*Asian Journal of Research in Computer Science*

***Volume 16, Issue 4, Page 354-371, 2023; Article no.AJRCOS.110417***
***ISSN: 2581-8260***

# IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience

**Oluwaseun Oladeji Olaniyi [a++*], Olalekan Jamiu Okunleye [a++], Samuel Oladiipo Olabanji [b#], Christopher Uzoma Asonze [c†] and Samson Abidemi Ajayi [d‡]**

*[a] University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America.*
*[b] Midcontinent Independent System Operator (MISO Energy), 720 City Center Drive, Carmel, Indiana 46032, United States of America.*
*[c] Federal University of Technology Owerri, PMB 1526, Owerri, Imo State, Nigeria.*
*[d] Polaris Bank, MMWay Ilorin, Kwara State, Nigeria.*

***Authors' contributions***

*This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.*

***Article Information***

DOI: 10.9734/AJRCOS/2023/v16i4397

**Open Peer Review History:**
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/110417

***Original Research Article***

***Received: 09/10/2023***
***Accepted: 13/12/2023***
***Published: 16/12/2023***

## ABSTRACT

The Internet of Things (IoT) has rapidly become a pivotal, transformative force, seamlessly integrating billions of physical devices through sophisticated networks of embedded sensors, software, and internet connectivity. This expansive and interconnected ecosystem offers a broad

*[++] Information Technology Researcher;*
*[#] Senior Business Analyst;*
*[†] Cybersecurity and Information Governance Expert;*
*[‡] Chemist, Researcher, Security Expert, and Data Analyst;*
**Corresponding author: E-mail: oolaniyi00983@ucumberlands.edu;*

spectrum of applications, significantly benefiting urban infrastructure with innovative solutions, enhancing industrial operations through optimization, and enriching consumer experiences with smart devices for safety and convenience. Despite the numerous benefits, the widespread adoption of IoT technologies has challenges, particularly in security and privacy. The proliferation of IoT devices has opened up new avenues for potential cyber threats, posing risks of data breaches and privacy violations. An in-depth analysis of notable IoT security incidents, such as the 2015 Jeep Hack, the Owlet WiFi Baby Heart Monitor Hack, and the TRENDnet Webcam Hack, highlights the critical vulnerabilities inherent in many IoT systems.

Organizations must adopt comprehensive and robust security measures to address these security concerns, including implementing advanced encryption protocols, deploying effective firewalls stringent access control mechanisms, and conducting regular security audits. A multi-layered security architecture becomes essential in mitigating such threats and ensuring the integrity of IoT networks. Furthermore, integrating blockchain technology presents a promising enhancement to IoT security and privacy protocols. Blockchain's inherent features of decentralization, transparency, and immutability offer an additional layer of security, making it more difficult for unauthorized entities to compromise IoT systems.

Equally crucial is the need to elevate IoT security awareness among organizations; this can be achieved through persistent research, fostering collaborations with security experts, and promoting best practices in IoT security. By actively addressing these security challenges, organizations can not only harness the full potential of IoT but also protect their reputations, build trust with stakeholders, and ensure the privacy and safety of their data. Therefore, while IoT presents an array of opportunities for innovation and efficiency, the importance of vigilance in security cannot be overstated. Balancing the benefits of IoT with robust security measures will be vital to realizing its full potential safely and reliably.

*Keywords: Internet of things; cloud computing; data analytics; security; privacy; reputation loss; blockchain; research; security awareness.*

## 1. INTRODUCTION

The Internet of Things (IoT) represents a sophisticated network encompassing various physical entities, commonly called "things." These entities are uniquely equipped with embedded sensors, software, and other technologies, enabling them to establish seamless communication and data exchange with other computer systems and gadgets across the Internet [1]. This technological paradigm has experienced rapid growth and escalated popularity in recent years [1]. The current global landscape of IoT devices is vast, with estimates indicating their presence in the tens of billions. Furthermore, projections suggest a significant and continual increase in these numbers in the foreseeable future.

The practical applications of IoT devices are diverse and permeate various aspects of daily life, as highlighted by Nord et al. [1]. In urban settings, cities have effectively leveraged IoT applications to address and mitigate infrastructure challenges; this includes deploying systems capable of identifying maintenance requirements for crucial urban components like bridges and streets [1]. The industrial sector has witnessed a transformative adoption of IoT devices, which offer critical insights into various operational areas such as supply chain management, logistics, human resource allocation, and production processes. This adoption has catalyzed the creation of substantial business efficiencies [1]. On the consumer front, there is a growing trend towards integrating IoT devices into everyday life. This trend encompasses a wide range of products, including but not limited to smartwatches, smartphones, and an array of smart home appliances like refrigerators, automated lighting systems, baby monitors, and thermostats. These devices are increasingly sought after for their contributions to safety and convenience in daily living [1].

In their comprehensive study, Flores et al. [2] delve into the multifaceted applications and components of the Internet of Things (IoT), elucidating its growing significance in various sectors. The research identifies the three primary applications of IoT, which include its predominant use in production processes, accounting for 63% of its application. This usage primarily revolves around supporting real-time process control within diverse ecosystems. Additionally, IoT finds

significant application in data collection, with 47% usage in gathering crucial data to facilitate informed decision-making, particularly in predictive maintenance. Lastly, technology is vital in monitoring and controlling machinery, with a notable 43% application in this area.

The study by Flores et al. [2] further delineates the four critical components that form the backbone of IoT technology. First is connectivity, which primarily employs RFID technology and Wireless Sensor Networks (WSNs) to establish seamless communication links. Second is the Middleware, an integral platform bridging communication gaps between heterogeneous devices. Third, Cloud Computing is highlighted as a pivotal element, ensuring real-time access and storage of these interconnected devices' substantial volume of big data. Lastly, Data Analytics is emphasized for its crucial role in analyzing the vast amounts of data produced [3].

However, despite these advancements and applications, IoT technology has challenges. As Flores et al. [2] point out, several key issues remain unresolved and are subjects of ongoing refinement. These challenges encompass aspects such as the reliability and performance of IoT devices, their interoperability, and crucial concerns regarding security and privacy [3]. This acknowledgment underscores the notion that while IoT presents numerous opportunities and advantages, it is still a technology in continuous evolution and improvement.

In their insightful analysis, Salazar and Silvestre [4] address the pressing issue of security within the increasingly complex and tense business environment, particularly in the context of Internet of Things (IoT) implementations. They underscore the critical need for a standardized and unified architecture dedicated to IoT security. The intricacy of ensuring security and privacy in IoT, characterized by heterogeneous networks, is a focal point of their study. This complexity is primarily attributed to the IoT's core functionality, which involves exchanging information across a vast network of internet-connected objects. Securing these data exchanges is paramount to prevent potential losses, security breaches, or privacy compromises.

Further, Salazar and Silvestre [4] highlight a significant concern: the multitude of systems and networks involved in an IoT ecosystem presents numerous vulnerabilities that malicious attackers can exploit. This susceptibility to attacks underscores the need for heightened security measures in IoT devices, protocols, and systems. Implementing robust and secure mechanisms is not just a recommendation but a necessity to safeguard against potential threats [5]. Moreover, the authors emphasize the importance of recent advancements in areas related to IoT, such as embedded systems security, industrial malware analysis, and the detection and prevention of threats. These advancements enhance IoT services and operations' overall functionality and safety.

Building upon this foundation, the study aims to provide a comprehensive overview of the history of three notable IoT security breaches. It will delve into the probable preventive measures that could have been implemented and explore the subsequent repercussions these breaches had on the implicated companies. This examination serves as a historical recount and a learning tool to understand better and mitigate future security challenges in the IoT landscape.

## 2. LITERATURE REVIEW

Various scholarly works contribute to a multifaceted understanding of the challenges and potential solutions in the dynamic and rapidly evolving field of Internet of Things (IoT) security. This integrated literature review synthesizes these diverse perspectives, offering a comprehensive view of the state of IoT security. The complexities and vulnerabilities in IoT security are profound, owing to the heterogeneous nature of IoT devices, each presenting unique security challenges. Dicholkar and Sekhar [6] highlight the vast array of security vulnerabilities inherent in IoT systems, underscoring the necessity for comprehensive security mechanisms. Bhatt and Sharma [7] delve into advanced cryptographic solutions, including quantum cryptography, suggesting future-oriented techniques for enhancing IoT defenses. Vojković et al. [8] also highlight the privacy risks of IoT and smart home technologies, highlighting the real-world consequences of security breaches.

The potential role of emerging technologies such as blockchain in enhancing IoT security is explored by Sok et al. [9] who argue that blockchain's decentralized nature could offer innovative security solutions. Ray et al. [10] emphasize the critical role of secure hardware, particularly in the Internet of Medical Things (IoMT), pointing to the need for fortified software

and hardware in IoT systems. The literature also considers the regulatory and ethical dimensions of IoT security. Kerr [11] and the Federal Trade Commission [12] discuss the legal implications of IoT security breaches and the importance of robust legal frameworks. Newman and Al-Nemrat [13]. advocate for an evidence-based approach that integrates ethical considerations, highlighting the multidimensional challenges in IoT security.

Sector-specific concerns in IoT security are evident in various industries. King & Klinedinst [14] examine the automotive sector, where incidents like the Jeep hack underscore the importance of cybersecurity. The vulnerabilities in consumer IoT devices, illustrated by the TrendNet security camera case [15,16] demonstrate the real-world impact of security gaps. Advancements in predictive analytics for IoT security are discussed by Olaniyi et al. [17] who highlight its role in transforming data into actionable insights for preemptive security measures. Adebiyi [18] extends this concept to accounting and auditing practices, indirectly underlining its relevance in IoT security risk mitigation. The intersection of IoT with cloud computing brings additional security considerations. Olaniyi et al. [19] emphasize data-driven decision-making in smart cities contingent on secure cloud-based IoT systems. Microsoft [20] provides insights into database security, which is crucial for protecting data generated by IoT devices.

In healthcare, the importance of compliance in IoT security is discussed by Thomasian and Adashi [21] who stress stringent security measures for the Internet of Medical Things (IoMT). Olaniyi and Omubo [22] highlight the need for compliance with frameworks like COSO in IT auditing, essential for sectors like healthcare. The National Institute of Standards and Technology [23] details specific IoT device vulnerabilities, while the FTC's response to the TrendNet incident (2014) serves as a case study in regulatory action, reinforcing the government's role in ensuring IoT security. Adigwe et al. [24] explore innovative leadership in IoT security management and suggest that effective leadership, combined with advanced data analytics, is vital for developing adaptive security strategies.

The role of education and communication in IoT security is highlighted by Olagbaju et al. [25] who discuss the importance of clear communication in training programs [26,27] emphasizes best practices in education, extendable to IoT security training for various stakeholders. Thus, this integrated literature review reveals the complexities of IoT security, encompassing technological, regulatory, ethical, and industry-specific dimensions. The integration of advanced technologies, emphasis on regulatory frameworks, ethical considerations, and industry-specific vulnerabilities are essential for constructing robust IoT ecosystems. Additionally, predictive analytics, cloud security, compliance, innovative leadership, and effective communication and education are crucial in addressing IoT security challenges, underscoring the need for a comprehensive, multidisciplinary approach [28].

## 2.1 Three Popular IoT Security Breaches

In the rapidly evolving world of the Internet of Things (IoT), the security of connected devices has been a subject of increasing concern, illustrated poignantly by several high-profile cyber-attacks. Each of these incidents exposed critical vulnerabilities and marked a turning point in how we perceive and address IoT security. The 2015 Jeep Hack is a stark reminder of the risks associated with connected vehicles. In a dramatic demonstration of vulnerability, hackers remotely infiltrated a Jeep Cherokee's Uconnect system, seizing control of vital functions like the engine, brakes, and steering [29]. This incident did not just trigger a massive recall by Jeep; it sent shockwaves through the automotive industry, igniting a discourse on the urgent need for robust cybersecurity in connected vehicles [29].

Equally unsettling was the breach involving the Owlet WiFi Baby Heart Monitor. Designed to monitor a baby's vital signs and relay the data to parents via WiFi, this device fell prey to hackers, exposing infants to unseen dangers and leaving parents grappling with the fear of compromised privacy [9]. This incident highlighted the delicate balance between innovative convenience and the security risks inherent in IoT devices, especially those used in sensitive contexts like infant care [9]. Lastly, the TRENDnet Webcam Hack laid bare the vulnerabilities in home security systems [30]. Thousands of private webcams were hacked across the globe, enabling unauthorized access to live feeds and striking a chilling chord about the safety of personal spaces [30]. This breach served as a sobering reminder of the importance of securing home IoT devices, particularly those related to surveillance and

personal privacy. Together, these incidents form a narrative that underscores the complex challenges of securing IoT devices. They illustrate a landscape where the stakes range from individual privacy to public safety, demanding a proactive and comprehensive approach to cybersecurity in connected devices.

## 2.2 The 2015 Jeep Hack

### 2.2.1 History of the attack and affected devices

Contemporary automobile models are increasingly referred to as "computers on wheels." This moniker stems from the vehicles' integration of over a million lines of code, which facilitates advanced safety functionalities like forward collision warnings, automatic emergency braking, sophisticated navigation systems, and lane departure assistance [29]. While these technological advancements significantly enhance vehicular safety and operational efficiency, they concurrently escalate the susceptibility of these vehicles to cybersecurity threats. A pivotal incident illustrating this vulnerability occurred in 2015, involving ethical hackers Chris Valasek and Charlie Miller. Their groundbreaking demonstration highlighted a critical zero-day vulnerability in the Jeep Cherokee [29] reported. Valasek and Miller could access the vehicle's system remotely through this vulnerability. This access allowed them to track the vehicle's location and speed and granted them complete control over several essential systems. These systems included the radio, air conditioning vents, digital display, windshield wipers, and transmission.

More disturbingly, their control extended to shut down the engine, manipulate the steering, and apply the brakes from a remote location. The implications of such capabilities in the hands of malicious actors are severe, with potential outcomes ranging from privacy invasion to life-threatening accidents [29]. The root of this vulnerability was identified in the Uconnect system, which manages the car's cellular connections. This system is responsible for various functionalities, including entertainment, navigation, phone calls, and the generation of fake WiFi hotspots. The critical weakness discovered by Valasek and Miller was that anyone with knowledge of the car's IP address could exploit this flaw, thereby gaining unauthorized access to the vehicle's system [29]. This incident underscored the pressing need for enhanced cybersecurity measures in modern vehicles to protect against such vulnerabilities and ensure the safety of the occupants and the public. Fig. 1 below shows the architecture diagram of the hack.

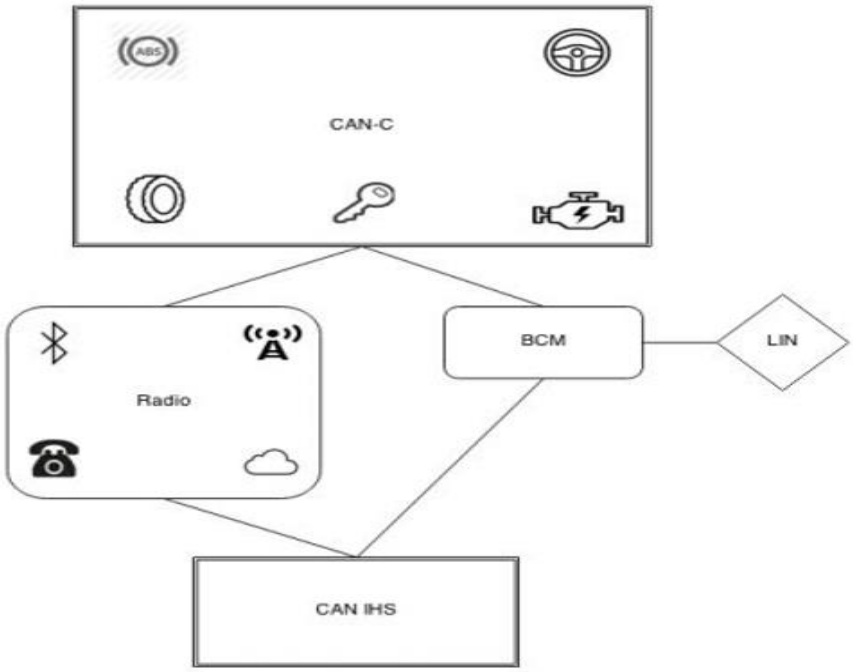


**Fig. 1. Jeep cherokee architecture diagram**
*Source - Schwartz, [29].*

The Jeep Cherokee's security flaws were particularly alarming. The car's WiFi, for instance, was secured by a password based on the system's initial activation time. While this seems secure at first glance, knowledge of the car's manufacturing month could dramatically reduce the possible combinations. The actual password generation was even weaker, based on a default time, making it extremely easy to crack [29]. Once inside the system, the hackers could manipulate the multimedia unit, causing driver distractions like changing the radio station or volume. They were also able to track the vehicle using GPS. The hackers' next step was to breach the car's internal network through the Sprint Cellular network. The main challenge was bypassing the "air gap" between the multimedia system and the car's critical electronic systems, interconnected via a CAN bus. This bus, designed for internal communication, was assumed to be isolated from external access. However, the Jeep Cherokee had no effective air gap, with two CAN buses for the engine and other systems [29].

The breakthrough came when the hackers reprogrammed a chip connected to the multimedia controller and the CAN bus, enabling two-way communication. This increased control over almost all the car's functions, including steering, brakes, transmission, and even the ability to turn off the brakes during movement [29]. The reality of these vulnerabilities was demonstrated on a Jeep Cherokee driven by Wired reporter Andy Greenberg. Initially, the hackers' control manifested in annoyances like blasting cold air and changing radio stations. However, it quickly escalated to turning off the transmission while on a busy overpass. The research, culminating from three years of work, led to a significant recall and changes in the Sprint network. It highlighted the urgent need for more secure vehicle designs to protect against cyberattacks, ensuring driver safety in an increasingly connected automotive world.

## 2.3 Prevention

In the current era of automotive technology, vehicles are equipped with an intricate network of sensors and electronic control units (ECUs). These ECUs manage various vehicular functions, from critical operations like steering, braking, and acceleration to auxiliary systems such as door locks and infotainment [14]. The interconnected architecture of these ECUs is facilitated through a network known as Controller Area Networks (CANs), enabling high-speed communication among different vehicle components [14]. These CANs are linked to onboard diagnostics (OBD-II) ports near the driver's side. This connectivity allows insurance companies and fleet managers to access vehicle data directly, enabling applications like pay-per-mile insurance and vehicle tracking [14]. Integrating such technology signifies a move towards more connected and data-driven vehicle management.

However, these systems' increasing sophistication and interconnectedness have introduced notable security vulnerabilities. Notably, the CAN bus protocol, a cornerstone of vehicular communication networks, is susceptible to security breaches. Many modern devices transmit unencrypted serial data from wireless interfaces (e.g., Bluetooth, WiFi, cellular) to the vehicle's OBD-II port. This data is then relayed to the vehicle's CAN bus. In scenarios where this data is not adequately filtered or sanitized, there exists a risk of unauthorized access and control. An attacker could potentially hijack the device and issue unauthorized commands to crucial safety components like brakes, steering, and accelerator systems.

This vulnerability was starkly demonstrated in the well-documented Jeep hack by security researchers Valasek and Miller [14]. Their demonstration highlighted the potential for remote attackers to gain control over a vehicle's critical systems, posing significant safety risks. This incident underscores the need for robust security measures in modern vehicle design to protect against such cyber threats, ensuring the safety and integrity of automotive systems in an increasingly connected world. Therefore, to elevate the security of automobiles to a level commensurate with the technological advancements in the industry, a paradigm shift is essential in automotive companies' approach toward cybersecurity [29]. These companies must transition from treating security as a secondary consideration to making it a core aspect of their responsibility and accountability. This change is about enhancing technological safeguards and embedding a security culture within the automotive industry.

In response to the growing need for stringent cybersecurity measures, the SPY (Security and Privacy in Your Car) Car Act was introduced in 2017, aiming to set a benchmark for automakers in terms of cybersecurity [29]. The Act is a legislative step towards establishing a

comprehensive framework of minimum standards and transparency requirements. Its primary goal is to protect drivers' data, security, and privacy in an age where vehicles are increasingly interconnected and susceptible to cyber threats [29]. The provisions of the SPY Car Act encompass various critical aspects of vehicle security. These include the implementation of robust isolation protocols to separate vital car components from other networked parts of the vehicle. Such isolation is crucial to prevent the cascading effect of a cyber breach from impacting critical vehicle functions. Additionally, the Act mandates regular and rigorous security assessments of vehicles, ensuring that potential vulnerabilities are identified and addressed proactively. Furthermore, it calls for integrating advanced systems capable of real-time detection and response to unauthorized intrusions or hacking attempts [29].

The SPY Car Act represents a significant stride towards embedding a culture of cybersecurity in the automotive industry. Establishing clear standards and requirements aims to ensure that security is ingrained in vehicles' design and operation, thereby safeguarding drivers' interests and safety in a digitally connected world.

## 2.4 Reputation Loss and Damages to Jeep

The revelation of the Jeep hack precipitated a significant recall by Chrysler, affecting approximately 1.4 million vehicles [29]. In response to the identified vulnerability, Chrysler dispatched USB drives to Jeep owners containing a software update designed to rectify the exploited flaw. This update was intended for the owners to install independently, aiming to mitigate the risk exposed by the hack [29]. Chrysler’s handling of the situation following the Jeep hack was marked by an apparent underestimation of the issue's gravity. They suggested that the software manipulation, which the recall aimed to address, necessitated specialized technical skills, prolonged physical access to the target vehicle, and extensive time dedicated to coding the exploit [31]. Additionally, Chrysler maintained that no inherent defect was identified in their vehicles and that the recall was merely a precautionary step [31].

However, such a stance by Chrysler could be seen as precarious, particularly in the context of vehicle owners who may need more in-depth security knowledge. The company's downplayed narrative might lead these users to underestimate the severity of the vulnerability. Consequently, they might need to recognize the urgency or importance of applying the USB software update, leaving their vehicles potentially unprotected [31]. This oversight could open a window for malicious entities to exploit the vulnerability, potentially resulting in significant financial and reputational damages for Jeep and its parent company [31]. While Chrysler's response involved a proactive recall and provision of a software fix, their communication strategy potentially minimized the perceived risk among consumers. This approach could have led to a lack of immediate action by vehicle owners to secure their vehicles and also underscored the need for automakers to balance technical responses with effective, transparent communication in addressing cybersecurity threats in the automotive industry.

## 2.5 The Owlet WiFi Baby Heart Monitor Hack

### 2.5.1 History of the attack and affected devices

The Owlet WiFi Baby Heart Monitor, as detailed in the research by Sok et al. [9] has gained significant popularity among parents for its ability to monitor infants' health remotely. This innovative device is designed to provide real-time health data, which gives parents a sense of security regarding their child's well-being. The device encompasses a wearable sensor conveniently attached to the infant's foot and a base station that establishes a connection with a wireless network. This setup enables the sensor to transmit vital data to the base station, which then relays this information to smartphones and other devices, facilitating remote monitoring by parents. However, the Owlet Monitor faces substantial security challenges as an Internet of Things (IoT) device. These challenges are critical as they compromise the confidentiality and integrity of the sensitive health data managed by the device.

The concerns regarding security breaches are not unfounded; as Sok et al. [9] emphasize, various stakeholders have identified security issues in IoT devices, including the Owlet WiFi Baby Heart Monitor. Such vulnerabilities are a matter of grave concern, considering the sensitive nature of the information involved. Despite these security concerns, the Owlet

Monitor is generally perceived as user-friendly. It features an alert system that notifies parents of significant changes in their infant's health metrics. The balance between user-friendliness and the need for robust security measures is a pivotal aspect of the ongoing discourse in IoT device development and usage, especially in applications as sensitive as monitoring infant health. Sok et al. [9] underscore the importance of addressing these security vulnerabilities to ensure the safe and effective use of such IoT devices in healthcare and parental monitoring contexts. Fig. 2 shows the architectural diagram of the Baby Heart Monitor.

## 2.6 Prevention

Implementing robust security measures in the context of the Owlet WiFi Baby Heart Monitor is not just a recommendation but a necessity. Bhatt and Sharma [7] have pointed out the potential of quantum cryptography as a groundbreaking approach to bolster the security of Internet of Things (IoT) devices. This suggestion is particularly pertinent given the sensitive nature of the health data processed by devices like the Owlet monitor. Similarly, Dicholkar and Sekhar [6] emphasized the imperative need for proactive protective measures concerning IoT devices. Their insights underline the importance of reactive and anticipatory security strategies in the IoT landscape.

In an essential contribution to this field, Ray et al. [10] introduced an advanced sensor designed for Internet of Medical Things (IoMT) applications. This development is significant as it offers a tailored solution for healthcare-related IoT devices, explicitly addressing security and privacy concerns. The relevance of this development to the Owlet monitor must be considered, considering its role in monitoring infant health. For users of the Owlet monitor, Ray et al. [10] stresses the necessity of adopting various preventative measures to safeguard the device. These measures include the implementation of secure data encryption protocols, a practice that is fundamental in protecting the integrity and confidentiality of transmitted health data. Regular security audits are also recommended to identify and address potential vulnerabilities promptly. Adhering to established best practices for IoT protection further reinforces the security framework around these devices.

Another crucial aspect of maintaining the security of the Owlet WiFi Baby Heart Monitor, as indicated by Ray et al. [10] is the timely deployment of software updates. These updates are often released in response to emerging threats and vulnerabilities and play a critical role in keeping the device secure against evolving cyber threats. The combination of these strategies forms a comprehensive approach to securing the Owlet monitor and, by extension, safeguarding the sensitive health data of infants monitored by the device. In the rapidly evolving landscape of Internet of Things (IoT) security, the necessity for companies like Owlet to establish comprehensive and effective contingency plans for managing security breaches is paramount. This requirement is particularly critical given the sensitive nature of the data handled by Owlet's devices. Dicholkar and Sekhar [6] highlighted the importance of such plans, drawing lessons from past cyber-attacks to reinforce their arguments.

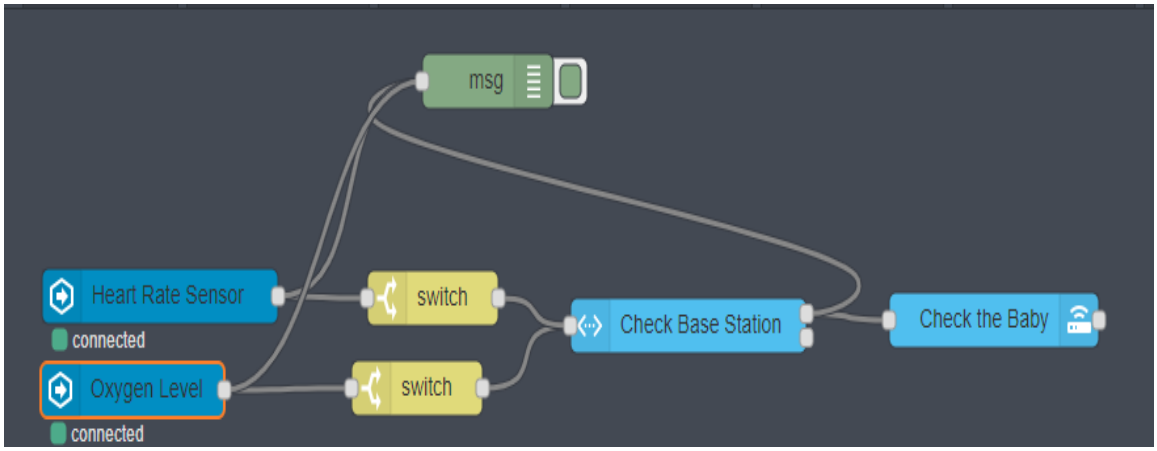


**Fig. 2. Baby heart monitor**
*Source - Sok et al. [9]*

According to Dicholkar and Sekhar [6] a well-devised incident response strategy is essential for any company operating in the IoT domain. This strategy should encompass procedures that enable the swift detection of security breaches. Once a breach is detected, it is crucial to notify affected users immediately, ensuring transparency and trust. Furthermore, cooperating with law enforcement and regulatory authorities at the earliest possible stage is vital to effectively managing a breach's aftermath. These steps are critical for damage control, maintaining user trust, and complying with legal and ethical standards. Likewise, Thomasian and Adashi [21] suggest that collaboration with cybersecurity experts or industry peers could significantly enhance the effectiveness of Owlet's contingency planning. Such collaborations can provide invaluable insights into the latest security trends and threats, thereby enabling Owlet to fortify its defenses against potential cyber incidents. This approach is about responding to incidents and proactively preventing them.

Additionally, these experts have advocated for integrating cutting-edge technologies like blockchain. As P.R. Newswire [32] reported, blockchain technology can offer practical solutions to address potential vulnerabilities inherent in IoT devices. The decentralized and tamper-resistant nature of blockchain makes it a suitable candidate for enhancing the security of IoT systems like those deployed by Owlet. Implementing such technologies is not merely a reactionary measure but a proactive step toward strengthening security defenses against future breaches. Thus, for a company like Owlet, navigating the complexities of IoT security demands a multifaceted approach. This approach must include developing a robust incident response strategy, fostering collaborations with cybersecurity experts, and integrating advanced technologies like blockchain. These measures are essential to safeguard against, respond to, and manage security breaches effectively, protecting sensitive health data and maintaining user trust.

## 2.7 Reputation Loss and Damages to Owlet

The importance of prioritizing security in the Owlet WiFi Baby Heart Monitor cannot be overstated, especially when considering its impact on the company's reputation and the continuity of its business operations. Research by Mangala and Venugopal [33] sheds light on the potentially detrimental effects of security breaches, such as eroding customer trust and the emergence of legal complications. These factors are critical for any business concerning sensitive infant health data. Furthermore, the insights from Newman and Al-Nemrat [13] emphasize the significance of maintaining a positive brand image as a cornerstone for retaining customers. This aspect is crucial for driving revenue growth, expanding market position, and fostering customer loyalty, which are vital for Owlet's financial success and market expansion.

Given these perspectives, it is evident that investing in robust security measures and developing comprehensive contingency planning strategies is more than a necessity; it is a strategic imperative. Such proactive measures would help mitigate risks associated with data breaches and other security incidents and play a pivotal role in safeguarding the company's business continuity. Equally important is preserving customer trust, which is fundamental to maintaining a solid customer base. In summary, for Owlet, the integration of stringent security protocols and effective contingency plans is essential for sustaining its business health and customer relationships in the long term.

## 2.8 The TRENDnet Webcam Hack

### 2.8.1 History of the attack and affected devices

In 2013, TrendNet, a company specializing in security cameras, encountered a significant controversy when the U.S. Federal Trade Commission (FTC) lodged a complaint against them for engaging in deceptive practices. This complaint arose from a severe security breach in their Internet of Things (IoT) infrastructure. In this incident, a hacker infiltrated TrendNet's system and gained access to live video feeds from over 700 subscribers, all without consent or authorization from these individuals. This unauthorized access led to the live feeds being disseminated online, which caused widespread social unrest and raised serious concerns about privacy and security. Before this breach, TrendNet had marketed its SecureView cameras as highly secure and well-protected. However, post-incident investigations by the FTC revealed that these cameras were equipped with flawed software. This software vulnerability enabled unapproved access to live feeds, resulting in

unauthorized surveillance, eavesdropping, and illegal intrusions into the private lives of individuals, thereby compromising their safety and privacy. This incident highlighted significant gaps in IoT security and underscored the importance of rigorous software testing and privacy safeguards in connected devices.

In a comprehensive and meticulous forensic investigation, the Federal Trade Commission (FTC) made a critical discovery regarding TrendNet's operations. They found that TrendNet had been markedly negligent in its approach, demonstrating a blatant disregard for evaluating potential security risks. This was highlighted between April 2010 and January 2012, during which TrendNet transmitted their subscribers' system login information over the Internet. The critical issue was the lack of encryption: the data was sent in plain, easily readable text. This practice left TrendNet's customers extremely vulnerable, exposing them to risks like unauthorized access, interception, and potentially malicious exploitation of their personal information [11].

Furthermore, the investigation revealed that the mobile applications linked to TrendNet cameras had also been handling user credentials similarly carelessly. These applications stored the users' login details in clear, easily readable text directly on the users' devices. Such a practice posed a significant security threat, further compromising the safety and privacy of the users [34]. This revelation underscored the severity of TrendNet's lax approach to data security and highlighted the far-reaching implications of such negligence for consumer safety [11]. Fig. 3 shows the flaw in home security cameras that expose live feeds to hackers.

## 2.9 Prevention

The comprehensive report by the National Institute of Standards and Technology (NIST) in 2020 highlighted significant security vulnerabilities in the TRENDnet ProView Wireless camera, particularly the TV-IP512WN 1.0R model with firmware version 1.0.4. The report identified a critical issue: an unauthenticated stack-based buffer overflow that arises during the processing of RTSP packets. This vulnerability is in the "respond" binary within the "/sbin" directory. It is triggered when the binary attempts to process an overly long "Authorization: Basic" RTSP header. Such a flaw poses a substantial risk, including the potential for denial-of-service attacks or even remote code execution within TrendNet's operational framework.

**Fig. 3. The flaw in home security cameras exposes live feeds to hackers**
*Source – Wired - Zetter, B. (2012).*

In the context of legal and regulatory compliance, TRENDnet's oversight in thoroughly evaluating its device and service processing operations is evident. Adherence to pertinent legal frameworks and standards, such as those set by the Federal Trade Commission and Consumer Protection laws, is crucial. These regulations are designed to prevent fraudulent and deceptive business practices. Beyond mere compliance, TRENDnet could have significantly enhanced the security of its enterprise and the protection of subscriber data through various measures. These include implementing firewalls and encryption techniques, deploying intrusion detection and prevention systems, and establishing robust auditing, logging, access control, backup, recovery, authentication, and authorization protocols.

Encryption, utilizing both asymmetric and symmetric methods, is fundamental in converting plain text into ciphertext, thereby safeguarding subscriber data [34]. Firewalls act as critical defensive barriers, monitoring and controlling incoming and outgoing network traffic to identify potential threats and prevent unauthorized access [34]. Access control measures are essential for restricting data and resource access to authorized users, while authentication and authorization processes ensure that access is granted appropriately [34]. Furthermore, Intrusion Detection and Prevention Systems (IDPSs) are instrumental in monitoring network traffic for malicious activities [34]. Additionally, implementing auditing and logging can enhance overall security by monitoring database activities, a practice recommended by industry leaders such as Microsoft. Finally, had TRENDnet incorporated these comprehensive security measures, it would have markedly strengthened its overall security posture, thereby significantly elevating its security stance and resilience against potential cyber threats.

## 2.10 Reputation Loss and Damages to TrendNet

TrendNet's deceptive practices severely tarnished its reputation, primarily due to inadequate security measures that betrayed consumer trust and heightened the risk of privacy violations and potential harm [11]. The Federal Trade Commission (FTC) held TrendNet accountable, enacting prohibitions against the company's misrepresentation of camera security and privacy of information (FTC, 2014). This ruling prompted a wave of subscription cancellations, leading to substantial financial losses for TrendNet, a direct consequence of their fiscal misrepresentations [12]. Additionally, the FTC mandated that TrendNet establish a comprehensive security program to safeguard against unauthorized access. The company was also required to undergo biennial third-party security evaluations for twenty years, promptly inform customers about potential security issues, and ensure the provision of technical support and assistance for at least two years [12].

## 2.11 Security Outlook For The Internet of Things

In a detailed analysis by P.R. Newswire in 2020, it was predicted that the Internet of Things (IoT) security market would experience a significant expansion, growing by USD 4.35 billion by 2025. This represents an impressive annual growth rate of 34.7%. A key driver of this growth is the increasing demand for smart city technologies. The implementation of IoT in smart cities is revolutionizing urban management. It includes effectively managing traffic flow, accommodating rising populations, and enhancing safety and security measures. IoT devices in these urban settings work collaboratively, collecting and analyzing data to address challenges inherent in urban living. This collaboration improves current urban life and paves the way for future advancements. A critical aspect of this technological revolution is the security of IoT devices. IoT security protects networks, devices, and user interfaces from unintentional errors and deliberate cyber threats. Various institutions have developed solutions targeting specific IoT-related vulnerabilities, including brute force password attacks, remote vehicle hijackings, and privacy breaches to combat these threats.

P.R. Newswire [32] also highlighted the emergence of blockchain technology as a vital solution to IoT security challenges. Integrating blockchain into IoT networks significantly enhances privacy and security, which is crucial for businesses operating in competitive environments. The convergence of blockchain and IoT offers numerous advantages, such as efficient transaction processing, secure record-keeping, easy tracking of devices, and improved compliance measures [34]. This synergy effectively prevents data breaches, leaks, and fraud while streamlining the dispute resolution process.

However, the advancement of IoT technology also brings to light the importance of security

education and awareness. P.R. Newswire [32] noted that the need for a comprehensive understanding of IoT security risks significantly hinders the industry's growth. Malware attacks on IoT devices are a significant concern for service providers. Addressing these issues requires more than just installing devices; it demands an enhanced understanding and management of IoT risks. A survey conducted by Trend Micro revealed that most IT leaders recognize the need for better awareness and management of IoT-related threats to prevent system vulnerabilities and data breaches.

Finally, the evolution of IoT is reshaping the business landscape, as discussed by Dabholkar and Sekhar in 2020. Staying ahead of security threats is essential for businesses to remain competitive. This requires ongoing commitment, attention, and education from individuals, companies, and government entities. Businesses should invest in research and development to address potential risks and collaborate with security experts for insights into emerging threats [6]. By creating a culture of security awareness and best practices, businesses can strengthen their ability to protect the interests of their customers and stakeholders, ultimately earning their trust. Security, therefore, is not just a necessity but a strategic advantage in the evolving IoT landscape [34].

## 2.12 Security Measures and Principles in Azure, Google Cloud, and AWS

The expanding Internet of Things (IoT) universe, featuring "smart" devices like robotic vacuum cleaners, doorbell cameras, and smart locks, has become increasingly popular for its ability to enhance home and office convenience [34]. However, security considerations are often an afterthought, only gaining attention after incidents like data breaches, underscoring the importance of proactive security measures [35]. In response to these vulnerabilities, ongoing monitoring of IoT devices and infrastructure is vital, particularly in enterprise and industrial environments [34]. Security strategies should encompass network setups with firewalls, centralized security oversight, and secure integration of external devices. It is also critical to monitor older legacy devices to prevent them from becoming security liabilities [34]. Fig. 4 below further explains The IoT device infrastructure for the warehouse climate control system.

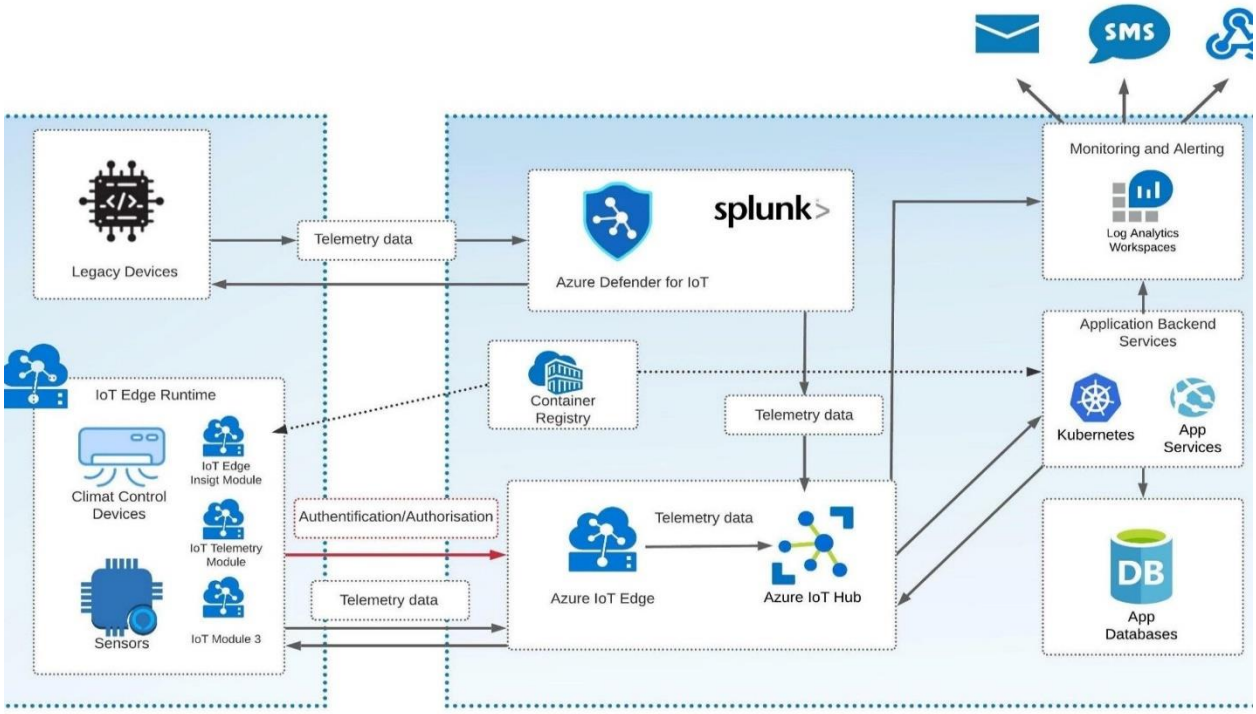


**Fig. 4. The IoT device infrastructure for the warehouse climate control system**
*Source: Zaikin [35]*

Adopting integrated security approaches from the production stage of IoT devices, such as using JSON Web Tokens (JWTs), is advisable. These preemptive measures are generally more cost-effective and efficient than post-production fixes. Additionally, enhancing IoT device security with Transport Layer Security (TLS) or Lightweight Cryptography (LWC) is recommended (Oladoyinbo et al., 2023). Regarding cloud platforms, Azure fortifies IoT security through tools like Azure IoT Hub, IoT Edge, and Azure Defender for IoT Olabanji, [34]. Fig. 5 shows the authentication process for generating public and private keys in the cloud system.

Google Cloud's IoT Core also offers comprehensive security features, including device management, data analysis, and robust encryption. Similarly, AWS IoT Core provides analogous services, with AWS IoT Device Defender supplementing these by analyzing device logs and identifying security threats [36]. Fig. 6 shows AWS IoT Defender.

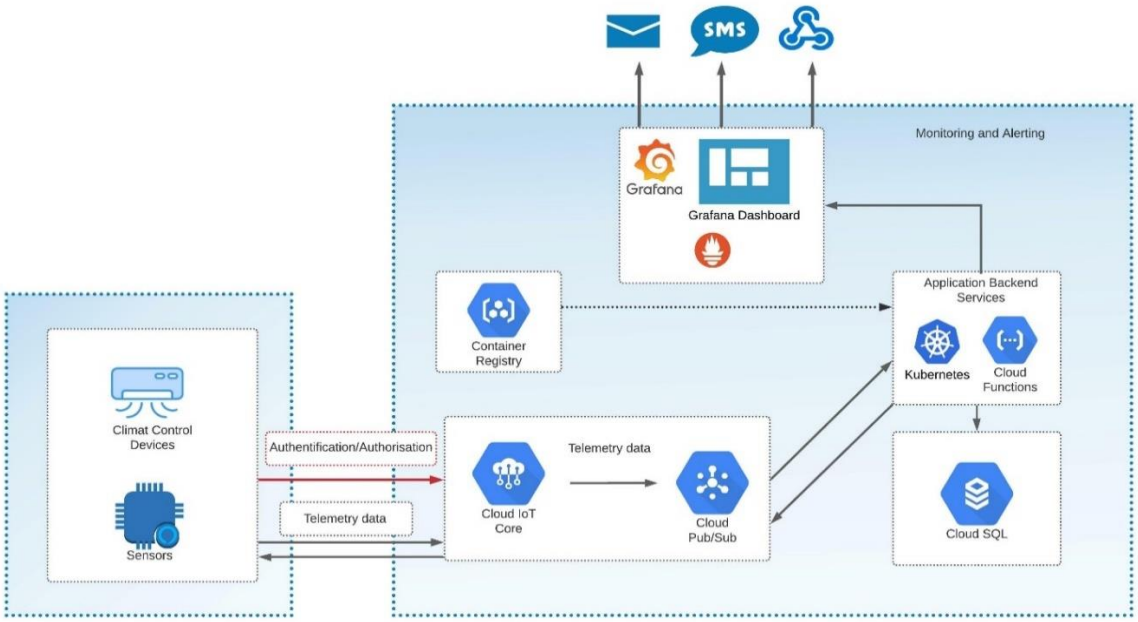


**Fig. 5. Authentication process for the generation of public and private keys in the cloud system**

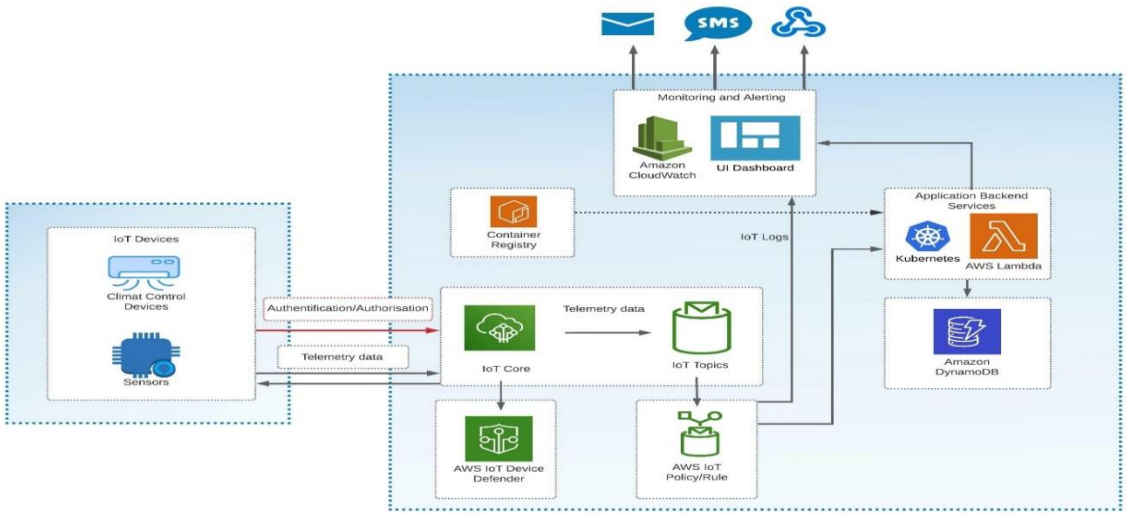


**Fig. 6. AWS IoT defender**

## 3. CONCLUSION

The Internet of Things (IoT), a rapidly evolving technological paradigm, integrates physical devices for data exchange via the Internet, significantly impacting various aspects of daily life, including city infrastructure, industrial supply management, and consumer electronics [1]. It encompasses real-time process control, predictive maintenance, and machine monitoring applications, supported by technologies like RFID, Wireless Sensor Networks (WSNs), communication middleware, cloud computing, and data analytics [2]. Despite its growing adoption, IoT faces critical challenges regarding reliability, performance, interoperability, and security and privacy concerns [2]. The intricacy of IoT's interconnected framework demands standardized, unified security architectures to mitigate these challenges [1].

This ffindings emphasizes the urgency of prioritizing security in IoT deployments, showcasing three notable security breaches. It advocates for implementing robust security protocols, encryption, stringent access controls, and regular security audits to safeguard IoT networks and devices [37]. Additionally, it underscores the significance of collaboration with cybersecurity experts and adherence to regulatory standards as strategies to reinforce security practices [21]. Given the severe implications of security breaches, including reputational and financial damages, adopting proactive security measures and comprehensive incident response strategies becomes crucial [6].

The future of IoT security appears promising, with the industry poised for significant growth and emerging technologies like blockchain offering potential enhancements in privacy and security [32]. However, a persistent challenge lies in raising awareness about IoT security. This necessitates investments in research, collaborative efforts, and security awareness programs to develop robust defenses against evolving threats and protect IoT devices and networks (Dicholkar & Sekhar, 2020). Addressing these security challenges is critical to unlocking IoT's full potential, fostering consumer trust, and paving the way for future advancements [34].

## 4. RECOMMENDATIONS

As the Internet of Things (IoT) continues to weave itself into the fabric of our daily lives, the importance of robust security measures becomes increasingly critical. Integrating IoT across various sectors — from smart homes to industrial applications — brings convenience and efficiency and introduces many security challenges. These challenges stem from IoT devices' diverse nature, extensive connectivity, and the sensitive data they handle. In recognition of these concerns, this section provides recommendations to fortify IoT security [34-38]. These recommendations are predicated on a multidisciplinary approach, recognizing that adequate IoT security is not solely a technological challenge but involves legal, ethical, educational, and collaborative dimensions. The following recommendations are designed to guide manufacturers, policymakers, users, and other stakeholders in enhancing the resilience and security of IoT ecosystems. By addressing these key areas, we can work towards a more secure and dependable IoT environment, ensuring that security vulnerabilities do not undermine the benefits of this revolutionary technology [39-44].

- Strengthening Cybersecurity Frameworks and Protocols: Encourage developing and implementing comprehensive cybersecurity frameworks. This includes robust encryption protocols, firewalls, access control systems, and regular security audits to protect IoT networks and devices.
- Promoting Collaboration and Knowledge Sharing: Advocate for increased collaboration between IoT device manufacturers, security experts, and regulatory bodies. Sharing knowledge and best practices can lead to the developing of more secure IoT systems.
- Investing in Security Education and Awareness: Highlight the importance of educating users, developers, and stakeholders about IoT security risks. Develop programs and workshops to raise awareness and train individuals in identifying and mitigating potential security threats.
- Fostering Research and Innovation in IoT Security: Suggest allocating resources for research and development in IoT security. This can lead to innovative solutions and advancements in securing IoT devices and networks.
- Embracing Emerging Technologies: Encourage the exploration and integration of emerging technologies like blockchain, which offers enhanced security features

such as decentralization and immutability, potentially bolstering IoT security.

- Establishing Standardized Security Practices: Recommend creating and adopting standardized security protocols and practices across the IoT industry to ensure a unified approach to security.
- Developing Responsive Incident Management Strategies: Stress the importance of having effective incident response strategies in place. This includes procedures for quick detection, reporting, and remediation of security breaches.
- Regulatory Compliance and Ethical Considerations: Emphasize the need for IoT devices and services to comply with relevant legal frameworks and standards. Also, it encourages ethical considerations in IoT device development and deployment.
- Prioritizing Privacy and Data Protection: Advice on prioritizing user privacy and data protection in the design and operation of IoT devices. Implement measures to safeguard user data against unauthorized access and breaches.
- Long-term Security Maintenance: Suggest that manufacturers and service providers commit to the long-term security maintenance of their IoT products, including regular updates and patches to address new vulnerabilities.

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES


1. Nord JH, Koohang A, Paliszkiewicz J. The Internet of Things: Review and theoretical framework. The Association for Computing Machinery. 2019 ;133:97–108. Available:https://doi.org/10.1016/j.eswa.2019.05.014
2. Flores M, Maklin D, Golob M, Al-Ashaab A, Tucci C. Awareness towards Industry 4.0: Key enablers and applications for the Internet of Things and big data. IFIP Advances in Information and Communication Technology. 2018;377–386. Available:https://doi.org/10.1007/978-3-319-99127-6_32
3. Olaniyi FG, Olaniyi OO, Adigwe CS, Abalaka AI, Shah NH. Harnessing Predictive Analytics for Strategic Foresight: A Comprehensive Review of Techniques and Applications in Transforming Raw Data to Actionable Insights. Asian Journal of Economics, Business and Accounting. 2023; 23(22):441–459. Available:https://doi.org/10.9734/ajeba/2023/v23i221164
4. Salazar J, Silvestre S. Internet of Things. TechPedia; 2017. Available:https://core.ac.uk/download/pdf/132530214.pdf
5. Omogoroye OO, Olaniyi OO, Adebiyi OO, Oladoyinbo TO, Olaniyi FG. Electricity Consumption (kW) Forecast for a Building of Interest Based on a Time Series Nonlinear Regression Model. Asian Journal of Economics, Business and Accounting. 2023’23(21):197–207. Available:https://doi.org/10.9734/ajeba/2023/v23i211127
6. Dicholkar SV, Sekhar D. Review-IoT Security Research Opportunities. International Conference on Convergence to Digital World - Quo Vadis (ICCDW), Mumbai, India. 2020;1–4. Available:https://doi.org/10.1109/ICCDW45521.2020.9318641
7. Bhatt AP, Sharma A. Quantum cryptography for Internet of Things security. Journal of Electronic Science and Technology. 2019;17(3):213–220. Available:https://doi.org/10.11989/JEST.1674-862X.90523016
8. Vojković G, Milenković M, Katulić T. IoT and smart home data breach risks from the perspective of data protection and information security law. Business Systems Research. 2020;11(3):167-185. Available:https://doi.org/10.2478/bsrj-2020-0033
9. Sok K, Colin JN, Po K. Blockchain and the Internet of Things opportunities and challenges. In Proceedings of the 9th International Symposium on Information and Communication Technology. 2018; 150-154. ISBN (Electronic) - 9781450365390
10. Ray PP, Dash D, Kumar N. Sensors for the Internet of medical things: State-of-the-art, security and privacy issues, challenges, and future directions. Computer Communications. 2020;160:111–131. Available:https://doi.org/10.1016/j.comcom.2020.05.029

11. Kerr D. FTC and TrendNet settle claims over hacked security cameras. CNET; 2013. Available:https://www.cnet.com/news/privacy/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/
12. FTC. FTC approves final order settling charges against TrendNet, Inc. Federal Trade Commission; 2014.. Available:https://www.ftc.gov/news-events/news/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc
13. Newman B, Al-Nemrat A. Making the Internet of Things sustainable: an evidence-based practical approach in finding solutions for yet-to-be-discussed challenges in the Internet of Things. Digital Forensic Investigation of Internet of Things (IoT) devices. 2021;255–285. Available:https://doi.org/10.1007/978-3-030-60425-7_11
14. King C, Klinedinst DJ. Vehicle Cybersecurity: The Jeep Hack and Beyond. Carnegie Mellon University, Software Engineering Institute; 2016.. Available:https://insights.sei.cmu.edu/blog/vehicle-cybersecurity-the-jeep-hack-and-beyond/
15. Zetter B. A flaw in home security cameras made by Trendnet potentially exposed thousands of customers to possible hackers who could access the live video feeds without a password. Wiredl; 2012. Available:https://www.wired.com/2012/02/home-cameras-exposed/
16. Munawwar W. TrendNet wireless camera buffer overflow vulnerability. Payatu ; 2020. Available:https://payatu.com/blog/trendnet-wireless-camera-buffer-overflow-vulnerability/
17. Olaniyi OO, Olabanji SO, Abalaka AI. Navigating Risk in the Modern Business Landscape: Strategies and Insights for Enterprise Risk Management Implementation. Journal of Scientific Research and Reports. 2023;29(9):103–109. Available:https://doi.org/10.9734/jsrr/2023/v29i91789
18. Adebiyi OO. Exploring the Impact of Predictive Analytics on Accounting and Auditing Expertise: A Regression Analysis of LinkedIn Survey Data. Asian Journal of Economics, Business and Accounting. 2023;23(22):286–305. Available:https://doi.org/10.9734/ajeba/2023/v23i221153
19. Olaniyi OO, Olabanji SO, Okunleye OJ. Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives. Journal of Scientific Research and Reports. 2023;29(9):73–81. Available:https://doi.org/10.9734/jsrr/2023/v29i91786
20. Microsoft. What is database security? Learn how to secure your database and protect it from threats. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-database-security/#faq; 2023.
21. Thomasian NM, Adashi EY. Cybersecurity on the Internet of medical things. Health Policy and Technology. 2021;10(3):100549. Available:https://doi.org/10.1016/j.hlpt.2021.100549
22. Olaniyi OO, Omubo DS. The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management. The International Journal of Innovative Research & Development; 2023. Available:https://doi.org/10.24940/ijird/2023/v12/i5/MAY23001
23. NIST National Vulnerability Database - CVE-2020-12763 Detail. National Institute of Standards and Technology, U.S. Department of Commerce; 2020. Available:https://nvd.nist.gov/vuln/detail/CVE-2020-12763#:~:text=TRENDnet%20ProView%20Wireless%20camera%20TV,Authorization%3A%20Basic%22%20RTSP%20header.
24. Adigwe CS, Abalaka AI, Olaniyi OO, Adebiyi OO, Oladoyinbo TO. Critical Analysis of Innovative Leadership through Effective Data Analytics: Exploring Trends in Business Analysis, Finance, Marketing, and Information Technology. Asian Journal of Economics, Business and Accounting. 2023;23(22):460–479. Available:https://doi.org/10.9734/ajeba/2023/v23i221165
25. Olagbaju OO, Babalola RO, Olaniyi OO. Code Alternation in English as a Second Language Classroom: A Communication

and Learning Strategy. Nova Science; 2023.
Available:https://doi.org/10.52305/YLHJ5878

26. Olagbaju OO, Olaniyi OO. Explicit and Differentiated Phonics Instruction on Pupils' Literacy Skills in Gambian Lower Basic Schools. Asian Journal of Education and Social Studies. 2023;44(2):20–30.
Available:https://doi.org/10.9734/ajess/2023/v44i2958
27. Olaniyi OO. Best Practices to Encourage Girls' Education in Maiha Local Government Area of Adamawa State in Nigeria. The University of Arkansas Clinton School of Public Service (Research Gate); 2022.
Available:https://doi.org/10.13140/RG.2.2.26144.25606
28. Abalaka AI, Olaniyi OO, Adebiyi OO. Understanding and Overcoming the Limitations to Strategy Execution in Hotels within the Small and Medium Enterprises Sector. Asian Journal of Economics, Business and Accounting. 2023;23(22):26–36.
Available:https://doi.org/10.9734/ajeba/2023/v23i221134
29. Schwartz E. Buckle Up: Let's be (Car) careful about security. Comp116 Security Final Project; 2016.
Available:https://www.cs.tufts.edu/comp/116/archive/fall2016/eschwartz.pdf
30. Penelova M. Access Control Models. Cybernetics and Information Technologies CIT. 2021;21(4):77–104.
Available:https://doi.org/10.2478/cait-2021-0044
31. Mearian L. Update: Chrysler recalls 1.4M vehicles after Jeep hack. Computerworld; 2015.
Available:https://www.computerworld.com/article/2952186/chrysler-recalls-14m-vehicles-after-jeep-hack.html
32. PR. Newswire. Internet of Things/IoT Security Market Outlook, 2020-2030 Forecast Report; 2020.
Available:https://go.openathens.net/redirector/ualr.edu?url=https://www.proquest.com/wire-feeds/internet-things-iot-security-market-outlook-2020/docview/2338986023/se-
33. Mangala N, Venugopal KR. Current challenges in IoT Cloud smart applications. In 2021 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). 2021 ;36-40.
Available:https://doi.org/10.1007/s10479-023-05285-7
34. Olaniyi OO, Abalaka AI, Olabanji SO. Utilizing Big Data Analytics and Business Intelligence for Improved Decision-Making at Leading Fortune Company. Journal of Scientific Research and Reports. 2023; 29(9):64–72.
Available:https://doi.org/10.9734/jsrr/2023/v29i91785
35. Zaikin B. Mobile and IoT Security Strategies in the Cloud; 2021.
Available:https://www.boriszaikin.com/mobile-and-iot-security-strategies-in-the-cloud
36. Olabanji SO. Technological Tools in Facilitating Cryptocurrency Tax Compliance: An Exploration of Software and Platforms Supporting Individual and Business Adherence to Tax Norms. Current Journal of Applied Science and Technology. 2023;42(36):27–39.
Available:https://doi.org/10.9734/cjast/2023/v42i364239
37. Shi B. Computer Network Information Security Protection Based on Virtual Private Network. Journal of Physics. Conference Series. 2020;1646(1):12121.
Available:https://doi.org/10.1088/1742-6596/1646/1/012121
38. Olabanji SO. Advancing Cloud Technology Security: Leveraging High-Level Coding Languages like Python and SQL for Strengthening Security Systems and Automating Top Control Processes. Journal of Scientific Research and Reports. 2023;29(9):42–54.
Available:https://doi.org/10.9734/jsrr/2023/v29i91783
39. Oladoyinbo TO, Adebiyi OO, Ugonnia JC, Olaniyi OO, Okunleye OJ. Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach. Asian Journal of Economics, Business and Accounting. 2023;23(21): 222–231.
Available:https://doi.org/10.9734/ajeba/2023/v23i211129
40. Olaniyi OO, Okunleye OJ, Olabanji SO. Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing

Literature. Current Journal of Applied Science and Technology. 2023;42(25):10–18.
Available:https://doi.org/10.9734/cjast/2023/v42i254181

41. Olaniyi OO, Olaoye OO, Okunleye OJ. Effects of Information Governance (IG) on profitability in the Nigerian banking sector. Asian Journal of Economics, Business and Accounting. 2023;23(18): 22–35.
Available:https://doi.org/10.9734/ajeba/2023/v23i181055
42. Olaniyi OO. Omubo DS. WhatsApp Data Policy, Data Security, And Users' Vulnerability. The International Journal of Innovative Research & Development; 2023.
Available:https://doi.org/10.24940/ijird/2023/v12/i4/APR23021
43. Velimirovic, A. (2022, December 1). The eight types of firewalls. PhoenixNAP Global I.T.
Services.
https://phoenixnap.com/blog/types-of-firewalls
44. Velimirovic A. What Is an Intrusion Detection System? PhoenixNAP
Global I.T. Services; 2022.
Available:https://phoenixnap.com/blog/intrusion-detection-system



*Peer-review history:*
*The peer review history for this paper can be accessed here:*
*https://www.sdiarticle5.com/review-history/110417*