction

IoT has experienced rapid development and is used in various applications, including health, smart transportation, and environmental monitoring. However, security threats persist, hindering the growth and maturity of IoT technology. To enhance security and maturity, future research should address the following issues [39, 41-43]:

1. *Architecture Standards:* IoT security control is challenging due to the lack of standard algorithm design and implementation policies. An IoT network consists of different devices, services, and protocols, making it essential for a “federated architecture” with internal autonomy or a unified unit. A universal standard should govern the integration process of smaller IoT frameworks into larger ones, such as smart cars and smart homes.
2. *Identity Management:* IoT devices identify themselves by exchanging credentials, making the entire

network and devices vulnerable to attacks like MitM and eavesdropping. To address this challenge, a dedicated and predefined identity management unit can monitor device connections in IoT networks, using cryptography and other techniques to prevent identity theft.

3. *Session Layer:* The three layers of IoT do not accommodate opening, closing, and session management among devices. Therefore, it is crucial to introduce session layer protocols that facilitate communication among devices across different sessions in the IoT network. Additionally, the IoT architecture should include a distinctive session layer to handle connections, protocols, and sessions among communicating heterogeneous devices.

8. Conclusion

The IoT has been a popular topic of study over the last decade due to its potential to impact many aspects of human existence significantly. The IoT necessitates the interoperability of many devices running on a wide variety of platforms and communicating via a wide variety of technologies at several levels (including the physical network and application layer). This leaves the framework vulnerable at every level to a variety of potential dangers and assaults. A single security framework for the IoT remains an unattainable goal due to a lack of significant studies. Thus, dealing with IoT security threats is crucial to creating a unified security architecture. The suggested unified IoT framework summarized the state of the art in terms of IoT attack frameworks and highlighted problems at various IoT levels. The paper's taxonomy of attacks will be useful in determining what kinds of security risks and assaults may occur at different tiers of an IoT network. Appropriate countermeasures against vulnerabilities at each level of the IoT network were also spelled out in the proposed unified federated security architecture for IoT.

Abbreviations

IoT	Internet of Things
KMS	Key Management Systems
(SOA)	Service-Oriented Architecture
CoAP	Constrained Application Protocol
E2E	End-to-End
DoS	Denial of Service
DDoS	Distributed Denial of Service
SDN	Software-Defined Networking
NFV	Network Function Virtualization
DTLS	Datagram Transport Layer Security
MitM	Man-in-the-Middle
IDN	Intelligent Digital Network
AES	Advanced Encryption Standard
SSLs	Secure Sockets Layer

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] W. T. Sung, I. V. Devi, S. J. Hsiao, and F. N. Fadillah, "Smart Garbage Bin Based on AIoT," Intell. Autom. Soft Comput., vol. 32, no. 3, pp. 1387–1401, 2022, https://doi.org/10.32604/IASC.2022.022828

[2] M. Jingyao, Z. Gang, and Z. Ling, "Governance mechanisms implementation in the evolution of digital platforms: a case study of the Internet of Things platform," R D Manag., vol. 52, no. 3, pp. 498–516, 2022, https://doi.org/10.1111/radm.12494

[3] K. P. Seng, L. M. Ang, and E. Ngharamike, "Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks," Int. J. Distrib. Sens. Networks, vol. 18, no. 3, 2022, https://doi.org/10.1177/15501477211062835

[4] P. Title and T. Name, "Presentation Schedule," pp. 1–13, 2023, https://doi.org/10.1109/globconet56651.2023.10150157

[5] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges," Sci. African, vol. 20, no. March, p. e01638, 2023, https://doi.org/10.1016/j.sciaf.2023.e01638

[6] A. A. Pise et al., "Enabling Artificial Intelligence of Things (AIoT) Healthcare Architectures and Listing Security Issues," Comput. Intell. Neurosci., vol. 2022, pp. 1–14, 2022, https://doi.org/10.1155/2022/8421434

[7] A. Bano, I. Ud Din, and A. A. Al-Huqail, "AIoT-Based Smart Bin for Real-Time Monitoring and Management of Solid Waste," Sci. Program., vol. 2020, 2020, https://doi.org/10.1155/2020/6613263

[8] A. Okubanjo, A. Okandeji, and E. Daniel, "Smart Bin and IoT: A Sustainable Future for Waste Management System in," J. Sci., vol. 37, no. 1, 2023, https://doi.org/10.35378/gujs.1254271

[9] M. Tauseef, M. R. Kounte, A. H. Nalband, and M. R. Ahmed, "Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 4, pp. 885–895, 2023, https://doi.org/10.14569/IJACSA.2023.0140498

[10] A. R. Khan, I. Abunadi, B. Alghofaily, H. Ali, and T. Saba, "Automatic Diagnosis of Rice Leaves Diseases Using Hybrid Deep Learning Model," J. Adv. Inf. Technol., vol. 14, no. 3, pp. 418–425, 2023, https://doi.org/10.12720/jait.14.3.418-425

[11] J. P. S. Piest, Y. Masuda, and M. E. Iacob, "Digital Architectures Under Society 5.0: An Enterprise Architecture Perspective," Lect. Notes Bus. Inf. Process., vol. 466 LNBIP, no. August, pp. 5–24, 2023, https://doi.org/10.1007/978-3-031-26886-1_1

[12] P. Singhal, P. Sharma, and D. Arora, "An approach towards preventing IoT based sybil attack based on contiki framework through cooja simulator," Int. J. Eng. Technol., vol. 7, no. 2.8, p. 261, 2018, https://doi.org/10.14419/ijet.v7i2.8.10421

[13] V. K. Patil, V. R. Pawar, S. P. Kulkarni, T. A. Mehta, and N. R. Khare, "Real Time Emotion Recognition with AD8232 ECG Sensor for Classwise Performance Evaluation of Machine Learning Methods," Int. J. Eng. Trans. C Asp., vol. 36, no. 6, pp. 1040–1047, 2023, https://doi.org/10.5829/ije.2023.36.06c.02

[14] Q. Zhang et al., "Wearable Triboelectric Sensors Enabled Gait Analysis and Waist Motion Capture for IoT-Based Smart Healthcare Applications," Adv. Sci., vol. 9, no. 4, pp. 1–13, 2022, https://doi.org/10.1002/advs.202103694

[15] D. Muhammed, E. Ahvar, S. Ahvar, and M. Trocan, "A User-friendly AIoT-Based Crop Recommendation system (UACR): concept and architecture," Proc. - 16th Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2022, no. April 2023, pp. 569–576, 2022, https://doi.org/10.1109/SITIS57111.2022.00091

[16] Y. J. Lin, Y. C. Chen, J. Y. Zheng, D. W. Shao, D. Chu, and H. T. Yang, "Blockchain-Based Intelligent Charging Station Management System Platform," IEEE Access, vol. 10, no. September, pp. 101936–101956, 2022, https://doi.org/10.1109/ACCESS.2022.3208894

[17] Z. Zhang, F. Wen, Z. Sun, X. Guo, T. He, and C. Lee, "Artificial Intelligence ‐ Enabled Sensing Technologies in the 5G/Internet of Things Era: From Virtual Reality/Augmented Reality to the Digital Twin," Adv. Intell. Syst., vol. 4, no. 7, p. 2100228, 2022, https://doi.org/10.1002/aisy.202100228

[18] Z. Boulouard, M. Ouaissa, M. Ouaissa, and S. El Himer, AI and IoT for Sustainable Development in Emerging Countries, vol. 105, no. January. 2022. https://doi.org/10.1007/978-3-030-90618-4

[19] A. Chauhan, M. Bahadir, and B. Teichgräber, "Sc Pt Ac," Water Res., 2017, [Online]. Available: http://dx.doi.org/10.1016/j.watres.2017.06.034

[20] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation," Secur. Commun. Networks, vol. 2018, 2018, https://doi.org/10.1155/2018/7178164

[21] M. A. R. Abdeen, I. A. Nemer, T. R. Sheltami, M. H. Ahmed, and M. Elnainay, "A Hierarchical Algorithm for In-city Parking Allocation Based on Open Street Map and AnyLogic Software," Arab. J. Sci. Eng., 2023, https://doi.org/10.1007/s13369-022-07528-4

[22] P. Knebel, "An Artificial Intelligence of Things based Method for Early Detection of Bark Beetle Infested Trees," Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform., vol. P-328, pp. 111–120, 2022.

[23] K. Ning, "Data-driven artificial intelligence techniques in renewable energy system," no. 1999, 2021, [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/132891/1263357737-MIT.pdf?sequence=1&isAllowed=y

[24] C. Chakraborty, M. R. Khosravi, S. H. Ahmed, and J. J. P. C. Rodrigues, "Guest Editorial AIoMT-Enabled Medical Sensors for Remote Patient Monitoring and Body-Area Interfacing: Design and Implementation, Practical Use, and Real Measurements and Patient Monitoring," IEEE J. Biomed. Heal. Informatics, vol. 26, no. 12, pp. 5769–5771, 2022, https://doi.org/10.1109/JBHI.2022.3220267

[25] A. H. Hassan, R. bin Sulaiman, M. A. Abdulgabber, and H. Kahtan, "Balancing Technological Advances with User Needs: User-centered Principles for AI-Driven Smart City Healthcare Monitoring," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 3, pp. 365–376, 2023, https://doi.org/10.14569/IJACSA.2023.0140341

[26] Y. J. Lin, Y. C. Chen, J. Y. Zheng, D. Chu, D. W. Shao, and H. T. Yang, "Blockchain Power Trading and Energy Management Platform," IEEE Access, vol. 10, no. June, pp. 75932–75948, 2022, https://doi.org/10.1109/ACCESS.2022.3189472

[27] M.-L. Tham, Y. J. Wong, B.-H. Kwan, X. H. Ng, and Y. Owada, Artificial Intelligence of Things (AIoT) for Disaster Monitoring using Wireless Mesh Network, vol. 1, no. 1. Association for Computing Machinery, 2023. https://doi.org/10.1145/3584871.3584905

[28] M. Wang, F. Zhang, L. Ma, and Y. Tian, "Adaptive VR Video Data Transmission Method Using Mobile Edge Computing Based on AIoT Cloud VR," J. Sensors, vol. 2022, 2022, https://doi.org/10.1155/2022/2022586

[29] P. Mishra and S. Shrivastava, "Cloud AIoT based Smart Wheelchair using Module for Social Distancing, Temperature Monitoring, and Oximeter Module," … J. Inf. Technol., vol. 7, no. 5, pp. 29–35, 2021, [Online]. Available: http://ijitjournal.org/volume-7/issue-5/IJIT-V7I5P6.pdf

[30] N. Chumuang, K. Kocento, M. Ketcham, and A. Farooq, "Design and Prototyping of Intelligent Bin by Using AIoT," Int. Conf. Cybern. Innov. ICCI 2022, no. February, 2022, https://doi.org/10.1109/ICCI54995.2022.9744170

[31] L. Lei, Y. Tan, K. Zheng, S. Liu, K. Zhang, and X. Shen, "Deep Reinforcement Learning for Autonomous Internet of Things: Model, Applications and Challenges," IEEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1722–1760, 2020, https://doi.org/10.1109/COMST.2020.2988367

[32] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the IoT edge based on sparse representation," Glob. IoT Summit, GIoTS 2019 - Proc., pp. 1–6, 2019, https://doi.org/10.1109/GIOTS.2019.8766388

[33] M. Y. Hiou, "AIoT-Based Quality Control Production Line," no. December, 2022, https://doi.org/10.13140/RG.2.2.32848.58882/2

[34] A. Kumar, "AIoT Technologies and Applications for Smart Environments," AIoT Technol. Appl. Smart Environ., no. December 2022, 2022, https://doi.org/10.1049/pbpc057e

[35] S. E. Najafi, H. Nozari, and S. A. Edalatpanah, "Artificial intelligence of things (AIoT) and industry 4.0-based supply chain (FMCG Industry)," A Roadmap Enabling Ind. 4.0 by Artif. Intell., no. December, pp. 31–42, 2022, https://doi.org/10.1002/9781119905141.ch3

[36] Y.-J. Lin, C.-W. Chuang, C.-Y. Yen, S.-H. Huang, J.-Y. Chen, and S.-Y. Lee, "An AIoT Wearable ECG Patch with Decision Tree for Arrhythmia Analysis," 2019 IEEE Biomed. Circuits Syst. Conf., no. October 2019, pp. 1–4, 2019, https://doi.org/10.1109/biocas.2019.8919141

[37] G. Ng et al., "Amalgamation of smart AIoT based construction site monitoring with robotics: viAct's extended horizon," no. November, 2021, [Online]. Available: https://www.researchgate.net/publication/355960096

[38] N. Cam-Winget, A.-R. Sadeghi, and Y. Jin, "Invited - Can IoT be secured," Proc. 53rd Annu. Des. Autom. Conf. - DAC '16, pp. 1–6, 2016, https://doi.org/10.1145/2897937.2905004

[39] H. M. Zahid, "A Framework for Identification and Classification of IoT Devices for Security Analysis in Heterogeneous Network," Wirel. Commun. Mob. Comput., vol. 2022, no. Idc, 2022, https://doi.org/10.1155/2022/8806184

[40] K. Ding, "Smart steel bridge construction enabled by BIM and Internet of Things in industry 4.0: A framework," ICNSC 2018 - 15th IEEE Int. Conf. Networking, Sens. Control, pp. 1–5, 2018, https://doi.org/10.1109/ICNSC.2018.8361339

[41] A. Kumar, K. S. Kumar, M. Sharma, C. Menaka, R. Naaz, and V. Vekriya, "Machine learning in molecular communication and applications for health monitoring networks," Soft Comput., 2023, https://doi.org/10.1007/s00500-023-08400-9

[42] M. C. Chiu, W. M. Yan, S. A. Bhat, and N. F. Huang, "Development of smart aquaculture farm management system using IoT and AI-based surrogate models," J. Agric. Food Res., vol. 9, no. August, p. 100357, 2022, https://doi.org/10.1016/j.jafr.2022.100357

[43] S. Praharaj, B. B. Mishra, U. S. Mishra, R. R. Panigrahi, and P. C. Mishra, "Role of Service Automation on Guest Experience of Hotel Industry," Tour. Hosp. Manag., vol. 29, no. 2, pp. 265–278, 2023, https://doi.org/10.20867/thm.29.2.11