Communication in Physical Sciences 2023, 9(4): 784-800

IoT and Network Security: Researching Network Intrusion and Security Challenges in Smart Devices

Precious Ogechi Ufomba* & Ogochukwu Susan Ndibe.
Received: 24 June 2023/Accepted: 03 September 2023/Published: 19 September 2023

Abstract :*The sheer proliferation of Internet of Things (IoT) devices across consumer, industrial, and critical infrastructure categories has brought with it a level of access and automation that has never been seen before. This increase, however, has brought about an even greater attack surface, with major security holes given the resource limitations, diversity, and non-standardization that come with an IoT environment. This paper examines the diverse security concerns raised by IoT networks such as threats to networks intrusion, network-level attacks as well as threats to IoT devices and some of the new forms of attacks that have evolved to attack smart devices. It rates the traditional and IoT-dedicated intrusion detection methods, lightweight encryption methods, and the place of AI and machine learning in detecting threats. Future-based initiatives like blockchain-based authentication, zero-trust architecture, and edge/fog computing to provide real-time defense are also discussed in the paper. Lastly, it identifies the significance of developing regulatory frameworks and offers practical suggestions to stakeholders as a way of ensuring the successful protection of IoT ecosystems. The study will serve to enhance the growth of innovative, flexible, and scalable security measures in the changing IoT environment.*

Keywords: IoT, intrusion, smart devices, encryption, ML, anomalies, zero-trust, blockchain, fog, standards

Precious Ogechi Ufomba
Cybersecurity, Katz School of Science and Health, Yeshiva University, New York, United States
Email: ufombapreciousoge@gmail.com

Ogochukwu Susan Ndibe
Cybersecurity & Information Assurance, University of Central Missouri, Warrensburg, Missouri, United States
Email: Sndibe7@gmail.com

1.0 Introduction

The concept of Internet of Things (IoT) can be described as an interconnection of physical objects such as consumer appliances to industrial-grade sensors and actuators that sense, transmit, and respond to data without explicit human control (Gurunath et al., 2018; Flauzac et al., 2015). The gadgets use the benefits of diverse communication technologies such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, and cellular IoT protocols. With time, the number of active IoT devices increased accordingly as tens of billions saw active IoT devices in the early 2020s and upward of 75 billion are expected by the year 2025 as the global spread of IoT devices sees explosive growth (Chaabouni et al., 2019). IoT ecosystem extends to consumer smart homes and the global market of wearable health-trackers, smart city infrastructure (traffic lights, environment sensors, surveillance, etc.), industrial Internet of Things (IIoT) solutions in manufacturing, power grids, and logistical systems. This heterogeneity has changed the digital space, creating new epochs of endpoint categories, creating massive distributions of sensor data, and pushing the data creation and data barter towards distributed environments.

IoT proliferation has changed the nature of network architecture: there may be highly resource-constrained (low CPU, minimal RAM and energy) nodes (endpoints) which are connected through special protocols and communicate with the edge gateway and with

the cloud. This redesigns the topology and dimension of present-day networks. In the sphere of utilities, IoT devices are already integrated into sectors with high reliability and latency requirements, e.g., medical monitoring, industrial control, mathematical and statistics in machine learning and intelligent traffic control, where reliable, real-time, and security are vital (Hamza et al., 2020; Hassan, 2019: Abolade 2023).

Smart home technologies such as thermostats, lighting controls, security cameras, and smart speakers as well as health wearables are finding their way more and more into daily life, a trend that started in the consumer sector and continues to intensify. One area that has developed rapidly is with sensors helping to do predictive maintenance and optimize the supplychain and make operations resilient called Industrial IoT (IIoT), and this has increased in areas like manufacturing, automation, the energy distribution sector, transport, farming, and agriculture (Alotaibi, 2023; Awotunde et al., 2023). IIoT models give way to intertwining legacy ICS/SCADA infrastructure and state-of-the-art edge computing devices to form hybrids that destroy the familiar security demarcations.

Such mass adoption has greatly increased the attack surface in the world. As an example in the healthcare sector, studies show that more than half of connected healthcare devices have critical risks and support by vendors in correcting them is not available in many cases (Alotaibi, 2023). Similarly, thousands of sensors and actuators can be involved in proposed smart manufacturers or logistics systems; these systems present the possibility of lateral intrusions, the compromising of supplychain, or exfiltration of data. The growing popularity of IoT also increases the desire to attack IoT devices over a specific target outlet of a medical or home system, ransomware microbotnet DDoS, and nationstate reconnaissance.

The old-fashioned enterprise networks are all based on well-provisioned endpoints, which might include desktops, servers, laptops and might be linked with centralized routers, firewalls which therefore might be configured as highly restricted security structures. These networks have expanded to be more of a complex ecosystem with resource-constrained devices, the middle nodes or gateways, such as the mesh network and cloud-connected platforms, which are the result of the Internet of Things (IoT) (Kim et al., 2023; Nguyen et al., 2021). Access to information is via lightweight protocols, typified by MQTT, Constrained Application Protocol (CoAP over DTLS), Zigbee and Z-Wave that have associated constraints and threat models. The diverse nature of protocols complicates the process of making common policy security with devices joining and leaving networks dynamically as in mobile or ad-hoc networks. The homogeneous networks that make up an industrial environment are worse: sensors streaming information to the edge ML platforms, actuators connected to the legacy ICS bus, and human interface devices working on the Wi-Fi or wired LAN, are all interconnected, which are neither isolated nor have coordinated policies (Awotunde et al., 2023). The division between convenient technology (OT) and other IT systems networks is becoming more permeable, which opens the opportunity of cross-space intrusions, unconspicuous attacks, and continuous threats without the upholding of security posture at all levels being consistently met.

The research aims and objectives are to examine in detail the security issues brought by IoT devices and their networks, specifically, the network intrusion methods and vulnerabilities endangering smart devices. Besides this, the study will seek to understand the flaws in the current security systems such as light traffic encryption, authentication, and intrusion detection systems with the view of

establishing areas where they have failed in defending the IoT networks. Moreover, the study will offer practical solutions to the stakeholders which can be other device manufactures, network operators, and policymakers so that they can take efforts in addressing the security risks and eventually facilitate the establishment of resilient networks of IoT. With these purposes, the research will be able to contribute to the development of safe IoT implementation that will be able to competently address the increasing need of interconnected smart devices.

2.0 Security Challenges in IoT Networks

Internet of Things (IoT) has redefined the current technology so that an interconnected device can collect, share, and process information without any human intervention. The uses of IoT are growing by leaps and bounds, including smart homes and industrial automation. Yet, this development has come with serious security threats, especially about network intrusion and cyber threat.

Securities in the fields of the IoT networks are associated with the features of connected devices, as they have limited computing resources, non-homogeneous architecture, and are widely used in critical infrastructure environments. Unlike the typical IT systems and devices, several IoT devices lack an element of security control, and they are highly subjected to being manipulated. The issue of IoT security non-standardization is one of the most significant ones. Designers focus more on cost and functionality and less on security where there exists weak default settings, unencrypted traffic as well as inadequate authentication measures. More than that, the total number of IoT devices (which already exceeds 30 billion and is expected to reach to 75 by 2025) represents an exploitable playing field to cybercriminals (Sagduyu, 2019). The next significant issue is the impossibility of employing the same security measures in IoT settings as in the past. Intrusion detection systems (IDS), firewalls and antivirus, which are common in the enterprise network are not effective to use with IoT as they limit resources. Majority of IoT devices are frequently powered by lightweight operating systems having little processing power, making it impossible to implement complicated encryption algorithms or threat detection in real-time. In addition, these IoT networks mostly involve using wireless communication protocols like Zigbee, Bluetooth Low Energy (BLE) and Wi-Fi, and are prone to eavesdropping, signal jamming or man-in-the-middle (MitM) attacks (Issa et al., 2023).

In contrast to conventional computing systems, the IoT devices tend to feature a vulnerable security system, and thus, they can make excellent targets of attackers. The dynamic nature of IoT ecosystems is in contrast to scenarios in which IT networks are static and only require maintenance of their existing constituents (Alam et al., 2021). It is hard to ensure that security policies remain stable, so there are loopholes that the attackers can take advantage of. Furthermore, a large number of IoT devices are unsupervised because they are in an industrial sensor or the smart city infrastructure, where it becomes a serious threat to physically tamper with them. If the device is not physically secured, attackers may extract cryptographic keys, change firmware or add malicious parts of hardware (Pilati et al., 2023).

In achieving this, researchers and industry players ought to come up with customized security solutions to IoT networks. Lightweight encryption technology, blockchain-based authentication, and artificial intelligence-based identification of anomalies are prospective solutions. However, mass adoption will demand the cooperation of the manufacturing industry, policymakers, and security professionals to implement definite security standards.

2.1 Inherent Vulnerabilities of IoT Devices

There is a long list of intrinsic weaknesses that characterize IoT devices based on design vulnerabilities at the hardware and software level.

Restricted computing capabilities: Most IoT gadgets, including sensors and wearables, also use microcontrollers that have low computing power. It reduces their options to use robust encryption standards such as AES-256 or RSA, which exposes transmitting data to interception (Kolias et al., 2017). As an illustration, researchers were able to show that insecure encryption can be used by attackers to hijack unencrypted voice commands or by imposing data that is not supported by the sensor (Zhang et al., 2020).

Weaknesses of firmware and poor update processes: Most of the IoT gadgets are deployed with outdated or firmware that is poorly hardened. The updating channel is often not secure, or firmware cryptographic signing lacks as a result of which the device is vulnerable to malicious injections of firmware or permanent compromise (Rajgure, 2023). Unless regularly patched, known issues are always subject to exploit (As n-day mining study by Cui and Pantoga note, mobile embedded devices in the industrial sector tend to be unpatched en masse) (Meneghello et al., 2019).

Weak authentication: Usually devises come either with non-existent authentication or poor authentication (e.g. the default choice of password on the device is either passwords (e.g. “admin”, “1234”) or does not require any authentication). In most cases, end-users never change such credentials, and the authentication can be broken by either brute-force or automated tools. The primary focus of the mass compromise attacks is still on the advance payments on the IoT devices, such as the botnet attacks with Mirai (Neshenko et al., 2019). It also explores the issue with a poor authorization control (Meneghello et al., 2019).

Exposure, vulnerabilities to cloning of devices: Most of the IoT devices are publically installed or left exposed, in unsecured, remote areas, exposed to potential physical tampering, opening, reverse engineering, or hardware hacks. This may allow them to implement malicious firmware or steal stored credentials or duplicate identifiers of devices (Kolias et al., 2017).

In combination, all these weaknesses make the IoT endpoints extremely vulnerable to infections, manipulation, and exploitation and introduce a significantly increased risk profile to the connected networks.

Table 1 provides a structured overview of the major categories of inherent vulnerabilities commonly found in IoT devices. These include limitations such as restricted processing power that prevent the implementation of strong encryption protocols, the use of outdated or poorly maintained firmware, insecure or absent update mechanisms, and the persistence of hardcoded or default credentials. In addition, the table highlights physical security risks—particularly in public or semi-public deployments—as well as the use of insecure communication protocols that transmit data without encryption. Weak authentication schemes and poor interoperability practices further compound the risk, especially when devices integrate with unvetted third-party services. Each entry in the table presents a specific vulnerability, a concise description, and a real-world example to illustrate how that vulnerability manifests in practice. This summary underscores the systemic nature of IoT security challenges and the need for comprehensive mitigation strategies at both the device and network levels.

2.2 Types of Network Attacks in IoT Environments

Various network-based attacks against IoT networks have a wide range of vulnerabilities and, therefore, are based on protocol-, infrastructure-, or device-level weaknesses.

Spoofing Attacks

Spoofing is a way of impersonating a trusted device through IP address falsification, MAC

addresses, or protocol identifiers. Examples of it are the IP spoofing, ARP spoofing (ARP poisoning), and DNS spoofing. These attacks favor higher level threats such as session hijacking, man in the middle (MITM) or eavesdropping (Van Der Merwe et al., 2018; Li et al., 2018). ARP spoofing can be used to capture or modify the information moving along networks locally, whereas DNS spoofing refers to redirecting routes towards malicious resources (Van Der Merwe et al., 2018).

Table 1 present different cartegories of thet systematically describes common security weaknesses found in Internet of Things (IoT) devices. It provides specific examples for each vulnerability, ranging from limited processing power and outdated firmware to insecure communication protocols and insufficient physical security, illustrating how these design flaws contribute to the overall insecurity of IoT ecosystems.

Table 1: Inherent Vulnerabilities of IoT Devices

Vulnerability	Description	Example
Limited Processing Power	Most IoT devices rely on low-power microcontrollers, making it difficult to implement strong encryption or advanced security protocols.	Smart thermostats or light bulbs that lack onboard encryption capabilities.
Outdated or Weak Firmware	Devices are often released with insecure or outdated firmware, and many lack ongoing update support.	IoT routers that continue to operate with known vulnerabilities due to the absence of patches.
Lack of Secure Update Mechanisms	Many devices do not support encrypted or authenticated firmware updates, leaving them vulnerable to malicious code injection.	Surveillance cameras that require manual updates through USB without verification processes.
Default or Hardcoded Credentials	Devices are frequently shipped with easily guessable factory-set usernames and passwords, which users often fail to change.	IP cameras accessible through unchanged default login credentials (e.g., “admin”, “1234”).
Insufficient Physical Security	IoT devices installed in public or unsecured locations can be physically tampered with, cloned, or reverse-engineered.	Smart vending machines or kiosks with exposed ports vulnerable to hardware manipulation.
Insecure Communication Protocols	Many devices use unencrypted or outdated communication protocols, allowing attackers to intercept data.	Wearable health devices transmitting plaintext data over unsecured Wi-Fi networks.
Weak Authentication Mechanisms	Some devices lack strong authentication methods, such as two-factor authentication or access control policies.	Home automation systems relying solely on simple passwords for access.
Interoperability Vulnerabilities	Poorly validated integration with third-party platforms can introduce vulnerabilities across connected systems.	A smart speaker linking to multiple unverified IoT applications with inadequate permission control.

(Source: Kolias et al., 2017; Meneghello et al., 2019; Zhang et al., 2020)

Man in the Middle Attacks (MITM) and Man on the Side Attacks

During a MITM attack an attacker secretly disarms and modifies a communication process between IoT devices or between an IoT device and its gateway. IPs are forced to traversing through the node of an attacker (e.g. via ARP poisoning), where it is possible to tamper with the data, steal credentials, or inject the expected command (Conti et al., 2016). Likewise, with a manontheside attack, the attacker may enter a message (e.g. a malware or spoofed response) more quickly than the response of the legitimate server and hence attack code can be entered without need to pretend to be either endpoint (Bhushan et al. 2017). These two mostly go unnoticed in protocols that do not have encryption or appropriate mutual authentication.

Denial of Service (DoS) and Distributed DenialofService (DDoS) Attacks

Denial of service attacks are designed to affect the availability of devices, through resource consumption (denial of network bandwidth, memory, or CPU resource). DDoS targets flood their targets through botnets that consist of the hacked IoT devices (Mirai variants), to make their services unavailable (Dong et al, 2019). There exist some innovative types, such as energy-focused DDoS (EDDoS) that drains battery-driven devices by repeatedly waking at the devices or overloading (Shah et al. 2022). There are also some slowlorislike attacks (e.g. partially sent HTTP request) at application layer (Osanaiye et al, 2016).

Side-Channel Attacks

The reason is that these attacks take advantage of indirect information leaks (in terms of power consumption, timing, electromagnetic emissions or acoustic signals). By way of example, dissimilarity can be inferred during the cryptographic keys by scrutinizing power consumption or timing nature on limited devices. The sensor-heavy or even embedded devices can be especially susceptible to differential power analysis (DPA) or cachetiming attacks in IoT (Sikder et al., 2021).

Other types of Network Attacks

Other vectors of attack are replay attacks, in which messages already captured previously as valid are sent on again, in order to impersonate commands or authentication (Dong et al, 2019); routing attacks which interfere with forwarding or identification in order to steer traffic away or to isolate nodes; they include sinkhole, wormhole or Sybil attacks (Flauzac et al., 2015). Most of the intrusions are preceded by reconnaissance methods such as traffic sniffing, masquerade (masquerading as legit nodes), and portscanning (Osanaiye et al, 2016).

Fig. 1, represents a conceptual diagram illustrating five distinct categories of cyberattacks that commonly target Internet of Things networks. Each attack type is represented by a unique icon within a circular emblem, clearly identifying threats such as Spoofing Attacks, Man-in-the-Middle Attacks, DDoS Attacks, and two instances of Side-Channel Attacks.

2.3 Attack Vectors Specific to Smart Devices

Specific attack vectors are present in devices used on a smart basis, including cameras, thermostats, baby monitors, or medical sensors, as they may be designed and deployed in different ways.

Camera and Visual Feed: A prominent one is the breach in OvertheAir SDKs of smart cameras and baby monitors with exposures of a live video and audio stream to remote unauthorized access through predictable unique identifiers and the lack of encryption encapsulating millions of devices (Osanaiye et al, 2016). The SDKs of many manufacturers are proprietary and do not include a strong cryptographic security, which renders hijack attacks to be practical until hardware/firmware updates are installed.

RJ45 and USB Charging (Juice Jacking): Insecure places of public charging may allow a malware infection or theft of data. USB juicing and USB attacks (juicejacking, BadUSB, Trustjacking) use the data stream during charging, which results in either credential theft of remote code execution (Chaabouni et al., 2019).

Sensorbased Attacks: Smart gadgets have a variety of sensors: Accelerometers, gyroscopes, microphones, ambient sensors, each one of which can be abused. Through these sensors, attackers can see the keystroke, presence or environmental context through sidechannel extraction. Such side channels can be used by sensortargeting malware to monitor user activity or dump confidential information (Sikder et al., 2021).

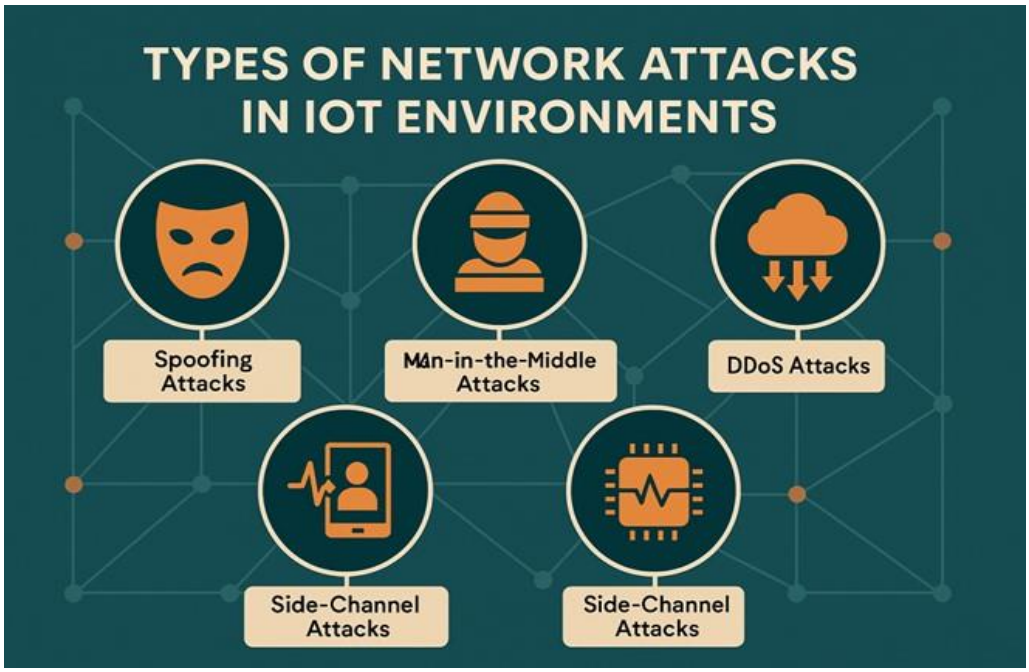

Fig 1: Different types of network attacks

Firmware Supplychain and Cloning Attacks: The devices tend to be provided by OEMs with little publicity. Attackers may load malicious firmware in production, in the supplychain, cloning of hardware. The absence of signed firmware update procedures means that an attacker is able to replicate the identity of devices or use persistent, undetected compromise (Osanaiye et al, 2016).

Operational Technology (OT) / Medical Device Vectors: Some medical IoT devices (insulin pumps, connected defibrillators, bedside monitors) are often used in safety-critical environments where the equipment contains obsolete firmware, low authentication and poor patching because regulations lag. Examples like the MedJack campaign has shown that attackers can use medical devices to have insider lateral movement within hospital networks (Zhang et al., 2020). Moreover, the devices implanted in the industrial control system, or in smartcity control, can be located in pivot points of wide reconnaissance and network traversal.

3.0 Intrusion Detection and Prevention Mechanisms in IoT

3.1 Traditional vs. IoT-Specific Intrusion Detection Systems (IDS)

Well-known network-centric IDS that use signature-based detection includes Snort or Bro/Zeek, which relies on a fit between the observed traffic pattern and known bad behavior. Such systems work well against identified threats but perform poorly against

unknown threats, also known as zeroday attacks, and also need regular signature updates (Heidari et al., 2023; Elrawy et al., 2018). Conventional IDS systems are customarily used on centrally located servers or network bottleneck locations where the computing resources like CPU and memory are sufficient and these solutions will not fit in the limited resource allocation of IoT devices. Instead, IoT-specific IDS are meant to be utilized in an extremely challenging environment, and frequently the detection task may be shared across device, edge/fog, and cloud layers (Spadaccino & Cuomo, 2020; Heidari et al., 2023). IoTspecific systems tend to incorporate the hybrid aspects of detection that would incorporate signaturebased detection models (when dealing with known threats) as well as anomalybased one (detecting deviations in expected behavior) (Elrawy et al., 2018). These could be done, for example, with the H2ID model that applies lightweight local detection to devices associated with heavier, cloud-based analytics (Heidari et al., 2023). A second one is ROSEBOX, a lightweight IDS that uses the efficient feature selection and model pruning, designed to work in resource-constrained IIoT (Spadaccino & Cuomo, 2020). These architectures can maximize both detection accuracy and real-time succeeding; acknowledge the limitations of a device.

Table 2, provides a comparative overview of key features distinguishing conventional Intrusion Detection Systems from those specifically designed for IoT environments. It highlights differences in target environment, detection approach, resource requirements, deployment location, update mechanisms, traffic characteristics, security models, machine learning integration, scalability, flexibility, and provides examples for each type of IDS.

3.2 Lightweight Security Mechanisms for Resource-Constrained Devices

Restricted IoT-based sensors, wearables and smart devices, which are resource-oriented, need to have lightweight security mechanisms that address vulnerabilities without affecting battery life and performance. The benefits of lightweight encryption protocols, like AES-CCM, ChaCha, or SPECK include the possibility of preserving secure communication with limited computational cost and offering this opportunity to devices whose capabilities of computation are limited (Diro & Chilamkurti, 2018). Such authentication systems, such as elliptic curve cryptography (ECC) provide great security using smaller keys as compared to the traditional RSA protocols, hence conserving energy and time used. Secure boot places limits on what code is loaded on the device by requiring that only trusted code be run, such as by malicious code execution, whereas integrity checks such as hash-based verification will detect that untrusted code has changed the firmware (Diro et al., 2020). Nevertheless, these mechanisms are not without their problems, since cryptographic functions can be high battery consumers and manufacturers are usually lax on patch management, making fixes available to known attacks. IoT intrusion prevention systems (IPS) accomplish intrusion prevention by rule-based filtration of traffic that may have been identified as suspicious, although they suffer the drawback of being unable to signify suspicious objects until an update has delivered in real-time and require the compatibility of numerous possible protocols (Khan et al., 2020). Sharing security devices via security models include increasing detection abilities by sharing intelligence about threats on a network between security devices but issues of oversaturation of the limited network or introducing new vulnerabilities can be serious concerns when designing these security models. As an example, lighter intrusion detection frameworks, like those using a bloom filter, consume less memory and still achieve the same accuracy of the heavier frameworks, although they need to be optimized so that they

perform and do not move closer to impracticality (Sicari et al., 2015).

3.3 Role of Machine Learning, AI, and Anomaly Detection in Securing IoT

Artificial intelligence (AI) and machine learning (ML) play a crucial role in improving the IoT security by providing real-time changing threat detection and response.

Table 2: Traditional vs. IoT-Specific Intrusion Detection Systems (IDS)

Feature	Traditional IDS	IoT-Specific IDS
Target Environment	General-purpose computing environments (e.g., enterprise networks, servers)	Resource-constrained IoT environments (e.g., sensors, embedded devices)
Detection Approach	Primarily signature-based and rule-based	More focus on anomaly-based, behavior-based, or lightweight hybrid detection
Resource Requirements	High processing power, memory, and bandwidth	Optimized for low power, limited memory, and minimal computational capacity
Deployment Location	Centralized (e.g., on a server or network gateway)	Distributed or edge-based (e.g., on gateway nodes or edge devices)
Update and Maintenance	Frequent updates with centralized management	Often lacks update mechanisms; may require OTA (over-the-air) lightweight updates
Traffic Characteristics	Handles diverse traffic volumes and formats	Needs to process constrained protocols (e.g., MQTT, CoAP, Zigbee)
Security Model	Built around secure OS, patching, and strong authentication	Must deal with insecure firmware, default credentials, and low-level protocols
Machine Learning Integration	Advanced integration with machine learning and analytics platforms	Limited ML capability, but growing use of lightweight models and edge AI
Scalability and Flexibility	Easier to scale and reconfigure in high-end systems	Must accommodate highly heterogeneous and dynamically scaling environments
Examples	Snort, Suricata, OSSEC	SVELTE, RIDES, and lightweight edge-based anomaly detection systems
Feature	Traditional IDS	IoT-Specific IDS

(Source : Spadaccino & Cuomo, 2020; Heidari et al., 2023)

Machine Learning, like decision trees, support vector machine, neural networks, and clustering, can be used to analyze the network traffic with the aim of detecting anomalies that can be related to attacks such as DDoS, MITM, or unauthorized access. Differently positioned

with signature-based approaches, ML-based anomaly detection can outperform most approaches on zero-day attacks by memorizing standard behaviors in devices and raising an alarm when they are different. As an illustration, it is possible to identify traffic as either malicious or benign using the supervised learning models based on labeled data sets and identify the outliers within the dynamic IoT environments using unsupervised models, such as k-means clustering (Moustafa et al., 2018). More complex deep learning models, including autoencoders, recurrent neural networks, etc, prove to be especially useful in working with high-dimensional IoT data, and with detecting slight anomalies in real-time. Nonetheless, training ML in resource-limited devices is difficult as it will require a lot of computations and memory. Such approaches as model compression, quantization or federated learning, where the training is done in the network but raw data is not shared among devices, reduce these limitations by performing the computation on the network. The AI-powered systems provide predictive security as well since they can predict based on the past events and trend. As an example, it can apply reinforcement learning toward enhancing any strategy that involves responding to intrusion, including isolating the compromised devices. Nevertheless, ML/AI systems remain remedied by such issues as the traditionally high false-positive rates, data privacy, and re-training to maintain results in the face of dynamic patterns of attacks. Another factor that renders it cumbersome to apply ML in IoT ecosystems is the adversarial attacks, in which attackers do modify ML models by feeding it with malicious data (HaddadPajouh et al., 2021).

3.4 Edge/Fog Computing as a Support Structure for Real-Time Detection

Edge and fog computing innovate real-time intrusion detection systems in IoT networks, which overcomes the latency, bandwidth, and scalability differences of the cloud systems. Edge computing runs the data locally on the devices or at local gateways so that severe threats such as intrusions, DDoS attacks, or abnormal behavior can be detected quickly. As an example, edge nodes can play a role in the real-time analysis of device traffic by lightweight ML models, minimizing latency and allowing a quick response, e.g., by isolating compromised devices. Fog computing goes even further, since it allows rather even distribution of computations over intermediate nodes, optimizing computer capacity utilization and reducing the amount of bandwidth used by combining data near the source (Mahmoud et al., 2015). This top-down model enables the advanced anomaly detection (as based on deep learning), carried out at fog nodes, and the edge-level, lightweight detection. The edge/fog systems also improve scalability by spreading the detection operations among the network, which is required to support the huge connectivity of IoT installation. E.g., fog nodes are able to organize threat intelligence between the edge devices to increase the accuracy of detection and response correlation. Nonetheless, such architectures come with their drawbacks such as resource constraints on edge devices, interoperability between different heterogeneous devices, and explicit communication between edge and fog nodes to allow mitigation of the MITM attack. Integrity of data in distributed processing is very important because broken nodes can feed wrong information. The combination of edge/fog computing with ML allows the improvement of detection efficiency by Kirr, but the use of resource limitations necessitates the fine-tuned algorithms. An instance of this is inferior-acting neural networks or decision trees that can be guaranteed at the edge rather than complicated models carried out on an allotted number of fog nodes, establishing a laytered defense mechanism (Zarpelao et al., 2017).

- Query successful

Fig. 2, titled "shows a conceptual diagram that illustrates the central theme of intrusion detection and prevention in Operational Technology (OT) environments, represented by a central cloud icon. Connected to this central theme are four key areas of discussion, each depicted in a distinct rectangular box: "Traditional vs. IoT-Specific IDS," "Role of Machine Learning, AI, and Anomaly Detection," "Lightweight Security Mechanisms for Resource-Constrained Devices," and "Edge/Fog Computing as a Support Structure for Real-Time Detection." The diagram visually summarizes the main topics covered in the manuscript's section on intrusion detection and prevention.

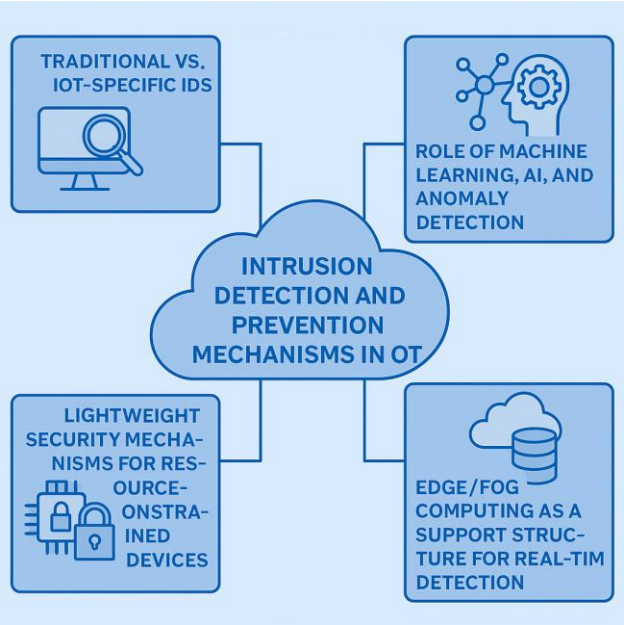

Fig 2: Intrusion detection and prevention mechanism.

4.0 Proposed Solutions and Future Trends

4.1 Cryptographic Techniques and Secure Communication Protocols for IoT

The lightweight algorithms such as AES-CCM and ChaCha ensure secure communications between the resource-constrained devices of the Internet of Things protocol, by the means of leveraging both efficiency and security. eavesdropping is end-to-end secured with secure protocols such as DTLS to CoAP. ECC complicates the key size authentication, however, there are still issues regarding the key management, and protocol compatibilities. The next trends refer to the development of quantum-resistant cryptography in order to survive the new threats (Sicari et al., 2015).

4.2 Decentralized Identity to validate with Blockchain

Blockchain empowers decentralized authentication: through distributed ledgers, it is now possible to explore device identities based on the use of distributed ledgers instead of having to resort to spoofing. Secure access control is automated by using self-sovereign identity (SSI), and smart contracts. Light consensus systems, such as Proof-of-Authority, are appropriate in IoT but have an impediment due to requirements of computational power and scalability. The next trends towards energy efficiency are lightweight blockchains such as IOTA Tangle chain (Mosenia & Jha, 2016; HaddadPajouh et al., 2021).

4.3 Zero-Trust Architecture and its application to IoT

Zero-trust architecture (ZTA) considers nothing to be inherently trusted, it involves continuous authentication and permission-sets that include the least privileges. Marrying micro-segmentation with ECC-based authentication, ZTA in IoT attempts to contain the spread of attacks. A lack of resources and scalability are likely barriers to implementation, yet a future application will be integrating it with edge computing and using policy and AI to ensure compatibility (Sicari et al., 2015; Mahmoud et al., 2015: Ademilua & Areghan, 2022).

4.4 Emerging Standards and Regulatory Frameworks

Improving standards and regulatory systems are important to make the practices under IoT security standard and to make them compliant within different ecosystems. The National Institute of Standards and Technology (NIST)

offers such documents as NISTIR 8259, Foundational Cybersecurity Activities in the IoT Device Manufacturers, explaining the best practices in designing a secure device, such as authentication, encryption, and update implementations (NIST, 2020). The NIST SP 800-183 aims specifically at risk management of IoT systems and searches vulnerable areas and mitigating measures. In 2020, the ISO/IEC 27030 standard was published to give a framework to the security and privacy of IoT; it covers the management of the full lifecycle of devices, data protection, and secure communication protocols. A reference architecture of IoT in the ISO/IEC 30141 standard contributes to the interoperability and the security by design (ISO/IEC, 2018). These standards are supposed to deal with such obstacles as the poor authentication, the use of unsecure communication and software that is not updated by requiring the secure development methods and periodic auditing. Such regulatory mechanisms as the Cybersecurity Act and GDPR in the EU have an effect by requiring adherence to data protection and security requirements and therefore result in the IoT deployments in consumer and industrial applications. The emergence of cybersecurity labeling schemes, as it is the case with the IoT cybersecurity labeling program by NIST, is expected to notify consumers about the security levels of the devices and thus appealing to consumers to demand secure IoT products in the market (Zarpelao et al., 2017).

Table 3 presents a comprehensive overview of key guidelines and regulations aimed at enhancing security in IoT environments. For each standard or regulation listed, the table provides a concise description, outlines its key features, identifies associated challenges, and includes a reference to its source.

Table 3: Emerging Standards and Regulatory Frameworks

Standard/Regulation	Description	Key Features	Challenges	Reference
NISTIR 8259	A guideline for IoT device manufacturers to ensure secure device design and deployment.	- Secure development practices (authentication, encryption, updates). - Risk assessment and mitigation framework. - Device lifecycle management focus.	- Voluntary adoption limits enforcement. - Costly for low-cost device manufacturers. - Limited specificity for diverse IoT ecosystems.	(National Institute of Standards and Technology, 2020)
ISO/IEC 27030	International standard for IoT security and privacy, addressing risks across device and network layers.	- Data protection and privacy-by-design principles. - Risk-based security management. - Applicable to	- Varying global adoption due to regional differences. - Complex implementation for heterogeneous devices. -	(International Organization for Standardization, 2020)

		consumer and industrial IoT.	Needs updates for evolving threats.	
ISO/IEC 30141	Reference architecture for IoT to enhance interoperability and security-by-design.	- Standardized IoT architecture with security principles. - Supports interoperability and scalability. - Guidelines for secure data and device management.	- High costs for small-scale manufacturers. - Alignment with diverse protocols is complex. - Limited enforcement mechanisms.	(International Organization for Standardization, 2018)
EU Cybersecurity Act	EU regulation for cybersecurity certification of ICT products, including IoT devices, to enhance security and trust.	- Certification levels (basic, substantial, high) for IoT devices. - Mandates security compliance. - Aligns with GDPR for data protection.	- Limited to EU, affecting global applicability. - Certification costs burden small manufacturers. - Slow harmonization with non-EU standards.	(European Union, 2019)
GDPR	EU regulation governing data protection and privacy, impacting IoT devices handling personal data.	- Mandates data minimization, user consent, encryption. - Requires breach notifications within 72 hours. - Applies to IoT devices like wearables.	- Complex compliance for resource-constrained devices. - Jurisdictional conflicts for global deployments. - High penalties deter small vendors.	(European Union, 2016)

5.0 Conclusion

The high rate of growth of the Internet of Things (IoT) has brought in a revolutionary advantage in the industries and everyday life, as it can bring about smarter infrastructure, instant tracking, and improved automation. Nevertheless, the heterogeneous, decentralized and resource-poor character of IoT ecosystems has also broadened to generate a large and multi-dimensional attacker landscape. In this

study, the vulnerability associated with IoT devices as well as multiplicity and the changing types of attacks based on the network, and the weakness of traditional security approaches in securing the system have been identified. Among the important lessons is that smart devices are vulnerable to spoofing, denial-of-service (DoS), and man-in-the-middle (MITM) attacks, and the risk of insecure firmware, physical tampering, and poorly implemented authentication channel unique to such devices. New intrusion detection systems (IDS), lightweight cryptographic protocols, and anomaly detection using AI are promising countermeasures, but limited by the capabilities of their devices and the complexity of implementing AI-based approaches in interoperating with the rest of the system. With the ever-widening field of the IoT, the security of these interconnected systems needs to advance to an adaptive, collaboration-driven, and resource-efficient strategy that will provide real-time protection without the loss of performance and scalability.

Implement Secure-by-Design Principles: vendors should implement secure development methodology such as secure firmware updates, encrypted communications, and removal of default passwords. Such standards as NISTIR 8259 and ISO/IEC 27030 should become mandatory and applied throughout the lifecycle of devices, including their design.

Deploy Lightweight Cryptographic and Authentication: Depending on encryption algorithms like AES-CCM, or ChaCha, and authentication using elliptic curve cryptography (ECC) which provide high security even with minimal overhead.

Implement AI-powered Threat Detection and Anomaly Detection: Implement machine learning models on behavioral-based threat detection that is capable of detection of zero-day and evolving threats in real-time.

Use the Blockchain and Decentralized Identity: Use blockchain-basedlightweight, and scalable device authentication and integrity checks such as IOTA.

Enhance Regulatory Control and Consumer Oversight: Regulators and standard agencies need to speed up the processes to establish security regulation specific to IoT, such as certification and labelling of products. Additionally Educating users to make alterations to default credentials, frequent firmware upgrading and an overview of fundamental security hygiene.

6.0 References

Abolade, Y. A. (2023). Bridging Mathematical Foundations and intelligent system: A statistical and machine learning approach. Communications in Physical Sciences, 9, 4, pp. 773-783.

Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. *Communication in Physical Sciences*, 8, 4, pp. 674–688.

Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. M., Biswas, S., ... & Wang, Y. (2020). *A survey of network virtualization techniques for Internet of Things using SDN and NFV*. ACM Computing Surveys (CSUR), 53, 2, pp. 1-40.

Alotaibi, B. (2023). A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. *Sensors*, 23, 17, pp. 7470. https://doi.org/10.3390/s23177470

Awotunde, J. B., Folorunso, S. O., Imoize, A. L., Odunuga, J. O., Lee, C. C., Li, C. T., & Do, D. T. (2023). An ensemble tree-based model for intrusion detection in industrial internet of things networks. *Applied Sciences*, 13, 4, pp. 2479.

Bhushan, B., Sahoo, G., & Rai, A. K. (2017). *Man-in-the-middle attack in wireless and computer networking—A review*. In 2017 3rd International Conference on Advances in Computing, Communication &

Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21, 3, pp. 2671-2701.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18, 3, pp. 2027-2051.

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, pp. 761–768. https://doi.org/10.1016/j.future.2017.08.043

Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. *IEEE Access*, 8, pp. 60539-60551.

Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, 7, pp. 80813-80828.

Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, 7, 1, pp. 1-20.

European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2019). *Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification*. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Flauzac, O., Gonzalez, C., & Nolot, F. (2015). New security architecture for IoT network. *Procedia Computer Science*, 52, pp. 1028–1033. https://doi.org/10.1016/j.procs.2015.05.099

Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). *An overview: security issue in IoT network. In 2018 2nd international conference on I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC),* 2018 2nd international conference on (pp. 104-107). IEEE.

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2018). A survey on Internet of Things security: Requirements, challenges, and solutions. *Internet of Things*, 14, pp. 100129. https://doi.org/10.1016/j.iot.2021.100129

Hamza, A., Gharakheili, H. H., & Sivaraman, V. (2020). IoT network security: requirements, threats, and countermeasures. arXiv preprint arXiv:2008.09339.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, pp. 283-294. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing, 26, 6, pp. 3753-3780.

International Organization for Standardization. (2020). ISO/IEC 27030: Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT). https://www.iso.org/standard/44370.html

ISO/IEC. (2018). ISO/IEC 30141: Internet of Things (IoT) – Reference architecture. International Organization for Standardization. https://www.iso.org/standard/65695.html

Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*, 55, 9, pp. 1-43.

Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal*, 8, 6, pp. 4132-4156.

Kim, M., Oh, I., Yim, K., Sahlabadi, M., & Shukur, Z. (2023). Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. *IEEE access*, 12, pp. 33972-34001.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50, 7, pp. 80-84.

Li, L., Correia, P. L., & Hadid, A. (2018). Face recognition under spoofing attacks: countermeasures and research directions. Iet Biometrics, 7, 1, pp. 3-14.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). *Internet of Things (IoT) security: Current status, challenges and prospective measures. 2015* 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal, 6, 5, pp. 8182-8201*.

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing*, 5, 4, pp. 586-602.

Moustafa, N., Turnbull, B., & Choo, K. K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. IEEE *Internet of Things Journal*, 6, 3, pp. 4815–4830. https://doi.org/10.1109/JIOT.2018.2873784

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, 21, 3, pp. 2702-2733.

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE communications surveys & tutorials*, 23, 3, pp. 1622-1658. NIST. (2020).

NISTIR 8259: Foundational cybersecurity activities for IoT device manufacturers. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259

Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, pp. 147-165.

Pilati, F., Fontanelli, D., & Brunelli, D. (2023). *The Internet of Things and Its Potential for Industrial Processes. IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)*, pp. 233-264.

Rajgure, V. (2023). State-of-the-Art Applications in Computer Vision for Real-Time Target Detection: A Comprehensive Overview. *Indian Scientific Journal of Research In Engineering* And Management

Sagduyu, Y. E., Shi, Y., & Erpek, T. (2019). *IoT network security from the perspective of adversarial deep learning. In 2019 16th Annual IEEE* International Conference on Sensing, Communication, and Networking (SECON) (pp. 1-9). IEEE.

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. *Sensors*, 22, 3, pp. 1094.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, pp. 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials*, 23, 2, pp. 1125-1159.

Spadaccino, P., & Cuomo, F. (2020). Intrusion detection systems for iot: opportunities and challenges offered by edge computing and machine learning. arXiv preprint arXiv:2012.01174.

Van Der Merwe, J. R., Zubizarreta, X., Lukčin, I., Rügamer, A., & Felber, W. (2018). *Classification of spoofing attack types. In 2018 European Navigation Conference (ENC)* (pp. 91-99). IEEE.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, pp. 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

Zhang, X., Cao, Z., & Dong, W. (2020). Overview of edge computing in the agricultural internet of things: Key technologies, applications, challenges. *IEEE Access*, 8, pp. 141748-141761.

Declaration

Consent for publication

Not applicable

Availability of data

Data shall be made available on demand.

Competing interests

The authors declared no conflict of interest

Ethical Consideration

Not applicable

Funding

There is no source of external funding.

Authors' Contribution

Precious Ogechi Ufomba developed the research concept, conducted the literature review, and drafted the manuscript. Ogochukwu Susan Ndibe analyzed security frameworks, contributed to technical content, and reviewed the final version.