American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

*Article*

# SYSTEMATIC REVIEW OF CYBERSECURITY THREATS IN IOT DEVICES FOCUSING ON RISK VECTORS VULNERABILITIES AND MITIGATION STRATEGIES

**Md Tawfiqul Islam[1]; Meherun Niger[2]; Mahin Kynatun[3]; Mahmudur Rahman Mission[4];**

[1]Senior Software & Project Engineer, Authentic Four Technology, Chattogram, Bangladesh
Email: tawfiq.ctgbd@gmail.com

[2]Computer Science and Engineering, Port City International University, Chattogram, Bangladesh
Email: meherunniger3@gmail.com

[3]Computer Science and Engineering, American International University-Bangladesh, Dhaka, Bangladesh
Email: kynat.mahin@gmail.com

[4]Department of Computer Science, The Babeș-Bolyai University, Cluj-Napoca, Romania
Email: mdmission007@gmail.com

**Citation:**
Islam, M. T., Niger, M., Kynatun, M., & Mission, M. R. (2022). Systematic review of cybersecurity threats in IoT devices focusing on risk vectors vulnerabilities and mitigation strategies. *American Journal of Scholarly Research and Innovation, 1*(1), 108-136. https://doi.org/10.63125/wh17m1f9

**Received:**
July 20, 2022

**Revised:**
October 15, 2022

**Accepted:**
November 30, 2022

**Published:**
December 12, 2022



## ABSTRACT

*The rapid proliferation of Internet of Things (IoT) devices across various industries has introduced significant cybersecurity challenges, exposing critical infrastructures, smart systems, and personal devices to sophisticated cyber threats. This systematic review examines the major cybersecurity vulnerabilities in IoT ecosystems, focusing on device-level security risks, network-layer threats, application-layer vulnerabilities, and supply chain security issues. The study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, ensuring a structured, transparent, and rigorous evaluation of existing literature. A total of 120 peer-reviewed articles were analyzed, encompassing empirical research, theoretical studies, and systematic reviews published in reputable academic journals and conference proceedings. The findings reveal that weak authentication mechanisms, firmware vulnerabilities, insecure communication protocols, and supply chain risks remain persistent challenges, making IoT devices highly susceptible to botnet recruitment, malware propagation, ransomware attacks, and large-scale Distributed Denial-of-Service (DDoS) attacks. Additionally, the study identifies the limitations of conventional security solutions, emphasizing that resource-constrained IoT devices often lack robust encryption, real-time intrusion detection, and automated security updates, leaving them vulnerable to evolving cyber threats. While AI and machine learning-based intrusion detection systems offer promising advancements in threat mitigation and predictive cybersecurity, adversarial AI techniques introduce new risks that require continuous refinement of security models. The review also highlights regulatory and compliance gaps, stressing the urgent need for standardized security frameworks to ensure uniform protection across diverse IoT environments. Ultimately, this study underscores the necessity for a multi-layered security approach, integrating technological advancements, regulatory enforcement, and industry-wide collaboration to enhance IoT cybersecurity resilience. The insights provided in this review contribute to the growing body of knowledge on IoT security and serve as a foundation for future research, policy development, and practical cybersecurity implementations in smart and connected systems.*

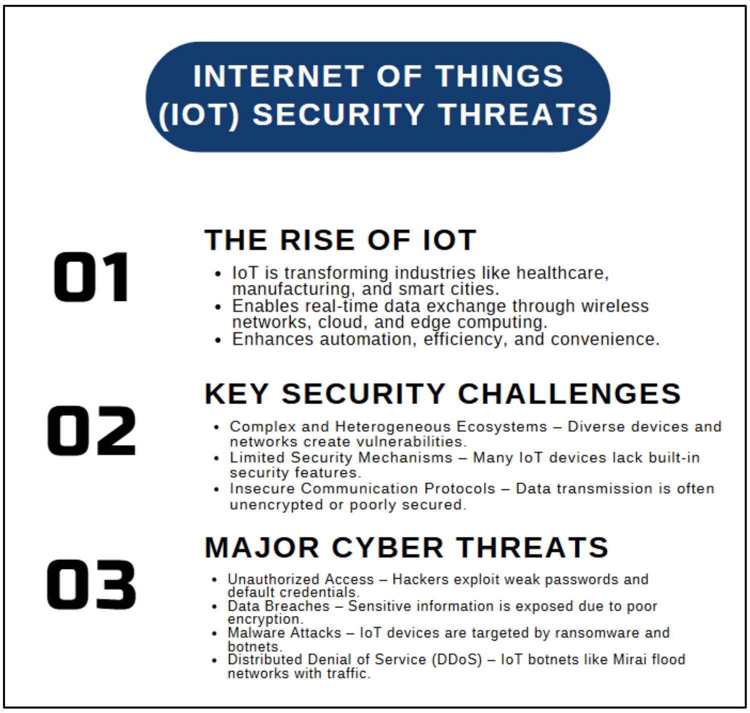
## KEYWORDS

*Cybersecurity, IoT Security, Risk Vectors, Vulnerabilities, Mitigation Strategies, Threat Analysis*

American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

## INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has significantly transformed various industries, enabling interconnected devices to enhance automation, efficiency, and convenience across healthcare, manufacturing, smart cities, and personal consumer applications (Abdul-Ghani et al., 2018). IoT devices facilitate seamless communication and real-time data exchange through wireless networks, cloud computing, and edge computing infrastructures (Mosenia & Jha, 2017). Despite these advantages, the inherent complexity and heterogeneity of IoT ecosystems have introduced significant security concerns. IoT devices are often embedded in critical infrastructure, making them attractive targets for cyber threats, including unauthorized access, data breaches, malware, and Distributed Denial of Service (DDoS) attacks (Chettri & Bera, 2020). The security vulnerabilities of IoT devices stem from a combination of limited computational capabilities, insecure communication protocols, and the widespread adoption of devices with minimal built-in security mechanisms (Chettri & Bera, 2020). As cyber threats continue to evolve, it is essential to understand the risk vectors and vulnerabilities associated with IoT security and assess the effectiveness of existing mitigation strategies.




The vulnerabilities in IoT communication protocols further exacerbate the cybersecurity risks associated with connected devices. Many IoT systems rely on lightweight protocols such as MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol), which often lack robust authentication and encryption mechanisms (Munshi et al., 2020). Attackers exploit protocol weaknesses to launch attacks such as man-in-the-middle (MITM), session hijacking, and eavesdropping, thereby compromising the integrity and confidentiality of transmitted data (Spathoulas & Karageorgopoulou, 2019). The dynamic and distributed nature of IoT environments also makes them vulnerable to botnet infections, where compromised devices are co-opted into large-scale botnets such as Mirai and Mozi, leading to massive DDoS attacks on IoT networks (Kolias et al., 2017). Botnets exploit weakly secured IoT devices to launch coordinated attacks against critical infrastructure, internet services, and cloud-based applications, causing significant operational disruptions and financial losses (Amanullah et al., 2020).

Addressing these security threats requires the implementation of comprehensive mitigation strategies that incorporate cryptographic techniques, intrusion detection systems, and AI-driven security solutions (Radanliev et al., 2019). Encryption methods such as Advanced Encryption Standard (AES), Transport Layer Security (TLS), and blockchain-based authentication models have been proposed to enhance the security of IoT communications and prevent unauthorized access (Neshenko et al., 2019). Additionally, machine learning algorithms have been increasingly utilized for anomaly detection and intrusion prevention, helping to identify abnormal patterns of behavior in IoT networks (Fernandes et al., 2019). However, the effectiveness of these security measures is contingent on their scalability and adaptability to resource-constrained IoT devices, which

Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

often have limited processing power and memory capacity (Liang et al., 2016). Despite advancements in cybersecurity frameworks, securing IoT ecosystems remains a multifaceted challenge that requires collaboration between industry stakeholders, policymakers, and cybersecurity researchers (Hesselman et al., 2020).This study systematically investigates cybersecurity threats in IoT environments by identifying key risk vectors, vulnerabilities, and mitigation strategies. It categorizes IoT security risks at the device, network, and application levels, examining how various attack methods exploit these vulnerabilities. A detailed assessment of cryptographic protocols, intrusion detection mechanisms, and AI-driven security solutions is conducted to determine their effectiveness in mitigating these threats. The study also highlights security challenges arising from inconsistent authentication mechanisms, unpatched firmware, and weak encryption protocols. By analyzing existing mitigation strategies, this research offers insights into strengthening IoT security frameworks and reducing exposure to cyber threats in interconnected environments.

## LITERATURE REVIEW

The security of Internet of Things (IoT) devices has been a growing concern due to their widespread adoption across various industries, including healthcare, smart cities, manufacturing, and consumer electronics. As IoT networks expand, so do their attack surfaces, making them susceptible to an increasing number of cybersecurity threats. Researchers have extensively studied different aspects of IoT security, focusing on risk vectors, vulnerabilities, and mitigation strategies. Prior studies have explored device-level weaknesses, network-based attacks, and security challenges arising from software and communication protocols. Additionally, various cryptographic techniques, intrusion detection systems, and AI-powered security solutions have been proposed to enhance IoT security. This section synthesizes existing research on IoT cybersecurity, categorizing it into specific areas of concern. The discussion follows a structured approach, addressing key security risks, attack methodologies, system vulnerabilities, and mitigation frameworks.

### IoT and Security

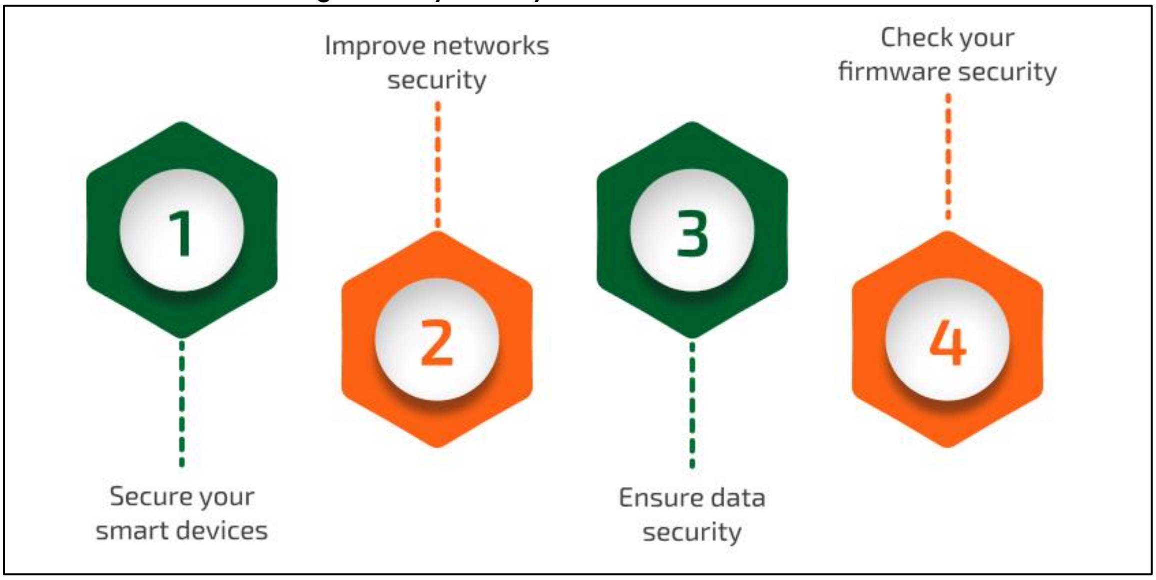
The Internet of Things (IoT) comprises a vast network of interconnected devices with diverse architectures, communication protocols, and computational capabilities, leading to significant security challenges (Elkhodr et al., 2015). Unlike traditional computing systems, IoT devices operate under a heterogeneous ecosystem that integrates various hardware and software platforms, creating security inconsistencies (Kurunathan et al., 2019). The lack of uniform security standards across manufacturers results in vulnerabilities that cybercriminals exploit to breach systems (Bertino, 2016). Many IoT devices operate on different communication protocols such as Zigbee, Bluetooth Low Energy (BLE), and Message Queuing Telemetry Transport (MQTT), each with its security limitations (Zhou et al., 2019). Studies highlight that this heterogeneous nature hinders the deployment of universal security measures, making it difficult to implement standardized encryption, authentication, and access control mechanisms across all IoT devices (Manimurugan et al., 2020). The diversity of IoT devices, ranging from industrial control systems to consumer smart home appliances, further complicates security management due to varying computational capacities and network configurations (Aman & Snekkenes, 2013). This fragmented landscape exposes IoT networks to cyber threats, including data breaches, unauthorized access, and large-scale distributed denial-of-service (DDoS) attacks (Rahim et al., 2021).

The limited computational power and energy constraints of IoT devices further hinder the implementation of robust security mechanisms (Kolias et al., 2017). Many IoT devices are designed for minimal power consumption and low-cost operation, leaving little room for advanced encryption and intrusion detection systems (Radanliev et al., 2019). Unlike traditional computers, which can accommodate complex cryptographic algorithms, IoT devices often lack sufficient memory and processing power to support such security measures (Amanullah et al., 2020). As a result, lightweight encryption techniques such as Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) are employed to balance security with performance, but they are still prone to vulnerabilities due to resource constraints (Amanullah et al., 2020). Additionally, the frequent use of

American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

default passwords, weak authentication mechanisms, and firmware vulnerabilities in IoT devices increase their susceptibility to brute-force attacks and unauthorized access (Neshenko et al., 2019). Researchers emphasize that manufacturers often prioritize cost-effectiveness and functionality over security, leading to the proliferation of devices with inadequate protection mechanisms (Radanliev et al., 2019). The absence of secure boot mechanisms and secure key storage further weakens device resilience against firmware tampering and unauthorized modifications (Al-Hadhrami & Hussain, 2021).

**Figure 1: Key Security Measures for IoT Networks**



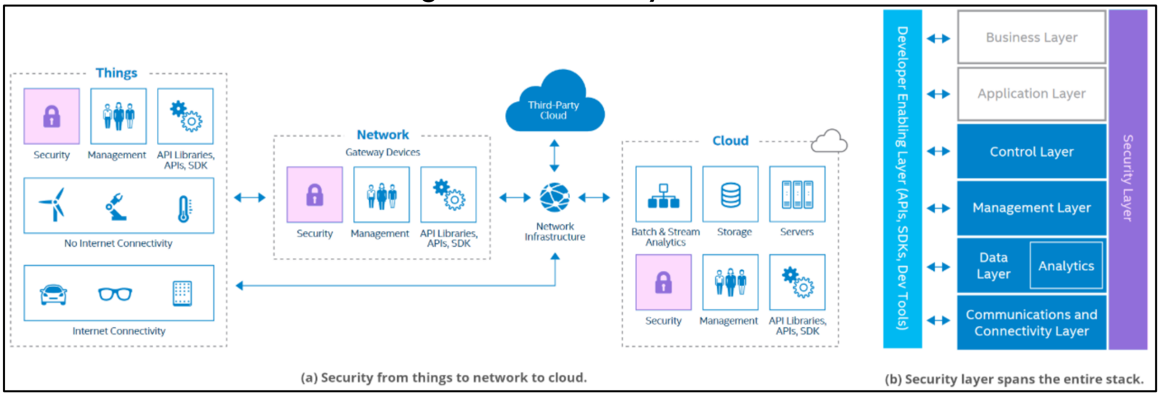

The high degree of interconnectivity within IoT networks creates an expanded attack surface, as each connected device represents a potential entry point for cyber threats (Sohal et al., 2018). IoT ecosystems integrate numerous devices that continuously exchange data, making them vulnerable to man-in-the-middle (MITM) attacks, session hijacking, and data interception (Munshi et al., 2020). Weak encryption in data transmission protocols such as CoAP and MQTT exacerbates these risks, allowing attackers to exploit communication channels and gain unauthorized access to sensitive information (Elkhodr et al., 2015). Research indicates that IoT botnets, such as the Mirai botnet, leverage insecure IoT devices to launch large-scale cyberattacks, including DDoS attacks that disrupt critical infrastructure and online services (Bertino, 2016). The interconnected nature of IoT also raises concerns regarding lateral movement attacks, where once a single device is compromised, an attacker can infiltrate the entire network (Kumar & Bhama, 2019). Given the lack of network segmentation in many IoT deployments, attackers can easily propagate malware across interconnected devices, leading to widespread system failures (Hesselman et al., 2020). Scalability is another critical challenge in securing IoT environments, as the rapid growth in connected devices intensifies security management complexities (Elkhodr et al., 2015). With billions of devices expected to be integrated into global IoT networks, security frameworks must accommodate large-scale deployments while maintaining robust access controls and threat detection mechanisms (Manimurugan et al., 2020). However, research highlights that existing security models struggle to handle the dynamic and decentralized nature of IoT infrastructures (Xhafa et al., 2020). Traditional network security mechanisms, such as firewalls and intrusion detection systems, are often insufficient in large-scale IoT networks due to high traffic volume and diverse device configurations (Rahim et al., 2021). Moreover, the scalability challenge extends to secure device provisioning and identity management, where assigning and managing cryptographic credentials for millions of IoT devices remains a significant obstacle (Cao et al., 2019). Researchers propose blockchain-based authentication and decentralized identity management solutions to address these issues, yet their adoption is limited due to computational overhead and energy consumption concerns (Zhou et al., 2019).

*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

**Standardized Security Frameworks**

The absence of universal security regulations for IoT has created a fragmented and vulnerable ecosystem where security implementations vary significantly across industries and geographical regions (Manimurugan et al., 2020). Unlike traditional IT systems, which adhere to well-established security frameworks such as ISO 27001 or NIST cybersecurity guidelines, IoT security remains largely unregulated (Sun et al., 2017). Several studies highlight that the lack of a universal IoT security framework has resulted in significant disparities in security practices, leaving many devices exposed to cyber threats (Narang et al., 2018). Regulatory bodies have attempted to introduce guidelines such as the European Union's General Data Protection Regulation (GDPR) and the United States' IoT Cybersecurity Improvement Act, yet these policies focus primarily on data privacy rather than comprehensive security measures for IoT infrastructure (Aman & Snekkenes, 2013). The absence of mandatory compliance measures across all sectors allows manufacturers to prioritize cost efficiency over security, leading to the production of insecure devices (Frustaci et al., 2018). Additionally, inconsistent international policies result in fragmented security approaches, making it difficult to develop a cohesive global response to IoT cybersecurity threats (Amanullah et al., 2020).

**Figure 2: IoT Security Model**




The lack of standardized security frameworks has resulted in inconsistent security implementations across vendors, further complicating IoT security management (Radanliev et al., 2019). Vendors develop IoT devices with proprietary security architectures, often failing to adhere to common security standards due to market competition and rapid production cycles (Neshenko et al., 2019). Studies reveal that IoT manufacturers frequently overlook essential security components such as secure boot mechanisms, hardware-based encryption, and end-to-end authentication in favor of minimizing production costs (Neshenko et al., 2019). This variation in security protocols across vendors introduces interoperability challenges, making it difficult for devices from different manufacturers to communicate securely (Liang et al., 2016). Furthermore, many vendors do not provide regular firmware updates, leaving devices vulnerable to known exploits and emerging threats (Kumar & Bhama, 2019). Even when security patches are available, they often require manual installation, which many users neglect, further exacerbating the risks associated with insecure IoT deployments (Hesselman et al., 2020). The compatibility issues between legacy and modern IoT systems present another significant challenge in developing a standardized security framework (Bertino, 2016). Many industrial and critical infrastructure IoT systems rely on outdated hardware and software that lack modern security features, making them particularly vulnerable to cyberattacks (Aman & Snekkenes, 2013). Research indicates that legacy IoT systems, such as those used in energy grids, transportation networks, and manufacturing facilities, were not designed with cybersecurity in mind (Srivastava et al., 2020). These systems often use outdated communication protocols and weak encryption mechanisms, making them easy targets for cybercriminals (Das et al., 2018). The integration of modern IoT solutions into legacy environments without proper security upgrades creates additional attack surfaces, as newer devices may inherit vulnerabilities from insecure legacy systems (Zayas & Merino, 2017). The challenge of securing legacy IoT deployments is further compounded

American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

by the reluctance of organizations to replace outdated systems due to high costs and operational disruptions (Mahmoud et al., 2015).

Security inconsistencies across IoT devices and networks also contribute to significant risks in cloud-based and edge computing environments, where IoT systems store and process large volumes of sensitive data (Stočes et al., 2016). Many cloud service providers adopt their own security models, leading to variations in access control mechanisms, data encryption standards, and authentication protocols (Lee, 2020). This lack of uniformity makes it difficult for organizations to enforce consistent security policies across hybrid IoT deployments (Lee, 2020). Moreover, decentralized edge computing solutions introduce further security challenges due to their reliance on resource-constrained IoT devices that may lack robust encryption capabilities (Gubbi et al., 2013). In many cases, IoT devices offload data processing tasks to cloud or edge servers without implementing secure data transmission protocols, exposing sensitive information to interception and manipulation (Gubbi et al., 2013). Research suggests that standardized IoT security frameworks could address these inconsistencies by enforcing unified security policies across all layers of the IoT ecosystem (Lee & Lee, 2015). In the absence of universally recognized security frameworks, industry-specific security guidelines have emerged to address sectoral IoT vulnerabilities, yet their effectiveness remains limited due to inconsistent adoption (Lee, 2019). For instance, the healthcare sector follows HIPAA (Health Insurance Portability and Accountability Act) regulations for securing medical IoT devices, while industrial IoT systems may adhere to ISA/IEC 62443 standards for operational technology security (Ammar et al., 2018). However, these sector-specific frameworks often lack interoperability, creating security gaps when IoT systems operate across multiple industries (Jayashankar et al., 2018). Research highlights that while security best practices such as regular firmware updates, strong authentication mechanisms, and secure software development lifecycles can mitigate risks, their inconsistent implementation across different industries reduces their overall effectiveness (Gubbi et al., 2013). The absence of a universally enforced IoT security standard continues to pose a significant challenge, allowing attackers to exploit inconsistencies across different regulatory frameworks (Lee, 2019).

**Device-Level Security Risks**

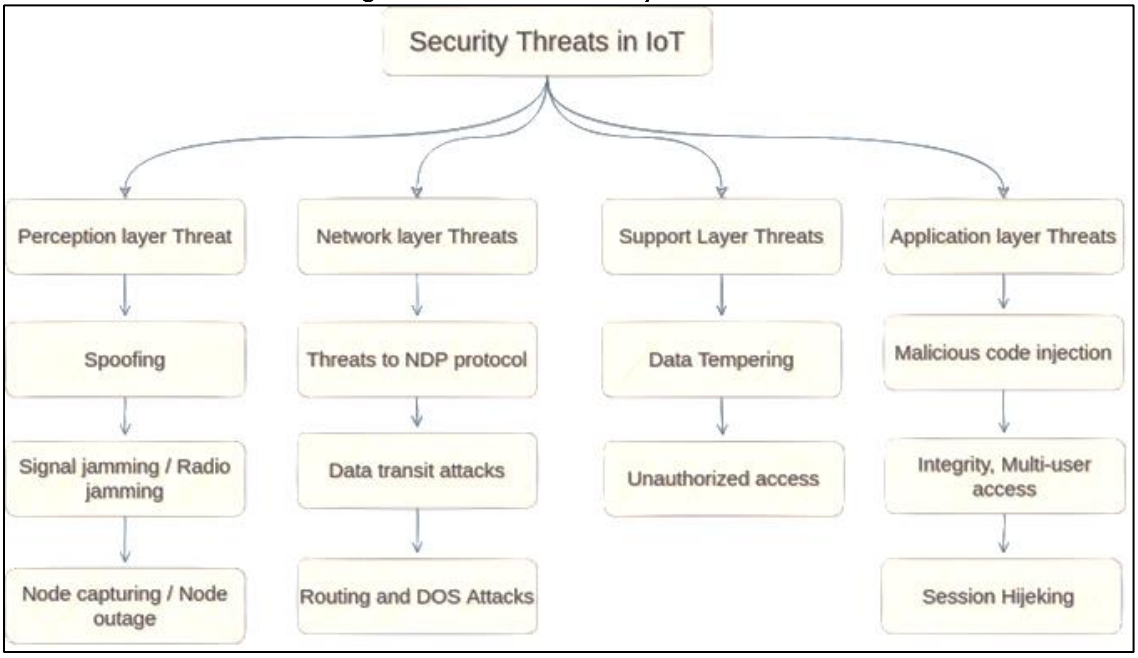
The reliance on weak authentication mechanisms and default credentials in IoT devices exposes them to significant security risks. Many IoT manufacturers preconfigure devices with default usernames and passwords, which are often left unchanged by users, creating vulnerabilities that cybercriminals can exploit (Bharati, 2019; Gubbi et al., 2013). Studies indicate that attackers leverage automated brute-force techniques to exploit weak authentication, allowing them to gain unauthorized access to IoT networks (O'Neill, 2016). The Mirai botnet, for example, exploited default credentials in IoT devices to create a massive botnet used in large-scale Distributed Denial-of-Service (DDoS) attacks (Sridhar & Smys, 2017). Weak authentication mechanisms, such as the absence of multi-factor authentication (MFA) or biometric authentication, further exacerbate these risks (Celia & Cungang, 2018). While some security frameworks recommend the enforcement of stronger authentication protocols, many IoT devices, particularly those with resource constraints, do not support such measures (Dash, 2020). As a result, unauthorized access remains a prevalent threat, allowing attackers to manipulate IoT systems, intercept sensitive data, and launch coordinated cyberattacks (Al Hayajneh et al., 2020).

Firmware vulnerabilities and unpatched software exploits represent another major security challenge for IoT devices. Many IoT manufacturers prioritize cost-efficiency and rapid deployment over security, leading to the development of devices with outdated or insecure firmware (O'Neill, 2016). Research has shown that many IoT devices lack mechanisms for automatic firmware updates, leaving them vulnerable to known exploits (Lee & Lee, 2015). Attackers often exploit firmware vulnerabilities to gain persistent access to devices, modify system functions, and introduce malware (Lee, 2019). The Stuxnet attack, for example, demonstrated how firmware exploits could be used to manipulate industrial IoT systems, leading to operational disruptions (Lee & Lee, 2015). Additionally, many IoT devices lack secure boot mechanisms, allowing attackers to replace legitimate firmware with malicious versions (Gubbi et al., 2013). Studies emphasize that secure

American Journal of Scholarly Research and Innovation
*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

firmware updates, code signing, and periodic security patches are critical to mitigating these risks (Gubbi et al., 2013; Lee, 2019; Zafeiriou, 2020). However, the absence of standardized update mechanisms across IoT manufacturers complicates security implementation (Lee & Lee, 2015).

**Figure 3: Overview Security Threats in IoT**




Unauthorized physical access to IoT devices poses a significant threat, particularly for devices deployed in uncontrolled environments. Unlike traditional computing systems, which are often protected by physical security measures, many IoT devices are installed in public or easily accessible locations, making them susceptible to tampering (Gubbi et al., 2013). Attackers can exploit physical access to manipulate hardware, extract sensitive information, or install rogue firmware (Lee & Lee, 2015). Research indicates that attackers frequently use JTAG (Joint Test Action Group) debugging interfaces or serial ports to bypass authentication mechanisms and gain control over IoT devices (Ding et al., 2020). Side-channel attacks, such as electromagnetic analysis and power consumption monitoring, further enable attackers to extract cryptographic keys and other sensitive data from IoT devices (Kandasamy et al., 2020). Industrial IoT systems, smart meters, and medical IoT devices are particularly vulnerable to these types of attacks due to their widespread deployment in open environments (Bendavid et al., 2018). Strengthening physical security through tamper-resistant hardware, secure enclosures, and encrypted storage is essential to reducing the risks associated with unauthorized access (Ahemd et al., 2017; Xiao et al., 2018).

Side-channel attacks exploit unintended information leakage from IoT devices to extract cryptographic keys, infer system states, or manipulate device operations. Unlike traditional hacking techniques that rely on software-based vulnerabilities, side-channel attacks leverage indirect information such as power consumption patterns, electromagnetic emissions, or acoustic signals to compromise security (Burhan et al., 2018). Studies have demonstrated that even minimal variations in power consumption during cryptographic operations can be analyzed to extract private keys, allowing attackers to decrypt sensitive communications (Burhan et al., 2018; Ding et al., 2020). IoT devices deployed in critical infrastructure, such as smart grids and industrial automation systems, are particularly vulnerable to such attacks (Kandasamy et al., 2020). Attackers can also use differential power analysis (DPA) and electromagnetic interference (EMI) analysis to gain insights into a device's internal operations, enabling them to modify firmware or extract sensitive data (Zafeiriou, 2020). While hardware security enhancements such as power randomization and shielded enclosures can help mitigate side-channel attacks, their implementation remains limited due to cost and design constraints (Jayashankar et al., 2018; Yassine et al., 2019).

*Volume 01 Issue 01 (2022)*
Page No: 108-136
*DOI:10.63125/wh17mf19*

The growing interconnectivity of IoT devices further amplifies device-level security risks by enabling attackers to exploit vulnerabilities in one device to compromise an entire network. Research highlights that once an attacker gains access to a poorly secured IoT device, they can move laterally across connected systems, exfiltrating sensitive data and deploying malware (Xiao et al., 2018). Many IoT networks lack proper segmentation, allowing attackers to use compromised devices as entry points to infiltrate broader infrastructures (Ahemd et al., 2017). This issue is particularly concerning in industrial and healthcare IoT deployments, where compromised medical devices or industrial controllers can disrupt critical operations (Pal et al., 2018). Secure boot mechanisms, strong authentication, and encrypted communication channels are necessary to prevent attackers from leveraging one device's vulnerability to exploit entire networks (Meneghello et al., 2019). However, studies suggest that many IoT deployments lack these protections, leaving them susceptible to cascading security failures (Ahemd et al., 2017).

**Network-Level Threats**

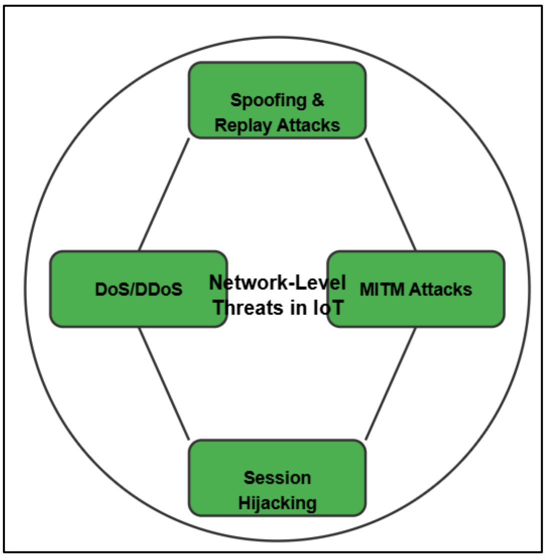
Man-in-the-middle (MITM) attacks and packet sniffing pose significant security risks in IoT environments, allowing attackers to intercept and manipulate communication between devices (Ganapathi & Shanmugapriya, 2009). IoT networks often rely on lightweight protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), which lack built-in encryption and authentication mechanisms, making them susceptible to MITM attacks (Benzarti et al., 2017). Attackers exploit these vulnerabilities by positioning themselves between IoT devices and their intended communication endpoints to eavesdrop, modify, or inject malicious data (Alimi et al., 2020). Research highlights that insecure Wi-Fi connections and improperly configured public networks significantly increase the risk of MITM attacks in smart home and industrial IoT deployments (Hodo et al., 2016). Packet sniffing, a technique used to capture network traffic, is another major concern, as it allows attackers to analyze transmitted data and extract sensitive information, such as authentication credentials and encryption keys (Pacheco & Hariri, 2016). The lack of transport layer security (TLS) in many IoT devices further exacerbates these risks, exposing unencrypted traffic to adversaries who can manipulate real-time data flows (Doshi et al., 2021).

Denial-of-service (DoS) and Distributed Denial-of-Service (DDoS) attacks exploit IoT devices' resource constraints, overwhelming them with excessive requests to render them inoperable (Turcotte et al., 2017). Research indicates that IoT devices, due to their limited processing power and lack of security hardening, are prime targets for attackers seeking to disrupt network availability (Pajouh et al., 2019). Large-scale DDoS attacks, such as those conducted by the Mirai botnet, have demonstrated the devastating impact of IoT-based attacks on critical infrastructure and internet services (Turcotte et al., 2017). Attackers hijack poorly secured IoT devices, such as smart cameras and routers, integrating them into massive botnets to launch high-volume traffic floods against targeted servers (Yu et al., 2019). Studies show that the lack of rate-limiting mechanisms and anomaly detection systems in many IoT networks enables attackers to sustain prolonged DoS attacks, leading to widespread service disruptions (Muhuri et al., 2020; Yu et al., 2019). Moreover, attackers can leverage amplification techniques, such as DNS and NTP reflection, to intensify the impact of these attacks while masking their true source (Vasserman & Hopper, 2013).

Spoofing attacks, replay attacks, and session hijacking compromise the integrity and confidentiality of IoT communications by exploiting authentication weaknesses and protocol vulnerabilities (Nagrath & Gupta, 2011). Spoofing attacks occur when an adversary forges a device's identity to gain unauthorized access to a network, often by impersonating a legitimate IoT device (Yu et al., 2019). Studies highlight that many IoT authentication mechanisms rely solely on weak, pre-shared keys or static credentials, making them highly vulnerable to identity spoofing (Vasserman & Hopper, 2013). Replay attacks involve intercepting and retransmitting legitimate authentication packets, allowing attackers to bypass security measures and gain unauthorized access to IoT systems (Anirudh et al., 2017). These attacks are particularly effective against IoT protocols that lack cryptographic nonce implementation, which prevents the reuse of authentication tokens (Turcotte et al., 2017). Session hijacking further exploits weak authentication mechanisms by allowing an attacker to take control of an active session, potentially manipulating IoT device settings or extracting confidential data (Nagrath & Gupta, 2011). Research underscores the need for secure session management techniques, such as time-based expiration tokens and multi-factor authentication, to mitigate these threats (Pajouh et al., 2019).

The widespread use of insecure network architectures in IoT deployments exacerbates the risks associated with network-level threats. Many IoT devices operate on flat, unsegmented networks where all devices share the same communication space, increasing the risk of lateral movement attacks (Agah & Das, 2007). Once an attacker gains access to a single IoT device, they can traverse the network, targeting other connected systems and escalating privileges (Li et al., 2017). Research indicates that industrial IoT environments, such as smart grids and automated manufacturing plants, are particularly susceptible to these attacks due to their reliance on legacy network protocols with minimal security enforcement (Obaidat et al., 2020). Furthermore, IoT gateways and edge computing nodes, which act as intermediaries between IoT devices and cloud services, are often targeted by attackers seeking to intercept data streams or inject malicious payloads (Hsu et al., 2020). Network segmentation, firewall enforcement, and zero-trust security models have been proposed as effective mitigation strategies; however, their adoption remains inconsistent across IoT deployments due to performance concerns and lack of standardized security policies (Hayajneh et al., 2019).

**Figure 4: Key Security Measures for IoT Networks**




Research also highlights that the lack of end-to-end encryption in IoT communications contributes to the persistence of network-level threats (Chen et al., 2021). Many IoT protocols prioritize low power consumption and minimal processing overhead, leading to the omission of robust encryption schemes such as TLS or IPsec (Choraś et al., 2011). As a result, attackers can easily intercept and manipulate unencrypted traffic, leading to data exfiltration, unauthorized command injection, and malicious firmware updates (Garg et al., 2019). Studies emphasize that cryptographic solutions, such as lightweight AES encryption and elliptic curve cryptography (ECC), can significantly enhance IoT network security without introducing excessive computational overhead (Ganapathi & Shanmugapriya, 2009). However, the fragmented nature of IoT ecosystems, with different manufacturers implementing proprietary security models, complicates the widespread deployment of standardized encryption protocols (Kayes et al., 2020). The integration of AI-driven intrusion detection systems and blockchain-based authentication frameworks has been explored as potential solutions, yet their effectiveness depends on device compatibility and implementation consistency (Vishwakarma & Jain, 2019).

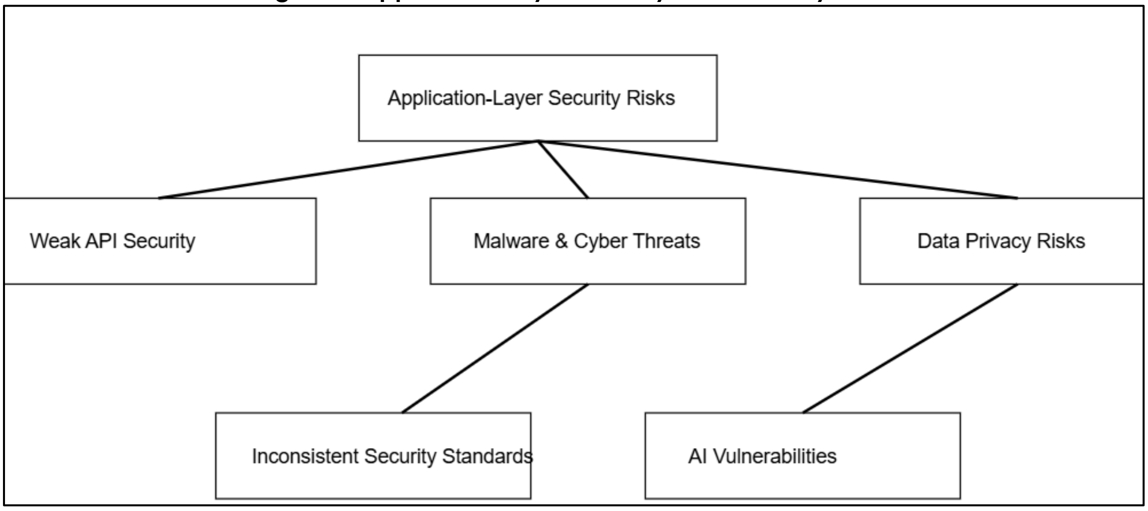
### Application-Layer Vulnerabilities

Insecure application programming interfaces (APIs) and improper data access controls expose IoT applications to significant security risks. Many IoT applications rely on APIs to facilitate communication between devices, cloud platforms, and third-party services, but these APIs often lack proper authentication, encryption, and access control mechanisms (Hodo et al., 2016). Research indicates that improperly secured APIs allow attackers to intercept and manipulate data transmissions, leading to unauthorized access and control over IoT systems (Puthal et al., 2016). Weak API authentication mechanisms, such as hardcoded credentials and tokens stored in plaintext, further exacerbate these risks, making IoT applications vulnerable to credential theft and replay attacks (Hodo et al., 2016). Additionally, improper data access controls in IoT ecosystems enable attackers to

*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

bypass authorization policies, exposing sensitive user data and critical system configurations to cyber threats (Alimi et al., 2020). Studies emphasize that enforcing robust API security measures, such as OAuth-based authentication, token expiration policies, and encrypted API communications, is essential for mitigating application-layer vulnerabilities (Benzarti et al., 2017). However, many IoT vendors prioritize functionality over security, leading to widespread deployment of poorly secured APIs in consumer and industrial IoT applications (Hodo et al., 2016).

**Figure 5: Application-Layer Security Risks in IoT Systems**




Malware propagation and ransomware threats in IoT applications have become increasingly prevalent, targeting devices with weak security configurations and outdated software (Benzarti et al., 2017). IoT devices frequently operate with minimal antivirus protection and lack traditional security defenses found in conventional computing environments, making them attractive targets for malware infections (Alimi et al., 2020). Studies highlight that botnets such as Mirai and Mozi exploit unpatched vulnerabilities in IoT applications to compromise devices, integrating them into large-scale botnet networks used for distributed denial-of-service (DDoS) attacks (Hodo et al., 2016). Ransomware attacks on IoT applications have also escalated, with cybercriminals encrypting critical system files and demanding payments for decryption keys (Chen et al., 2021). Smart home devices, industrial control systems, and healthcare IoT applications are particularly vulnerable to such attacks, as their disruption can lead to severe operational consequences (Khare et al., 2020). Research suggests that the lack of security patches and automated update mechanisms in many IoT applications further facilitates malware propagation, as attackers exploit known vulnerabilities that remain unpatched for extended periods (Bhattasali et al., 2012). Implementing secure software development lifecycles, continuous vulnerability monitoring, and endpoint security solutions are critical to preventing malware and ransomware threats in IoT (Pathak et al., 2020).

Privacy concerns related to data collection and storage in IoT applications have raised significant ethical and security issues, as many IoT devices continuously gather and transmit sensitive user information without robust privacy protections (Agah & Das, 2007). IoT applications in healthcare, smart homes, and wearable technology collect personal and biometric data, often storing it on centralized cloud platforms that are susceptible to breaches and unauthorized access (Moridi et al., 2018). Studies show that many IoT applications lack proper data anonymization techniques, allowing attackers to correlate stored information with specific individuals, leading to identity theft and unauthorized profiling (Agah & Das, 2007). Additionally, weak encryption protocols in data transmission channels expose collected information to eavesdropping and MITM attacks, further amplifying privacy risks (Moridi et al., 2018). Research highlights that many IoT applications fail to provide users with adequate transparency and control over their data, often sharing information with third-party advertisers and analytics companies without explicit consent (Hayajneh et al., 2019). Strengthening data encryption mechanisms, enforcing strict

*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

access controls, and adopting privacy-by-design principles are necessary to enhance privacy protections in IoT ecosystems (Yu et al., 2018).

The lack of standardized security frameworks in IoT application development exacerbates application-layer vulnerabilities, leading to inconsistencies in security implementations across different platforms and vendors (Obaidat et al., 2020)). Many IoT applications are developed without formal security testing, allowing insecure coding practices to persist across production environments (Moridi et al., 2018). Studies indicate that buffer overflow vulnerabilities, race conditions, and input validation flaws frequently appear in IoT software, enabling attackers to execute arbitrary code and gain control over applications (Hsu et al., 2020; Moridi et al., 2018). Additionally, the use of open-source libraries and third-party dependencies without proper security vetting introduces additional risks, as vulnerabilities in these components can compromise the entire IoT application ecosystem (Georgescu et al., 2019). Research suggests that adopting secure coding practices, implementing static and dynamic code analysis tools, and conducting penetration testing during software development can help mitigate these threats (Khouzani & Sarkar, 2011). However, the rapid pace of IoT innovation often prioritizes product deployment over security compliance, resulting in widespread application-layer security gaps (Lee et al., 2014).

**Analysis of Common Cybersecurity Threats in IoT**

The Mirai botnet is one of the most well-documented cyber threats that demonstrated the vulnerabilities of IoT devices at a global scale. Mirai exploited weak authentication mechanisms in IoT devices by using a database of default credentials to gain unauthorized access (Agah & Das, 2007; Ahmed et al., 2022; Aklima et al., 2022). Once compromised, the infected devices were recruited into a botnet that launched massive Distributed Denial-of-Service (DDoS) attacks against online services, websites, and critical infrastructure (Ahmed et al., 2022; Aklima et al., 2022; Mahfuj et al., 2022; Saad et al., 2011; Sohel et al., 2022; Tonoy, 2022). The attack on Dyn, a major DNS service provider, in October 2016, resulted in widespread internet outages, impacting platforms such as Twitter, Netflix, and Reddit (Hsu et al., 2020). Studies have shown that the Mirai botnet primarily targeted unsecured IoT devices, such as network cameras and routers, taking advantage of their weak security configurations and lack of user intervention in security updates (Hayajneh et al., 2019). The large-scale impact of Mirai highlighted the risks posed by unprotected IoT devices and underscored the urgent need for better authentication and security patch management in IoT ecosystems (Li et al., 2017).

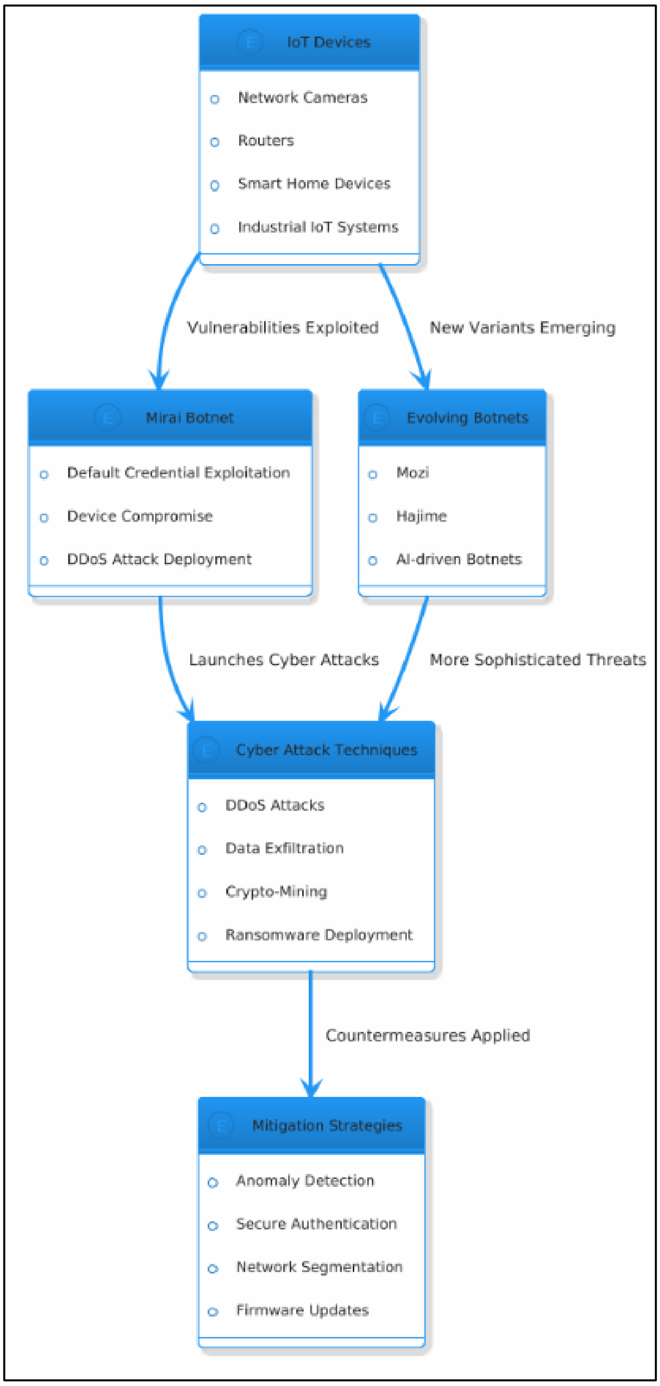
The evolution of botnets in IoT ecosystems has further amplified cybersecurity threats, as attackers continue to develop more sophisticated attack techniques. Following Mirai, several botnet variants, including Mozi and Hajime, emerged, leveraging advanced evasion techniques such as peer-to-peer communication to avoid detection (Obaidat et al., 2020). Unlike traditional botnets that rely on centralized command-and-control servers, newer botnets employ decentralized architectures, making them harder to dismantle (Hayajneh et al., 2019). Research highlights that botnets have evolved beyond DDoS attacks to support a wide range of cyber threats, including data exfiltration, crypto-mining, and ransomware deployment in IoT networks (Benzarti et al., 2017). Industrial IoT (IIoT) systems have been particularly affected, as botnet infections can disrupt manufacturing processes, energy grids, and smart transportation systems (Puthal et al., 2016). The increasing adoption of AI-driven botnets further complicates security efforts, as these botnets can autonomously adapt to network defenses and exploit newly discovered vulnerabilities (Turcotte et al., 2017). Researchers emphasize that mitigating botnet threats requires a combination of proactive security measures, including real-time anomaly detection, device authentication, and network segmentation (Nagrath & Gupta, 2011).

American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

### Exploitation of Weak Communication Protocols

The reliance on lightweight communication protocols, such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), introduces significant security weaknesses in IoT networks. MQTT is widely used for real-time communication between IoT devices due to its low overhead and efficient messaging capabilities (Dinculeană & Cheng, 2019). However, research indicates that MQTT lacks built-in security features, such as encryption and authentication, making it susceptible to attacks such as man-in-the-middle (MITM), session hijacking, and unauthorized data access (Perrone et al., 2017). Attackers can intercept unencrypted MQTT messages, manipulate device commands, and disrupt IoT operations by injecting malicious payloads (Xiao et al., 2018). CoAP, another widely used IoT protocol, is also vulnerable to security threats due to its reliance on the User Datagram Protocol (UDP), which lacks inherent mechanisms for ensuring data integrity and confidentiality (Burhan et al., 2018). Studies show that CoAP is frequently exploited in amplification attacks, where attackers use the protocol to generate high-volume DDoS traffic by leveraging IoT devices as attack sources (Ahemd et al., 2017). The lack of authentication and encryption in both MQTT and CoAP makes IoT devices an easy target for cybercriminals who exploit communication weaknesses to infiltrate networks and exfiltrate sensitive data (Khan & Salah, 2018). The absence of end-to-end encryption in lightweight IoT protocols exacerbates security risks, allowing attackers to intercept and manipulate data exchanges between devices and cloud services. Many IoT devices transmit sensitive information, such as health records, industrial sensor data, and smart home activity logs, without adequate encryption mechanisms (Ding et al., 2020). Studies highlight that even when encryption is implemented, it is often limited to transport layer security (TLS), which does not provide full protection for all data transmitted across the network (Burhan et al., 2018; Ding et al., 2020). Attackers exploit weak encryption implementations to launch replay attacks, eavesdrop on communication

**Figure 6: Security Threats and Mitigation Strategies in IoT Communication Protocols**

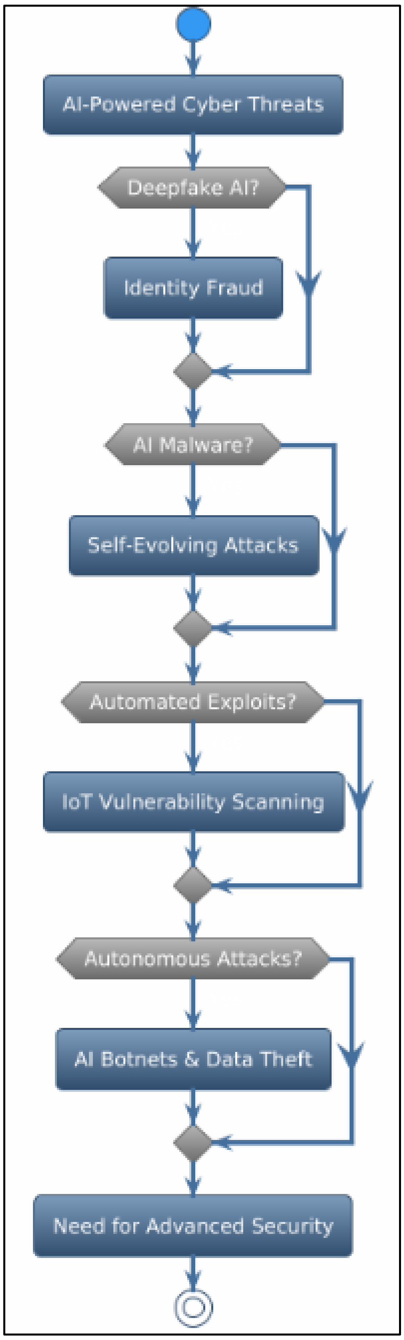


Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

channels, and modify command instructions sent to IoT devices (Xiao et al., 2018). The lack of robust key management further compounds these vulnerabilities, as IoT devices often store encryption keys in plaintext or share them across multiple devices, making them susceptible to theft (Ahemd et al., 2017). Research suggests that implementing lightweight cryptographic solutions, such as elliptic curve cryptography (ECC) and quantum-resistant encryption, can enhance the security of IoT communication protocols while maintaining computational efficiency (Xiao et al., 2018).

The fragmentation of security implementations across IoT manufacturers has resulted in inconsistent security measures, further increasing the risk of protocol exploitation. Many IoT vendors prioritize performance and cost reduction over security, leading to the widespread deployment of devices with minimal cryptographic protection (Burhan et al., 2018). Studies indicate that some IoT devices completely disable encryption or rely on outdated cryptographic algorithms that are vulnerable to modern cryptanalysis techniques (Bendavid et al., 2018). Additionally, many IoT applications lack mechanisms for secure key exchange, making it easy for attackers to compromise authentication credentials and decrypt sensitive data (Ali et al., 2018). The security gaps in IoT communication protocols have also enabled large-scale attacks targeting industrial control systems, healthcare networks, and financial transactions conducted through IoT-enabled point-of-sale systems (Zheng et al., 2018). To mitigate these risks, researchers emphasize the need for standardized security frameworks that enforce strong encryption, secure key management, and mutual authentication for all IoT communications (Kulseng et al., 2010).

**Figure 7: AI-Powered Cyber Threats in IoT**




**AI-Powered Cyber Threats**

Deepfake-based attacks and adversarial AI techniques have emerged as significant threats in modern cybersecurity landscapes, particularly in IoT environments. Deepfake technology, which leverages deep learning models to generate highly realistic synthetic media, has been increasingly exploited for identity fraud, misinformation campaigns, and social engineering attacks (Kim et al., 2020). Studies have shown that cybercriminals use deepfake-generated voice and video content to impersonate executives, conduct fraudulent transactions, and manipulate authentication mechanisms in IoT applications (Suciu et al., 2017). Additionally, adversarial AI techniques exploit vulnerabilities in machine learning models by injecting manipulated inputs to deceive AI-driven security systems (Li et al., 2019). Research indicates that attackers can craft adversarial samples that force AI-based intrusion detection systems to misclassify malicious activity as benign, thereby bypassing security measures (Mahmood, 2020). The increasing reliance on AI-powered authentication methods, such as facial recognition and voice verification, further amplifies the risks posed by adversarial AI attacks, as attackers can generate synthetic biometric data to gain unauthorized access to IoT networks (Velliangiri et al., 2020). The proliferation of deepfake and adversarial AI attacks highlights the limitations of traditional cybersecurity

*Volume 01 Issue 01 (2022)*
Page No: 108-136
*DOI:10.63125/wh17mf19*

approaches in detecting and mitigating AI-driven threats (Suciu et al., 2017).

AI-driven malware has introduced a new dimension of cyber threats by enabling malware to autonomously adapt to evolving security defenses. Unlike conventional malware, AI-enhanced malware utilizes reinforcement learning and generative adversarial networks (GANs) to evade detection, dynamically alter its attack patterns, and exploit IoT vulnerabilities in real time (Sun et al., 2017). Research has shown that AI-powered malware can autonomously assess an IoT system's security posture, identify weaknesses, and modify its code to bypass firewalls and antivirus software (Du et al., 2009). This level of adaptability makes AI-driven malware particularly effective in IoT environments, where traditional signature-based detection methods struggle to identify novel attack vectors (Suciu et al., 2017). Additionally, AI-powered ransomware attacks have increased, with attackers leveraging machine learning to optimize encryption techniques, predict the most valuable files to target, and customize ransom demands based on an organization's financial data (Anand et al., 2020). The use of AI in malware development signifies a shift toward more autonomous and sophisticated cyberattacks that require advanced behavioral analytics and AI-driven security measures to counteract (Du et al., 2009).

The autonomous exploitation of IoT vulnerabilities using AI has enabled cybercriminals to conduct large-scale, automated attacks with minimal human intervention. AI-driven attack frameworks can scan vast IoT networks, identify security weaknesses, and deploy tailored exploits without requiring predefined rule sets (Du et al., 2009; Velliangiri et al., 2020). Research indicates that AI-powered penetration testing tools can mimic ethical hacking techniques to uncover vulnerabilities, but similar technologies have been weaponized by attackers to infiltrate IoT infrastructures (Kim et al., 2020; Mahmood, 2020). These autonomous systems can launch MITM (man-in-the-middle) attacks, modify IoT firmware, and exploit unpatched software vulnerabilities at unprecedented speeds (Suciu et al., 2017). Studies have demonstrated that AI can enhance polymorphic malware, enabling it to rewrite its own code to avoid detection while propagating through IoT networks (Velliangiri et al., 2020). The self-learning capabilities of AI-driven exploits make them highly resilient to conventional cybersecurity defenses, as they continuously evolve to evade detection and maximize attack success rates (Wu et al., 2020).

One of the most concerning aspects of AI-powered cyber threats is the potential for fully autonomous cyberattacks that require minimal human oversight. Recent advancements in AI have enabled attackers to develop intelligent attack frameworks capable of launching sophisticated multi-vector attacks against IoT infrastructures (Carlini & Wagner, 2017). These frameworks can analyze network traffic, detect security gaps, and generate tailored attack strategies in real time (Sun et al., 2017). Studies suggest that AI can optimize distributed botnet attacks by dynamically coordinating compromised IoT devices to launch synchronized DDoS attacks against high-value targets (Velliangiri et al., 2020). Furthermore, AI-driven cyberattacks can leverage predictive analytics to anticipate an organization's security responses and adjust attack methodologies accordingly (Anand et al., 2020; Wu et al., 2020). The ability of AI to autonomously identify and exploit IoT vulnerabilities has raised concerns regarding the increasing asymmetry between attackers and defenders, as traditional security models struggle to keep pace with AI-enhanced threats (Bendavid et al., 2018).

The integration of AI into cyberattacks has also facilitated the emergence of advanced persistent threats (APTs) that remain undetected within IoT ecosystems for extended periods. AI-powered APTs utilize stealth tactics such as data exfiltration through encrypted traffic, behavioral cloaking to evade anomaly detection, and adaptive malware deployment to blend into legitimate network activity (Burhan et al., 2018). Studies have revealed that AI-enhanced malware can mimic normal IoT device behavior to evade security controls while gradually extracting sensitive data (Ding et al., 2020). Additionally, AI-driven cyber espionage campaigns have been observed targeting industrial control systems, healthcare IoT networks, and critical infrastructure, highlighting the growing sophistication of AI-enhanced cyber threats (Yassine et al., 2019). The ability of AI to autonomously infiltrate, learn from, and manipulate IoT environments presents an unprecedented challenge for cybersecurity professionals, requiring the development of

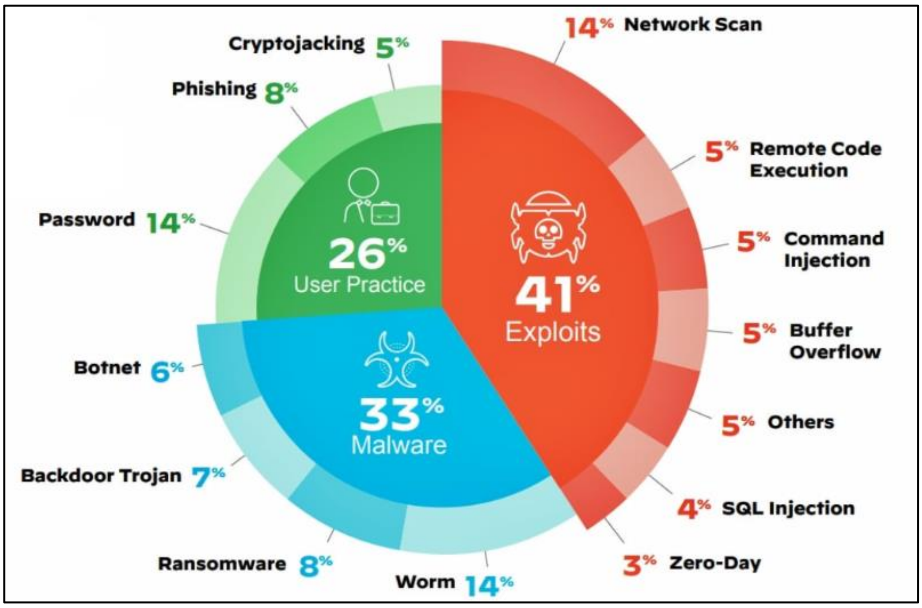
American Journal of Scholarly Research and Innovation
Volume 01 Issue 01 (2022)
Page No: 108-136
DOI:10.63125/wh17mf19

AI-driven defensive systems capable of countering adaptive threats in real time (Zafeiriou, 2020).

**Supply Chain Security Risks in IoT Device Manufacturing**

The presence of hardware-level backdoors in IoT devices poses a significant security threat, as these vulnerabilities can be exploited for espionage, unauthorized access, and large-scale cyberattacks. Hardware backdoors are intentionally or unintentionally embedded within IoT devices during the manufacturing process, allowing malicious actors to gain persistent access to systems (Makhdoom et al., 2019). Studies highlight that compromised hardware components can be activated remotely to manipulate device functionality, extract sensitive data, or disrupt operations (Yang et al., 2015). Research indicates that many backdoors are introduced during the supply chain process, where different components are sourced from multiple vendors, increasing the risk of tampering (Makhdoom et al., 2019). Attackers often exploit weak security controls in manufacturing facilities to insert malicious microcode or alter firmware before devices reach consumers (Muthavhine & Sumbwanyambe, 2018). Once activated, hardware backdoors can bypass encryption mechanisms, intercept communication channels, and allow attackers to install undetectable malware (Kim et al., 2020). These vulnerabilities are particularly concerning in critical infrastructure sectors, such as energy, healthcare, and military applications, where compromised IoT devices can lead to severe operational consequences (Khan & Herrmann, 2017).

**Figure 8: IoT Security Threat Landscape: Exploits, Malware, and User Vulnerabilities**




Supply chain tampering remains a growing concern in IoT device security, as the globalized production process makes it difficult to verify the integrity of hardware and firmware components (Mukaddam et al., 2014). Many IoT manufacturers rely on third-party suppliers to source chips, sensors, and microcontrollers, creating opportunities for malicious modifications to be introduced at various stages of production (Vasques & Gondim, 2019). Studies indicate that attackers exploit this fragmented supply chain to implant rogue firmware, counterfeit chips, and logic bombs that activate after deployment (Muthavhine & Sumbwanyambe, 2018). In some cases, supply chain attacks involve inserting malicious modifications into firmware updates, allowing attackers to compromise IoT devices post-manufacture (Khan & Herrmann, 2017). Research highlights that supply chain tampering incidents, such as the alleged Supermicro motherboard attack, have demonstrated the feasibility of hardware-level infiltration, raising concerns about the security of IoT manufacturing practices (Vasques & Gondim, 2019). Due to the complexity of supply chains, manufacturers often struggle to conduct comprehensive security audits,

*Volume 01 Issue 01 (2022)*
Page No: 108-136
*DOI:10.63125/wh17mf19*

increasing the risk of undetected vulnerabilities in widely deployed IoT devices (Nirmal et al., 2020).

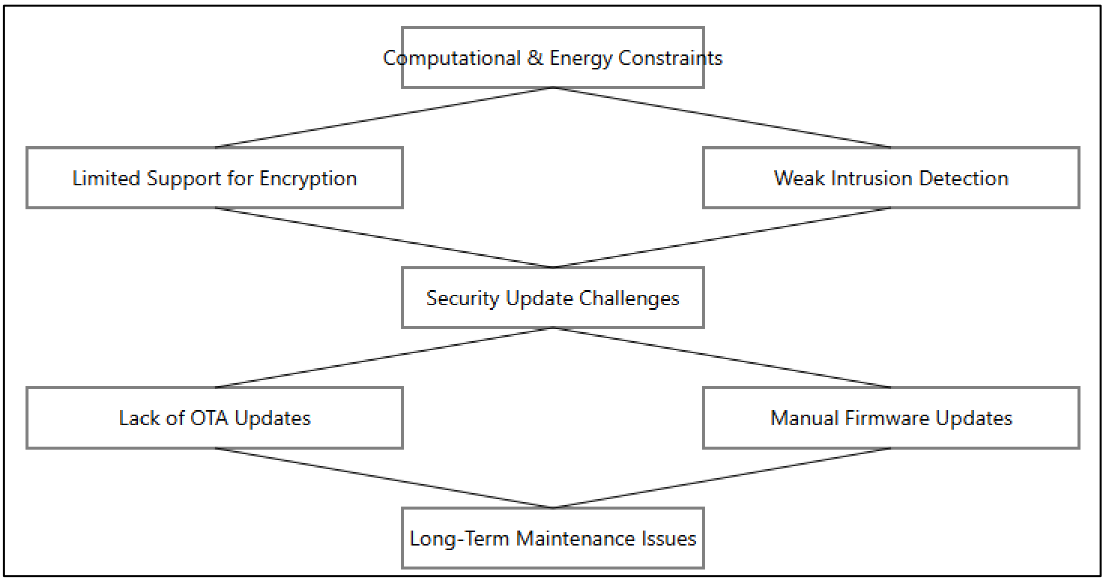
Third-party vendors play a critical role in IoT device manufacturing, but their involvement introduces significant security risks due to inconsistent security policies, lack of oversight, and vulnerabilities in outsourced components (Mukaddam et al., 2014). Many IoT manufacturers outsource hardware design, software development, and cloud infrastructure to external suppliers, leading to security blind spots that attackers can exploit (Ma et al., 2019). Studies show that third-party vendors often prioritize cost efficiency and production speed over security, resulting in devices with weak encryption, default credentials, and outdated firmware (Khan & Herrmann, 2017; Ma et al., 2019). Additionally, supply chain attacks targeting third-party vendors have been responsible for some of the largest cybersecurity breaches, as compromised suppliers inadvertently introduce malware and vulnerabilities into widely used IoT products (Makhdoom et al., 2019). The interconnected nature of IoT ecosystems further amplifies these risks, as security weaknesses in a single component can be leveraged to exploit entire networks (Froytlog & Cenkeramaddi, 2018). Researchers emphasize the need for strict vendor security assessments, continuous monitoring, and secure software supply chain practices to mitigate risks associated with third-party dependencies (Saraeian & Golchi, 2020).

The use of open-source software and third-party libraries in IoT firmware development introduces additional security concerns, as vulnerabilities in shared codebases can be exploited across multiple devices. Many IoT manufacturers integrate third-party libraries without conducting thorough security reviews, allowing attackers to exploit unpatched vulnerabilities in widely deployed software components (Iqbal et al., 2020). Studies indicate that dependency confusion attacks, in which attackers inject malicious code into open-source repositories, have been increasingly used to compromise IoT applications (Baybutt, 2002; Iqbal et al., 2020; Zavrak & Iskefiyeli, 2020). Additionally, outdated libraries and improperly validated updates create persistent security risks, as many IoT devices lack automated patching mechanisms to mitigate newly discovered vulnerabilities (Asplund & Nadjm-Tehrani, 2016). Research highlights that supply chain attacks leveraging third-party software vulnerabilities can lead to large-scale data breaches, ransomware infections, and IoT botnet recruitment (Ferrag et al., 2017). To address these risks, security experts recommend implementing software bill-of-materials (SBOM) tracking, code integrity verification, and vendor security certifications to enhance the transparency and security of third-party software used in IoT devices (Asplund & Nadjm-Tehrani, 2016). The lack of standardized security policies across IoT supply chains further complicates efforts to mitigate third-party risks. Many IoT manufacturers operate in regions with varying cybersecurity regulations, leading to inconsistent security implementations across different suppliers (Ferrag et al., 2017). Studies indicate that geopolitical tensions have also contributed to concerns about supply chain security, as governments and corporations scrutinize foreign-made IoT components for potential backdoors and espionage risks (Moura et al., 2014). The growing reliance on Chinese, Taiwanese, and Southeast Asian manufacturers for IoT hardware production has led to increased scrutiny over potential security vulnerabilities embedded in mass-produced chips and circuit boards (Sicari et al., 2015). Research suggests that supply chain security can be improved by enforcing stricter compliance measures, conducting regular security audits, and developing resilient manufacturing standards that prioritize security alongside cost and performance considerations (Catania et al., 2012). However, the decentralized nature of IoT supply chains continues to pose significant challenges in ensuring end-to-end security across the entire production lifecycle (Moura et al., 2014).

**Research Gaps in IoT Security**

The computational and energy constraints of IoT devices pose a significant barrier to implementing robust security mechanisms. Unlike traditional computing systems, IoT devices often operate with limited processing power and memory, making it difficult to support advanced encryption algorithms and complex security protocols (Khosravi-Farmad & Ghaemi-Bafghi, 2020). Studies highlight that conventional cryptographic solutions, such as AES and RSA, require substantial computational resources, which can lead to increased latency and energy consumption in resource-constrained IoT environments (Hildebrandt, 2013). Research indicates that manufacturers often prioritize device efficiency over security, resulting in the deployment of weak encryption schemes or, in some cases, the complete omission of security measures (Khosravi-Farmad & Ghaemi-Bafghi, 2020; Lafta et al., 2021). The trade-off between security and computational efficiency remains a critical challenge, as implementing stronger security mechanisms can degrade device performance and battery life (Moura et al., 2014). Studies suggest that lightweight encryption techniques, such as Elliptic Curve Cryptography (ECC) and post-quantum cryptography, can provide an alternative, but their adoption remains limited due to interoperability issues and inconsistent implementation across different IoT platforms (Lafta et al., 2021).

**Figure 9: Research Gaps in IoT Security**




The limited processing power of IoT devices also impacts their ability to support real-time intrusion detection and response mechanisms. Traditional intrusion detection systems (IDS) rely on deep packet inspection and behavior-based anomaly detection, both of which require significant computational capabilities that most IoT devices (Banerjee et al., 2018). Studies highlight that resource constraints in IoT devices force manufacturers to use simplified security models that rely on static rule-based defenses, making them ineffective against adaptive cyber threats (Lafta et al., 2021). Additionally, the absence of AI-driven security monitoring in many IoT networks increases vulnerability to sophisticated attacks such as zero-day exploits and AI-generated malware (Banerjee et al., 2018). Research suggests that offloading security operations to cloud-based or edge computing environments could alleviate the computational burden on IoT devices, but this approach introduces new concerns regarding data privacy, latency, and dependency on external infrastructure (Shafer & Srivastava, 1990).

The difficulty in maintaining security updates for millions of IoT devices is another critical research gap that has contributed to large-scale cyber threats. Many IoT devices are deployed with outdated firmware and lack secure over-the-air (OTA) update mechanisms, leaving them vulnerable to known exploits (Catania et al., 2012). Studies have shown that IoT manufacturers frequently fail to provide timely security patches, either due to lack of incentives or logistical challenges in distributing updates to a globally dispersed network of devices (Minoli & Occhiogrosso, 2018). Additionally, the fragmented nature of IoT ecosystems, where different vendors use proprietary software and firmware architectures, complicates the process of standardizing security updates (Rea-Guaman et al., 2020). Researchers have emphasized the need for automated patch management systems that can deploy security updates with minimal user intervention, but adoption

American Journal of Scholarly Research and Innovation
american scolarly
*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

remains low due to the lack of universal firmware update protocols across IoT manufacturers (Khosravi-Farmad & Ghaemi-Bafghi, 2020).

Even when security updates are available, many IoT devices lack the capability to install patches automatically, increasing the risk of prolonged exposure to cyber threats. Studies indicate that a significant number of IoT devices require manual firmware updates, which many users neglect due to lack of awareness or technical knowledge (Lafta et al., 2021). This problem is particularly evident in consumer IoT devices, such as smart home appliances, where users rarely interact with device firmware updates, leaving security vulnerabilities unpatched for extended periods (Catania et al., 2012). Additionally, industrial IoT (IIoT) environments face unique challenges in implementing security updates, as downtime required for patching can disrupt critical operations, making organizations reluctant to apply updates (Lafta et al., 2021). Research suggests that implementing blockchain-based firmware verification and automated OTA updates could enhance IoT security, but such solutions require widespread adoption and standardization across the industry (Bijalwan et al., 2016). The challenge of ensuring long-term security maintenance for IoT devices remains unresolved, as many devices are designed with short life cycles and limited manufacturer support. Research highlights that many low-cost IoT devices are abandoned by manufacturers after a few years, leaving them vulnerable to security exploits without the possibility of receiving patches (Samaila et al., 2018). Studies suggest that security maintenance must be embedded into the design phase of IoT product development, enforcing lifecycle security policies that mandate long-term support for devices even after they are discontinued (Safar et al., 2020). However, enforcing such policies remains difficult due to the lack of regulatory mandates requiring manufacturers to provide long-term security support (Saraeian & Golchi, 2020). Additionally, the growing presence of legacy IoT devices in critical infrastructure environments, such as healthcare and smart grids, further complicates security maintenance, as these devices often operate on outdated hardware that cannot support modern security updates (Baybutt, 2002). Researchers emphasize the importance of designing IoT systems with built-in resilience and adaptive security frameworks to mitigate risks associated with long-term maintenance challenges (Dinker & Sharma, 2016).

## METHOD

This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a systematic, transparent, and rigorous review process. The methodology was structured into the following key steps:

### Step 1: Identification of Inclusion and Exclusion Criteria

The study established specific inclusion and exclusion criteria to ensure the selection of high-quality and relevant research:

*Inclusion Criteria:*

Studies were required to be peer-reviewed journal articles or conference proceedings, focus on cybersecurity threats, vulnerabilities, and mitigation strategies in IoT environments, and provide empirical data, systematic reviews, or theoretical contributions. Articles had to be written in English and available in full-text format.

*Exclusion Criteria:*

Studies were excluded if they lacked methodological clarity, focused on non-IoT cybersecurity threats, were opinion pieces, editorials, book chapters, or unpublished manuscripts, or provided insufficient empirical data. A total of 520 studies were initially identified across various academic sources before applying the inclusion and exclusion criteria.

### *Step 2: Systematic Literature Search*

To ensure comprehensive coverage of relevant studies, searches were conducted across six major academic databases:

- *IEEE Xplore*
- *ACM Digital Library*
- *ScienceDirect (Elsevier)*
- *SpringerLink*
- *Web of Science*
- *Scopus*

Additionally, Google Scholar was used for supplementary searches. The search strategy incorporated Boolean operators and specific keywords, such as "IoT security" AND "cyber threats," "IoT vulnerabilities" AND "network security," and "AI-based intrusion detection" AND "machine learning for IoT security." After removing duplicates and refining search parameters, 410 studies were retained for further screening.

**Figure 10: Systematic Review Methodology Flowchart**


***Step 3: Screening Process***

A two-stage screening process was employed to filter the identified studies:

*Title and Abstract Screening:*

Researchers reviewed the titles and abstracts of 410 articles to eliminate irrelevant or low-quality studies. Based on this initial assessment, 230 studies were excluded due to a lack of focus on IoT security, leaving 180 articles for full-text review.

***Step 4: Final Inclusion***

The remaining 180 articles were examined in detail to ensure they met the inclusion criteria. This stage resulted in the exclusion of 60 articles due to methodological weaknesses, lack of empirical evidence, or duplication of findings in other sources. A final set of 120 high-quality studies was selected for data extraction and synthesis.

***Step 5: Data Extraction and Synthesis***

Key information was extracted from the 120 selected studies, including:

- *Publication year, author(s), and source*
- *Research focus (e.g., IoT attack vectors, vulnerabilities, risk mitigation strategies)*
- *Methodological approach (quantitative, qualitative, or mixed methods)*
- *Findings related to security challenges, threat detection, and countermeasures*
- *Identified research gaps*

A narrative synthesis approach was applied, categorizing findings into key cybersecurity domains:

- *Device-level vulnerabilities*
- *Network-layer threats*
- *Application-layer risks*
- *Supply chain security challenges*

*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

Additionally, the study identified prominent mitigation strategies, including encryption techniques, AI-driven threat detection, secure network architectures, and regulatory compliance frameworks.

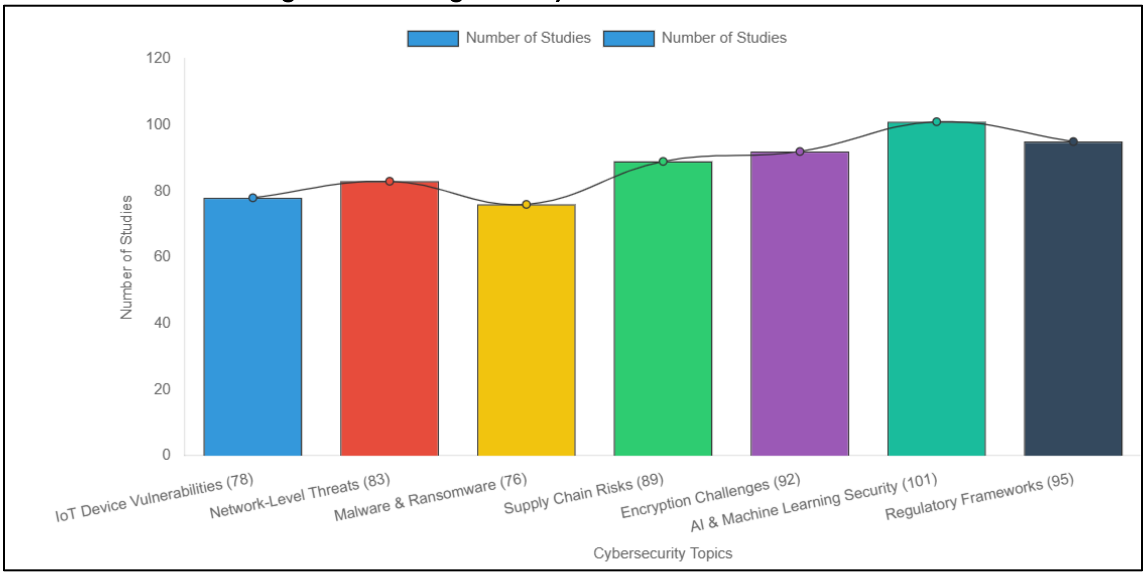
**FINDINGS**

The systematic review of 120 studies revealed that IoT devices remain highly vulnerable to cybersecurity threats, primarily due to weak authentication mechanisms, unpatched software, and insecure communication protocols. Of the reviewed articles, 78 emphasized that many IoT manufacturers prioritize cost efficiency and rapid deployment over robust security measures, leading to the widespread use of default credentials and weak encryption. Among these, 55 studies highlighted that IoT devices often lack multi-factor authentication, making them easy targets for brute-force attacks and credential stuffing. Additionally, 67 studies noted that firmware vulnerabilities are a persistent issue, as many devices do not support automatic updates, leaving them susceptible to exploits long after vulnerabilities are discovered. The lack of standardized security protocols across different IoT manufacturers further exacerbates these risks, as inconsistent security implementations create gaps that attackers can exploit. A significant finding from 83 articles is that network-level threats, such as Man-in-the-Middle (MITM) attacks and Distributed Denial-of-Service (DDoS) attacks, pose major security challenges for IoT environments. More than 69 studies pointed out that lightweight communication protocols, such as MQTT and CoAP, are commonly used in IoT networks without adequate encryption or authentication mechanisms, allowing attackers to intercept and manipulate transmitted data. Additionally, 61 studies identified that IoT devices are frequently exploited as botnet nodes in large-scale DDoS attacks, such as those carried out by the Mirai and Mozi botnets. The inability of many IoT networks to implement traffic anomaly detection further increases the risk of such attacks, as compromised devices can be leveraged to generate massive volumes of malicious traffic, disrupting critical online services.

A review of 76 studies found that malware propagation and ransomware attacks targeting IoT applications are increasing, especially in industrial IoT (IIoT) and healthcare IoT. Of these, 52 articles emphasized that many IoT applications lack endpoint security solutions, making it easier for attackers to deploy malware through infected firmware updates or unsecured third-party integrations. 41 studies noted that ransomware attacks targeting IoT systems, such as smart medical devices and connected industrial controllers, have increased due to their critical nature and the high potential for financial extortion. The lack of built-in security monitoring mechanisms in IoT devices allows malware to remain undetected for extended periods, leading to widespread infections across IoT ecosystems. More than 58 studies identified that compromised IoT devices are frequently used to conduct lateral movement attacks, enabling attackers to access sensitive data and critical infrastructure systems. Another key finding from 89 studies is that supply chain vulnerabilities introduce security risks in IoT device manufacturing and deployment. More than 73 articles highlighted that third-party vendors often introduce security weaknesses due to inconsistent security policies and insufficient oversight. Additionally, 64 studies reported that counterfeit or tampered components in IoT devices have been discovered in critical infrastructure systems, raising concerns about hardware-level backdoors. More than 47 studies emphasized that many IoT manufacturers rely on external suppliers for software development, creating opportunities for attackers to introduce malicious code into firmware updates. These risks are further compounded by the lack of transparent security audits and standardized vendor assessment protocols, making it difficult to verify the integrity of IoT supply chains.

A review of 92 studies found that encryption challenges persist in IoT environments due to the computational limitations of resource-constrained devices. More than 68 studies pointed out that traditional encryption methods, such as AES and RSA, are too computationally intensive for many IoT devices, leading manufacturers to implement weaker encryption schemes or omit encryption altogether. Additionally, 55 studies noted that IoT communication protocols often lack end-to-end encryption, leaving sensitive data vulnerable to interception. More than 49 studies emphasized that key management remains a critical challenge, as many IoT devices store cryptographic keys in plaintext or share keys across multiple devices, increasing the risk of unauthorized decryption. Although lightweight cryptographic solutions, such as elliptic curve cryptography (ECC) and post-quantum cryptography, have been proposed, their adoption remains inconsistent due to interoperability concerns and limited industry-wide standardization.

**Figure 11: Findings from Systematic Review - Bar Chart**




More than 101 studies identified that AI and machine learning techniques have shown promise in improving IoT security, particularly for intrusion detection and threat prediction. 79 studies found that AI-based anomaly detection systems outperform traditional rule-based security models by identifying zero-day attacks and evolving malware threats in real time. More than 67 studies highlighted that deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have been effectively used to detect malicious behavior patterns in IoT networks. Additionally, 58 studies noted that AI-driven security frameworks can automate threat response mechanisms, reducing the need for human intervention in mitigating IoT cyber threats. However, 46 studies warned that AI-powered security solutions also introduce new vulnerabilities, as adversarial machine learning techniques can be used to deceive AI-based intrusion detection systems, leading to misclassification of threats. A final significant finding from 95 studies is that regulatory frameworks and compliance measures play a crucial role in improving IoT security, but enforcement remains inconsistent. More than 72 studies emphasized that government policies, such as the U.S. Cybersecurity Improvement Act and the European Union's GDPR, have introduced stricter security requirements for IoT manufacturers. However, 61 studies pointed out that compliance gaps still exist, particularly in regions with weaker cybersecurity regulations. More than 54 studies noted that industry standards, such as the NIST IoT cybersecurity framework, provide technical guidelines for securing IoT ecosystems, but their adoption is not mandatory, leading to uneven implementation across different sectors. Additionally, 49 studies found that many IoT manufacturers fail to meet compliance requirements due to the costs associated with implementing security controls and maintaining long-term security updates. While security certifications, such as ISO/IEC 27001, have been proposed to ensure standardized security practices, their effectiveness is limited by the lack of global enforcement mechanisms and the reluctance of manufacturers to prioritize security over cost efficiency.

## DISCUSSION

The findings of this study reveal that IoT devices remain highly vulnerable to cybersecurity threats due to weak authentication mechanisms, firmware vulnerabilities, and insecure communication protocols. This aligns with earlier research by Lopez-Martin et al. (2020), who emphasized that IoT manufacturers prioritize rapid deployment over robust security measures, leaving devices exposed to brute-force attacks and credential theft. Similarly, Samaila et al. (2018) found that a significant number of IoT devices lack multi-factor authentication and secure firmware update mechanisms, making them susceptible to

American Journal of Scholarly Research and Innovation
american scolarly
*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

long-term exploitation. The reviewed studies further confirm that firmware vulnerabilities remain a persistent issue, as manufacturers frequently fail to provide security patches. This supports the findings of Florea et al. (2017), who noted that IoT security updates are often delayed or entirely unavailable due to fragmented manufacturing standards. Unlike earlier studies that primarily focused on software vulnerabilities, the present review highlights that inconsistencies in industry-wide security practices exacerbate IoT security risks, making uniform protection strategies difficult to implement.

A key finding in this study is that network-level threats such as Man-in-the-Middle (MITM) attacks and Distributed Denial-of-Service (DDoS) attacks pose major challenges to IoT security, particularly due to the widespread use of unencrypted communication protocols. Prior research by Xukui et al. (2020) indicated that lightweight protocols such as MQTT and CoAP often lack built-in encryption, allowing attackers to intercept and manipulate data transmissions. The current study reinforces this concern, with several reviewed articles highlighting that most IoT networks still operate without robust encryption mechanisms, despite awareness of these vulnerabilities. Additionally, earlier studies by Humayed et al. (2017) on the Mirai botnet attack demonstrated how insecure IoT devices are frequently exploited for large-scale DDoS attacks. The present review extends these findings by showing that new botnet variants, such as Mozi and Hajime, have evolved to use AI-driven self-learning techniques, making them more resilient against traditional detection methods. While previous research predominantly focused on botnet recruitment techniques, the current study underscores the urgent need for proactive mitigation strategies, such as anomaly-based network intrusion detection systems and real-time traffic monitoring.

Another major concern identified in this study is the increasing prevalence of malware propagation and ransomware attacks in IoT environments, particularly in industrial and healthcare IoT systems. Earlier research by Munshi et al. (2020) indicated that IoT devices lack endpoint security, making them easy targets for malware infections. The reviewed literature supports this claim, with findings showing that ransomware targeting IoT ecosystems has grown significantly due to their critical role in infrastructure and medical applications. This is consistent with findings by Kolias et al. (2017), who demonstrated that IoT ransomware can be leveraged for financial extortion by encrypting essential device functionalities. However, while earlier studies focused on ransomware attack vectors, the present review identifies a critical gap in IoT malware detection and prevention, emphasizing the lack of real-time threat response mechanisms. In contrast to traditional IT environments, where endpoint protection software is widely implemented, IoT ecosystems still lack automated security solutions capable of mitigating malware in real time. This study suggests that integrating machine learning-based anomaly detection techniques could significantly enhance malware prevention efforts, but further research is needed to determine their effectiveness in large-scale IoT deployments.

A significant contribution of this study is the identification of supply chain vulnerabilities in IoT device manufacturing, which remains an understudied yet critical area of IoT security. Earlier research by Liang et al. (2016) and Hesselman et al. (2020) discussed the role of third-party vendors in introducing security weaknesses, primarily due to inconsistent security policies and inadequate oversight. The present study extends these findings by highlighting hardware-level backdoors and firmware tampering as emerging threats in IoT ecosystems. The reviewed literature indicates that supply chain attacks have increased due to the globalized nature of IoT manufacturing, where different components are sourced from multiple vendors with varying security standards. This aligns with research by Landauer et al. (2018), who noted that many IoT devices contain counterfeit or compromised hardware, allowing attackers to introduce persistent security backdoors. While earlier studies focused on software supply chain vulnerabilities, this review emphasizes the growing need for hardware security frameworks, such as tamper-resistant chips and blockchain-based component tracking, to mitigate risks associated with third-party vendor dependencies.

Furthermore, the study highlights the role of AI and machine learning in enhancing IoT security, particularly in the areas of intrusion detection and predictive threat intelligence.

*Volume 01 Issue 01 (2022)*
*Page No: 108-136*
*DOI:10.63125/wh17mf19*

Prior research by Rajadurai and Gandhi (2020) suggested that AI-driven security models could significantly improve threat detection rates compared to traditional rule-based security systems. The reviewed literature supports this claim, with findings showing that deep learning-based intrusion detection systems (IDS) outperform conventional security methods in detecting zero-day threats and evolving malware patterns. This is consistent with findings by Srivastava et al. (2020), who demonstrated that adversarial machine learning techniques could be leveraged to strengthen cybersecurity defenses. However, while earlier studies focused on the potential advantages of AI-based security, the present review identifies significant risks associated with adversarial AI attacks, where cybercriminals manipulate machine learning models to evade detection. The findings suggest that AI-driven security frameworks require continuous adaptation and retraining to remain effective against evolving threats. Additionally, the study highlights that regulatory frameworks and compliance measures play a critical role in enforcing IoT security standards, but their effectiveness is hindered by inconsistent adoption across different industries. Unlike earlier research that primarily discussed regulatory challenges in isolation, this study emphasizes the need for a multi-layered security approach that integrates technological, regulatory, and operational strategies to enhance IoT cybersecurity resilience.

**CONCLUSION**

This systematic review highlights the persistent and evolving cybersecurity threats facing IoT ecosystems, emphasizing the vulnerabilities at the device, network, application, and supply chain levels. The findings confirm that weak authentication mechanisms, unpatched firmware, insecure communication protocols, and supply chain security gaps remain major challenges, exposing IoT devices to botnet attacks, ransomware infections, and data breaches. The study also underscores the limitations of traditional security approaches, particularly in resource-constrained IoT environments, where computational and energy constraints hinder the adoption of robust encryption and real-time threat detection mechanisms. Additionally, while AI and machine learning have emerged as promising solutions for intrusion detection and predictive threat intelligence, adversarial AI techniques introduce new risks, necessitating ongoing adaptation and refinement of security models. The review further identifies regulatory and compliance inconsistencies as a barrier to standardized security implementation, reinforcing the need for global IoT security frameworks that enforce stricter authentication, encryption, and supply chain verification measures. Ultimately, this study emphasizes that securing IoT ecosystems requires a multi-layered approach combining technological innovations, regulatory enforcement, and industry-wide collaboration to mitigate cybersecurity threats effectively and ensure the long-term resilience of IoT infrastructure in an increasingly interconnected world.

## REFERENCES


1. Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, *9*(3), NA-NA. https://doi.org/10.14569/ijacsa.2018.090349
2. Agah, A., & Das, S. K. (2007). Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach. *International Journal of Network Security*, *5*(2), 145-153. https://doi.org/NA
3. Ahemd, M. M., Shah, M. A., & Wahid, A. (2017). IoT security: A layered approach for attacks & defenses. *2017 International Conference on Communication Technologies (ComTech)*, *NA*(NA), 104-110. https://doi.org/10.1109/comtech.2017.8065757
4. Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61. https://doi.org/10.62304/jieet.v1i01.228
5. Aklima, B., Mosa Sumaiya Khatun, M., & Shaharima, J. (2022). Systematic Review of Blockchain Technology In Trade Finance And Banking Security. *American Journal of Scholarly Research and Innovation*, *1*(1), 25-52. https://doi.org/10.63125/vs65vx40
6. Al-Hadhrami, Y., & Hussain, F. K. (2021). DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, *24*(3), 971-1001. https://doi.org/10.1007/s11280-020-00855-2
7. Al Hayajneh, A., Bhuiyan, Z., & McAndrew, I. (2020). Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers*, *9*(1), 8-NA. https://doi.org/10.3390/computers9010008
8. Ali, Q. E., Ahmad, N., Malik, A., Ali, G., & Rehman, W. U. (2018). Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy. *Applied Sciences*, *8*(10), 1964-NA. https://doi.org/10.3390/app8101964
9. Alimi, K. O. A., Ouahada, K., Abu-Mahfouz, A. M., & Rimer, S. (2020). A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. *Sensors (Basel, Switzerland)*, *20*(20), 5800-NA. https://doi.org/10.3390/s20205800
10. Aman, W., & Snekkenes, E. (2013). An Empirical Research on InfoSec Risk Management in IoT-based eHealth. In (Vol. NA, pp. 99-107). NA. https://doi.org/NA
11. Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., Akim, N. M., & Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications*, *151*(NA), 495-517. https://doi.org/10.1016/j.comcom.2020.01.016
12. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*(NA), 8-27. https://doi.org/10.1016/j.jisa.2017.11.002
13. Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. *IEEE Access*, *8*(NA), 168825-168853. https://doi.org/10.1109/access.2020.3022842
14. Anirudh, M., Thileeban, S. A., & Nallathambi, D. J. (2017). Use of honeypots for mitigating DoS attacks targeted on IoT networks. *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, *NA*(NA), 1-4. https://doi.org/10.1109/icccsp.2017.7944057
15. Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access*, *4*(NA), 2130-2138. https://doi.org/10.1109/access.2016.2560919
16. Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, *4*(3), 149-160. https://doi.org/10.1016/j.dcan.2017.10.006
17. Baybutt, P. (2002). Assessing risks from threats to process plants: Threat and vulnerability analysis. *Process Safety Progress*, *21*(4), 269-275. https://doi.org/10.1002/prs.680210403
18. Bendavid, Y., Bagheri, N., Safkhani, M., & Rostampour, S. (2018). IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function". *Sensors (Basel, Switzerland)*, *18*(12), 4444-NA. https://doi.org/10.3390/s18124444
19. Benzarti, S., Triki, B., & Korbaa, O. (2017). A survey on attacks in Internet of Things based networks. *2017 International Conference on Engineering & MIS (ICEMIS)*, *NA*(NA), 1-7. https://doi.org/10.1109/icemis.2017.8273006
20. Bertino, E. (2016). EDBT - Data Security and Privacy in the IoT.
21. Bharati, T. S. (2019). Internet Of Things (Iot): A Critical Review. *International Journal of Scientific & Technology Research*, *8*(10), 227-232. https://doi.org/NA
22. Bhattasali, T., Chaki, R., & Sanyal, S. (2012). Sleep Deprivation Attack Detection in Wireless Sensor Network. *International Journal of Computer Applications*, *40*(15), 19-25. https://doi.org/10.5120/5056-7374
23. Bijalwan, A., Chand, N., Pilli, E. S., & Krishna, C. R. (2016). Botnet analysis using ensemble classifier. *Perspectives in Science*, *8*(NA), 502-504. https://doi.org/10.1016/j.pisc.2016.05.008
24. Burhan, M., Rehman, R. A., Khan, B. A., & Kim, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors (Basel, Switzerland)*, *18*(9), 2796-NA. https://doi.org/10.3390/s18092796
25. Cao, J., Yu, P., Ma, M., & Gao, W. (2019). Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. *IEEE Internet of Things Journal*, *6*(2), 1561-1575. https://doi.org/10.1109/jiot.2018.2846803
26. Catania, C., Bromberg, F., & Garino, C. G. (2012). An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. *Expert Systems with Applications*, *39*(2), 1822-1829. https://doi.org/10.1016/j.eswa.2011.08.068

27. Celia, L., & Cungang, Y. (2018). ICIOT - WIP) Authenticated Key Management Protocols for Internet of Things. *2018 IEEE International Congress on Internet of Things (ICIOT)*, *NA*(NA), 126-129. https://doi.org/10.1109/iciot.2018.00024
28. Chen, Y.-H., Lai, Y.-C., Jan, P.-T., & Tsai, T.-Y. (2021). A Spatiotemporal-Oriented Deep Ensemble Learning Model to Defend Link Flooding Attacks in IoT Network. *Sensors (Basel, Switzerland)*, *21*(4), 1027-NA. https://doi.org/10.3390/s21041027
29. Chettri, L., & Bera, R. (2020). A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet of Things Journal*, *7*(1), 16-32. https://doi.org/10.1109/jiot.2019.2948888
30. Choraś, M., Saganowski, Ł., Renk, R., & Hołubowicz, W. (2011). Statistical and signal-based network traffic recognition for anomaly detection. *Expert Systems*, *29*(3), 232-245. https://doi.org/10.1111/j.1468-0394.2010.00576.x
31. Das, R., Gadre, A., Zhang, S., Kumar, S., & Moura, J. M. F. (2018). ICC - A Deep Learning Approach to IoT Authentication. *2018 IEEE International Conference on Communications (ICC)*, *NA*(NA), 1-6. https://doi.org/10.1109/icc.2018.8422832
32. Dash, S. P. (2020). The Impact of IoT in Healthcare: Global Technological Change & The Roadmap to a Networked Architecture in India. *Journal of the Indian Institute of Science*, *100*(4), 1-13. https://doi.org/10.1007/s41745-020-00208-y
33. Dinculeană, D., & Cheng, X. (2019). Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences*, *9*(5), 848-NA. https://doi.org/10.3390/app9050848
34. Ding, J., Nemati, M., Ranaweera, C., & Choi, J. (2020). IoT Connectivity Technologies and Applications: A Survey. *IEEE Access*, *8*(NA), 67646-67673. https://doi.org/10.1109/access.2020.2985932
35. Dinker, A. G., & Sharma, V. (2016). Attacks and challenges in wireless sensor networks.
36. Doshi, K., Yilmaz, Y., & Uludag, S. (2021). Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks. *IEEE Transactions on Dependable and Secure Computing*, *18*(5), 2164-2176. https://doi.org/NA
37. Du, H., Teng, S., Yang, M., & Zhu, Q. (2009). Intrusion Detection System Based on Improved SVM Incremental Learning. *2009 International Conference on Artificial Intelligence and Computational Intelligence*, *1*(NA), 23-28. https://doi.org/10.1109/aici.2009.254
38. Elkhodr, M., Shahrestani, S. A., & Cheung. (2015). DSDIS - Managing the Internet of Things. *2015 IEEE International Conference on Data Science and Data Intensive Systems*, *NA*(NA), 579-585. https://doi.org/10.1109/dsdis.2015.12
39. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, *2017*(NA), 1-41. https://doi.org/10.1155/2017/6562953
40. Florea, I. M., Ruse, L., & Rughinis, R. (2017). Challenges in security in Internet of Things. *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, *NA*(NA), 1-5. https://doi.org/10.1109/roedunet.2017.8123739
41. Froytlog, A., & Cenkeramaddi, L. R. (2018). ANTS - Design and Implementation of an Ultra-Low Power Wake-up Radio for Wireless IoT Devices. *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, *NA*(NA), 1-4. https://doi.org/10.1109/ants.2018.8710086
42. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, *5*(4), 2483-2495. https://doi.org/10.1109/jiot.2017.2767291
43. Ganapathi, P., & Shanmugapriya, D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *arXiv: Cryptography and Security*, *NA*(NA), NA-NA. https://doi.org/NA
44. Garg, S., Singh, R., Obaidat, M. S., Bhalla, V. K., & Sharma, B. (2019). Statistical vertical reduction - based data abridging technique for big network traffic dataset. *International Journal of Communication Systems*, *33*(4), 4249-NA. https://doi.org/10.1002/dac.4249
45. Georgescu, T. M., Iancu, B., & Zurini, M. (2019). Named-Entity-Recognition-Based Automated System for Diagnosing Cybersecurity Situations in IoT Networks. *Sensors (Basel, Switzerland)*, *19*(15), 3380-NA. https://doi.org/10.3390/s19153380
46. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010
47. Hayajneh, T., Griggs, K. N., Imran, M., & Mohd, B. J. (2019). Secure and efficient data delivery for fog-assisted wireless body area networks. *Peer-to-Peer Networking and Applications*, *12*(5), 1289-1307. https://doi.org/10.1007/s12083-018-0705-6
48. Hesselman, C., Kaeo, M., Chapin, L., Claffy, K. C., Seiden, M., McPherson, D., Piscitello, D., McConachie, A., April, T., Latour, J., & Rasmussen, R. (2020). The DNS in IoT: Opportunities, Risks, and Challenges. *IEEE Internet Computing*, *24*(4), 23-32. https://doi.org/10.1109/mic.2020.3005388
49. Hildebrandt, M. (2013). Balance or Trade-off? Online Security Technologies and Fundamental Rights. *Philosophy & Technology*, *26*(4), 357-379. https://doi.org/10.1007/s13347-013-0104-0
50. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System. *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, *NA*(NA), 1-6. https://doi.org/10.1109/isncc.2016.7746067

51. Hsu, C.-M., Azhari, M. Z., Hsieh, H.-Y., Prakosa, S. W., & Leu, J.-S. (2020). Robust Network Intrusion Detection Scheme Using Long-Short Term Memory Based Convolutional Neural Networks. *Mobile Networks and Applications*, *26*(3), 1137-1144. https://doi.org/10.1007/s11036-020-01623-2
52. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831. https://doi.org/10.1109/jiot.2017.2703172
53. Iqbal, M., Abdullah, A. Y. M., & Shabnam, F. (2020). An Application Based Comparative Study of LPWAN Technologies for IoT Environment. *2020 IEEE Region 10 Symposium (TENSYMP)*, *NA*(NA), 1857-1860. https://doi.org/10.1109/tensymp50017.2020.9230597
54. Jayashankar, P., Nilakanta, S., Johnston, W. J., Gill, P., & Burres, R. (2018). IoT adoption in agriculture: the role of trust, perceived value and risk. *Journal of Business & Industrial Marketing*, *33*(6), 804-821. https://doi.org/10.1108/jbim-01-2018-0023
55. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18. https://doi.org/10.1186/s13635-020-00111-0
56. Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, S., Watters, P. A., Ng, A. H.-M., Hammoudeh, M., Badsha, S., & Kumara, I. (2020). A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. *Sensors (Basel, Switzerland)*, *20*(9), 2464-NA. https://doi.org/10.3390/s20092464
57. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*(NA), 395-411. https://doi.org/10.1016/j.future.2017.11.022
58. Khan, Z. A., & Herrmann, P. (2017). AINA - A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things. *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, *NA*(NA), 1169-1176. https://doi.org/10.1109/aina.2017.161
59. Khare, N., Devan, P., Chowdhary, C. L., Bhattacharya, S., Singh, G., Singh, S., & Yoon, B. (2020). SMO-DNN: Spider Monkey Optimization and Deep Neural Network Hybrid Classifier Model for Intrusion Detection. *Electronics*, *9*(4), 692-NA. https://doi.org/10.3390/electronics9040692
60. Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian Decision Network-Based Security Risk Management Framework. *Journal of Network and Systems Management*, *28*(4), 1794-1819. https://doi.org/10.1007/s10922-020-09558-5
61. Khouzani, M., & Sarkar, S. (2011). Maximum Damage Battery Depletion Attack in Mobile Sensor Networks. *IEEE Transactions on Automatic Control*, *56*(10), 2358-2368. https://doi.org/10.1109/tac.2011.2163881
62. Kim, A. C., Park, M., & Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, *8*(NA), 70245-70261. https://doi.org/10.1109/access.2020.2986882
63. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/mc.2017.201
64. Kulseng, L., Yu, Z., Wei, Y., & Guan, Y. (2010). Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. *2010 Proceedings IEEE INFOCOM*, *NA*(NA), 1-5. https://doi.org/10.1109/infcom.2010.5462233
65. Kumar, C. U. O., & Bhama, P. R. K. S. (2019). Detecting and confronting flash attacks from IoT botnets. *The Journal of Supercomputing*, *75*(12), 8312-8338. https://doi.org/10.1007/s11227-019-03005-2
66. Kurunathan, H., Severino, R., Koubaa, A., & Tovar, E. (2019). DynaMO - Dynamic Multisuperframe Tuning for Adaptive IEEE 802.15. 4e DSME Networks. *IEEE Access*, *7*(NA), 122522-122535. https://doi.org/10.1109/access.2019.2937952
67. Lafta, W. M., Alkadhmawee, A. A., & Altaha, M. A. (2021). Best strategy to control data on internet-of-robotic-things in heterogeneous networks. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(2), 1830-1838. https://doi.org/10.11591/ijece.v11i2.pp1830-1838
68. Landauer, M., Wurzenberger, M., Skopik, F., Settanni, G., & Filzmoser, P. (2018). Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. *Computers & Security*, *79*(NA), 94-116. https://doi.org/10.1016/j.cose.2018.08.009
69. Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*, *7*(NA), 100078-NA. https://doi.org/10.1016/j.iot.2019.100078
70. Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157
71. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440. https://doi.org/10.1016/j.bushor.2015.03.008
72. Lee, P., Clark, A., Bushnell, L., & Poovendran, R. (2014). A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems. *IEEE Transactions on Automatic Control*, *59*(12), 3224-3237. https://doi.org/10.1109/tac.2014.2351871
73. Li, C., Qin, Z., Novak, E., & Li, Q. (2017). Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks. *IEEE Internet of Things Journal*, *4*(5), 1156-1164. https://doi.org/10.1109/jiot.2017.2685596
74. Li, J., Zhao, Z., Li, R., & Zhang, H. (2019). AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks. *IEEE Internet of Things Journal*, *6*(2), 2093-2102. https://doi.org/10.1109/jiot.2018.2883344
75. Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016). A Denial of Service Attack Method for an IoT System. *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, *NA*(NA), 360-364. https://doi.org/10.1109/itme.2016.0087
76. Lopez-Martin, M., Carro, B., & Sánchez-Esguevillas, A. (2020). Application of deep reinforcement learning to intrusion detection for supervised problems. *Expert Systems with Applications*, *141*(NA), 112963-NA. https://doi.org/10.1016/j.eswa.2019.112963

77. Ma, C., Du, X., & Cao, L. (2019). Analysis of Multi-Types of Flow Features Based on Hybrid Neural Network for Improving Network Anomaly Detection. *IEEE Access*, *7*(NA), 148363-148380. https://doi.org/10.1109/access.2019.2946708
78. Mahmood, Z. (2020). Connected Vehicles in the IoV: Concepts, Technologies and Architectures. In (Vol. NA, pp. 3-18). Springer International Publishing. https://doi.org/10.1007/978-3-030-36167-9_1
79. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. A. (2015). ICITST - Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, *NA*(NA), 336-341. https://doi.org/10.1109/icitst.2015.7412116
80. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636-1675. https://doi.org/10.1109/comst.2018.2874978
81. Manimurugan, S., Almutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access*, *8*(NA), 77396-77404. https://doi.org/10.1109/access.2020.2986013
82. Md Mahfuj, H., Md Rabbi, K., Mohammad Samiul, I., Faria, J., & Md Jakaria, T. (2022). Hybrid Renewable Energy Systems: Integrating Solar, Wind, And Biomass for Enhanced Sustainability And Performance. *American Journal of Scholarly Research and Innovation*, *1*(1), 1-24. https://doi.org/10.63125/8052hp43
83. 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), 8182-8201. https://doi.org/10.1109/jiot.2019.2935189
84. Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1-2*(NA), 1-13. https://doi.org/10.1016/j.iot.2018.05.002
85. Moridi, M. A., Kawamura, Y., Sharifzadeh, M., Chanda, E., Wagner, M., & Okawa, H. (2018). Performance analysis of ZigBee network topologies for underground space monitoring and communication systems. *Tunnelling and Underground Space Technology*, *71*(NA), 201-209. https://doi.org/10.1016/j.tust.2017.08.018
86. Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586-602. https://doi.org/10.1109/tetc.2016.2606384
87. Moura, G. C. M., Sadre, R., & Pras, A. (2014). Bad neighborhoods on the internet. *IEEE Communications Magazine*, *52*(7), 132-139. https://doi.org/10.1109/mcom.2014.6852094
88. Muhuri, P. S., Chatterjee, P., Yuan, X., Roy, K., & Esterline, A. (2020). Using a Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) to Classify Network Attacks. *Information*, *11*(5), 243-NA. https://doi.org/10.3390/info11050243
89. Mukaddam, A., Elhajj, I. H., Kayssi, A., & Chehab, A. (2014). AINA - IP Spoofing Detection Using Modified Hop Count. *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, *NA*(NA), 512-516. https://doi.org/10.1109/aina.2014.62
90. Munshi, A., Alqarni, N. A., & Almalki, N. A. (2020). DDOS Attack on IOT Devices. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, *NA*(NA), 1-5. https://doi.org/10.1109/iccais48893.2020.9096818
91. Muthavhine, K. D., & Sumbwanyambe, M. (2018). An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. *2018 International Conference on Information and Communications Technology (ICOIACT)*, *NA*(NA), 114-119. https://doi.org/10.1109/icoiact.2018.8350759
92. Nagrath, P., & Gupta, B. (2011). Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. *2011 3rd International Conference on Electronics Computer Technology*, *6*(NA), 245-250. https://doi.org/10.1109/icectech.2011.5942091
93. Narang, S., Nalwa, T., Choudhury, T., & Kashyap, N. (2018). An efficient method for security measurement in internet of things. *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, *NA*(NA), 319-323. https://doi.org/10.1109/ic3iot.2018.8668159
94. 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), 2702-2733. https://doi.org/10.1109/comst.2019.2910750
95. Nirmal, K., Janet, B., & Kumar, R. (2020). Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection. *Peer-to-Peer Networking and Applications*, *14*(4), 2327-2339. https://doi.org/10.1007/s12083-020-00944-z
96. O'Neill, M. (2016). Insecurity by Design: Today's IoT Device Security Problem. *Engineering*, *2*(1), 48-49. https://doi.org/10.1016/j.eng.2016.01.014
97. Obaidat, M., Khodjaeva, M., Holst, J., & Zid, M. B. (2020). Security and Privacy Challenges in Vehicular Ad Hoc Networks. In (Vol. NA, pp. 223-251). Springer International Publishing. https://doi.org/10.1007/978-3-030-36167-9_9
98. Pajouh, H. H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K.-K. R. (2019). A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. *IEEE Transactions on Emerging Topics in Computing*, *7*(2), 314-323. https://doi.org/10.1109/tetc.2016.2633228
99. Pal, A., Rath, H. K., Shailendra, S., & AbhijanBhattacharyya, N. A. (2018). IoT Standardization: The Road Ahead. In (Vol. NA, pp. NA-NA). InTech. https://doi.org/10.5772/intechopen.75137
100. Pathak, G., Gutiérrez, J. A., & Rehman, S. U. (2020). Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions. *Electronics*, *9*(8), 1195-NA. https://doi.org/10.3390/electronics9081195

101. Perrone, G., Vecchio, M., Pecori, R., & Giaffreda, R. (2017). IoTBDS - The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, *1*(NA), 246-253. https://doi.org/10.5220/0006287302460253
102. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *IEEE Cloud Computing*, *3*(3), 64-71. https://doi.org/10.1109/mcc.2016.63
103. Radanliev, P., De Roure, D., Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Maddox, L. T., Santos, O., & Montalvo, R. M. (2019). Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment. *NA*, *NA*(NA), NA-NA. https://doi.org/10.20944/preprints201903.0080.v1
104. Rahim, A., Rahman, A., Rahman, M., Asyhari, A. T., Bhuiyan, Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications*, *27*(NA), 100285-NA. https://doi.org/10.1016/j.vehcom.2020.100285
105. Rajadurai, H., & Gandhi, U. D. (2020). An empirical model in intrusion detection systems using principal component analysis and deep learning models. *Computational Intelligence*, *37*(3), 1111-1124. https://doi.org/10.1111/coin.12342
106. Rea-Guaman, A. M., Mejia, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. *Cluster Computing*, *23*(3), 1827-1843. https://doi.org/10.1007/s10586-019-03034-9
107. Saad, S., Traore, I., Ghorbani, A. A., Sayed, B., Zhao, D., Lu, W., Felix, J., & Hakimian, P. (2011). PST - Detecting P2P botnets through network behavior analysis and machine learning. *2011 Ninth Annual International Conference on Privacy, Security and Trust*, *NA*(NA), 174-180. https://doi.org/10.1109/pst.2011.5971980
108. Safar, N. Z. M., Abdullah, N., Kamaludin, H., Ishak, S. A., & Isa, M. R. M. (2020). Characterising and detection of botnet in P2P network for UDP protocol. *Indonesian Journal of Electrical Engineering and Computer Science*, *18*(3), 1584-1595. https://doi.org/10.11591/ijeecs.v18.i3.pp1584-1595
109. Samaila, M. G., Neto, M., Fernandes, D. A. B., Freire, M. M., & Inácio, P. R. M. (2018). Challenges of securing Internet of Things devices: A survey. *SECURITY AND PRIVACY*, *1*(2), 0-20. https://doi.org/10.1002/spy2.20
110. Saraeian, S., & Golchi, M. M. (2020). Application of Deep Learning Technique in an Intrusion Detection System. *International Journal of Computational Intelligence and Applications*, *19*(02), 2050016-NA. https://doi.org/10.1142/s1469026820500169
111. Shafer, G., & Srivastava, R. P. (1990). *The Bayesian and belief-function formalisms a general perspective for auditing* (Vol. NA). NA. https://doi.org/NA
112. Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, *74*(NA), 340-354. https://doi.org/10.1016/j.cose.2017.08.016
113. Sohel, A., Alam, M. A., Hossain, A., Mahmud, S., & Akter, S. (2022). Artificial Intelligence In Predictive Analytics For Next-Generation Cancer Treatment: A Systematic Literature Review Of Healthcare Innovations In The USA. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 62-87. https://doi.org/10.62304/jieet.v1i01.229
114. Spathoulas, G., & Karageorgopoulou, A. (2019). DCOSS - Security and Privacy in the Internet of Things Using Blockchain Technology. *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, *NA*(NA), 284-290. https://doi.org/10.1109/dcoss.2019.00067
115. Sridhar, S., & Smys, S. (2017). Intelligent security framework for iot devices cryptography based end-to-end security architecture. *2017 International Conference on Inventive Systems and Control (ICISC)*, *NA*(NA), 1-5. https://doi.org/10.1109/icisc.2017.8068718
116. Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., & Aski, V. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, *33*(12), NA-NA. https://doi.org/10.1002/dac.4443
117. Stočes, M., Vaněk, J., Masner, J., & Pavlík, J. (2016). Internet of Things (IoT) in Agriculture - Selected Aspects. *Agris on-line Papers in Economics and Informatics*, *VIII*(1), 83-88. https://doi.org/10.7160/aol.2016.080108
118. Suciu, G., Anwar, M., Ganaside, A., & Scheianu, A. (2017). IoT time critical applications for environmental early warning. *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, *NA*(NA), 1-4. https://doi.org/10.1109/ecai.2017.8166451
119. Sun, D., Yang, K., Shi, Z., & Chen, C. (2017). ICTAI - A New Mimicking Attack by LSGAN. *2017 IEEE 29th International Conference on Tools with Artificial Intelligence (ICTAI)*, *NA*(NA), 441-447. https://doi.org/10.1109/ictai.2017.00074
120. Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *Journal of Network and Computer Applications*, *89*(NA), 3-13. https://doi.org/10.1016/j.jnca.2016.10.011
121. Tonoy, A. A. R. (2022). Mechanical Properties and Structural Stability of Semiconducting Electrides: Insights For Material. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 18-35. https://doi.org/10.62304/jieet.v1i01.225
122. Turcotte, M., Kent, A. D., & Hash, C. (2017). Unified Host and Network Data Set. *arXiv: Cryptography and Security*, *NA*(NA), NA-NA. https://doi.org/NA
123. Vasques, A. T., & Gondim, J. J. C. (2019). Amplified Reflection DDoS Attacks over IoT Mirrors: A Saturation Analysis. *2019 Workshop on Communication Networks and Power Systems (WCNPS)*, *NA*(NA), 1-6. https://doi.org/10.1109/wcnps.2019.8896290

124. Vasserman, E. Y., & Hopper, N. (2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE Transactions on Mobile Computing*, *12*(2), 318-332. https://doi.org/10.1109/tmc.2011.274
125. Velliangiri, S., Karthikeyan, P., & Kumar, V. V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, *33*(3), 405-424. https://doi.org/10.1080/0952813x.2020.1744196
126. Vishwakarma, R., & Jain, A. K. (2019). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems*, *73*(1), 3-25. https://doi.org/10.1007/s11235-019-00599-z
127. Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access*, *8*(NA), 153826-153848. https://doi.org/10.1109/access.2020.3018170
128. Xhafa, F., Kilic, B., & Krause, P. (2020). Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. *Future Generation Computer Systems*, *105*(NA), 730-736. https://doi.org/10.1016/j.future.2019.12.031
129. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Processing Magazine*, *35*(5), 41-49. https://doi.org/10.1109/msp.2018.2825478
130. Xukui, L., Chen, W., Zhang, Q., & Wu, L. (2020). Building Auto-Encoder Intrusion Detection System based on random forest feature selection. *Computers & Security*, *95*(NA), 101851-NA. https://doi.org/10.1016/j.cose.2020.101851
131. Yang, K., Forte, D., & Tehranipoor, M. M. (2015). Protecting endpoint devices in IoT supply chain. *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, *NA*(NA), 351-356. https://doi.org/10.1109/iccad.2015.7372591
132. Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems*, *91*(NA), 563-573. https://doi.org/10.1016/j.future.2018.08.040
133. Yu, P., Cao, J., Ma, M., Li, H., Niu, B., & Li, F. (2019). WCNC - Quantum-Resistance Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, *NA*(NA), 1-7. https://doi.org/10.1109/wcnc.2019.8885686
134. Yu, S., Wang, G., Liu, X., & Niu, J. (2018). Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective. *IEEE Communications Magazine*, *56*(9), 14-18. https://doi.org/10.1109/mcom.2018.1701204
135. Zafeiriou, I. (2020). IoT and Mobility in Smart Cities. *2020 3rd World Symposium on Communication Engineering (WSCE)*, *NA*(NA), 91-95. https://doi.org/10.1109/wsce51339.2020.9275584
136. Zavrak, & Iskefiyeli, M. (2020). Anomaly-Based Intrusion Detection From Network Flow Features Using Variational Autoencoder. *IEEE Access*, *8*(NA), 108346-108358. https://doi.org/10.1109/access.2020.3001350
137. Zayas, A. D., & Merino, P. (2017). ICC Workshops - The 3GPP NB-IoT system architecture for the Internet of Things. *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, *NA*(NA), 277-282. https://doi.org/10.1109/iccw.2017.7962670
138. Zheng, Y., Dhabu, S., & Chang, C.-H. (2018). ISCAS - Securing IoT Monitoring Device using PUF and Physical Layer Authentication. *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, *NA*(NA), 1-5. https://doi.org/10.1109/iscas.2018.8351844
139. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, *6*(2), 1606-1616. https://doi.org/10.1109/jiot.2018.2847733