Combined Proceedings of the 39th iSTEAMS Bespoke Conference – July, 2025
& iSTEAMS Emerging Technologies onference October, 2025

Society for Multidisciplinary & Advanced Research Techniques (SMART - Scientific Projects & Research Consortium (SPaRC)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
PearlRichards Foundations- Accra Ghana
International Institute for Multidisciplinary and Development Research
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2025

An Overview of Security Systems in the Internet of Things

[1]Fasoyiro Oluwatosin, [2]Fabiyi Ademola, [3]Amosa Babalola & [4]Odesanya Dele
[1]Department of Computer Science, Federal Polytechnic Ede, Nigeria
[2]Department of Cybersecurity, Federal Polytechnic Ede, Nigeria
[3]Department of Computer Science, Kanmi Alo Interlink Polytechnic Ijebu Jesa, Nigeria
[4]Department of Computer Science, Federal Polytechnic Bali, Nigeria
E-mails: samuelteejackson777@gmail.com,fabiyiademolaebony@gmail.com amosabmg@gmail.com
Phone Nos: +234 8162207470, +234 8025600073, +234 8034719314,

ABSTRACT

The rise of the Internet of Things (IoT) has revolutionized many aspects of our daily lives, offering convenience, efficiency, and productivity. This has led to a growing concern about security issues involving IoT devices and networks, and the need for effective security frameworks to protect them. This study aims to address the critical need for a robust and secure Internet of things security framework. Specifically, this study focuses on developing an extensive Internet of Things security framework that addresses the different and changing security problems naturally found in IoT environments. The purpose of this study is to give an overview of where IoT security systems currently stand, including their strengths and weaknesses, and to point to areas needing more research and development. The authors review the current state of the art in areas such as authentication, trust management, privacy, data security, network security, and intrusion detection systems. In addition, the authors discuss the strengths and limitations of knowledge-based, behavior-based and hybrid intrusion detector systems across various factors, such as their level of centralization, resource usage, and detection accuracy rates.

Keywords: IoT, Framework, Knowledge-based, Security, Cyber Crimes, Intrusion Detection

Proceedings Citation Format
Fasoyiro Oluwatosin, Fabiyi Ademola, Amosa Babalola & Odesanya Dele (2025): An Overview of Security Systems in the Internet of Things. Combined Proceedings of the 39th iSTEAMS Multidisciplinary Bespoke Conference 17th–19th July, 2025 & iSTEAMS Emerging Technologies Conference 30th–31st October, 2025. Ghana-Korean Information Resource Centre, Balme Library, University of Ghana, Accra, Ghana. Pp 105-114. www.isteams.net/ghana2025.
dx.doi.org/10.22624/AIMS/ACCRABESPOKE2025P12

1. INTRODUCTION

With the constant advancement of modern information technology, the Internet of Things (IoT) plays a crucial role in various aspects of daily life. The IoT market has expanded rapidly in recent years, enabling multiple devices to be controlled from a single central device, such as a smartphone.

Experts estimate that by 2025, there will be over 75 billion IoT devices worldwide (Statista, 2022). Researchers have examined IoT from both technological and socio-technological perspectives. The technological viewpoint defines IoT as an ecosystem of interconnected devices, while the socio-technological perspective considers its broader societal implications. This diversity of viewpoints highlights the absence of a universally accepted definition for IoT (Goumagias et al., 2021). According to Fang and Dong (2023), IoT refers to the interconnection of various entities within an environment, including machines, appliances, mobile phones, vehicles, cities, and streets. These entities function independently while remaining connected to the internet, enabling data collection and sharing through embedded sensors, software, and technologies. This interconnectivity facilitates automation, real-time monitoring, and data-driven decision-making across numerous domains. IoT is an emerging global internet-based structure that supports information exchange among connected devices (Stana & Hasani, 2018).

An IoT framework provides guiding principles, protocols, and standards that facilitate the implementation and deployment of IoT applications. With careful planning and responsible development, IoT has the potential to revolutionize how we live, work, and interact with our surroundings. Its impact on sectors such as healthcare, transportation, agriculture, and environmental monitoring is significant.

1.1 Overview of IoT Security Challenges

The widespread interconnectivity of IoT presents significant security challenges that must be addressed. The increasing number and diversity of IoT devices generating vast amounts of data introduce new vulnerabilities requiring effective solutions. Key security challenges include:

a. The diversity of IoT devices makes universal security implementation difficult (Mittal et al., 2022).
b. Many IoT devices prioritize functionality over security, employing weak encryption, poor password protection, and inadequate patching (Rad, 2023).
c. Weak identity verification and access control mechanisms allow unauthorized access (Dorri et al., 2021).
d. Data breaches compromise privacy, while a lack of transparency undermines trust (Xu et al., 2023).
e. Insecure communication channels enable eavesdropping and data manipulation (Makwana et al., 2022).

1.2. Importance of Securing IoT Devices And Networks

The lack of adequate security measures in IoT devices presents several threats. Ensuring the security of IoT devices and networks is essential for multiple reasons:

- Firstly, IoT devices collect and exchange sensitive data, including personal and financial information, which is highly valuable to cybercriminals. Implementing robust security measures is crucial to protect user privacy and prevent unauthorized access. Silva et al. (2020) highlighted that the extensive adoption of IoT technology exposes users to various security and privacy risks, as cybercriminals can intercept valuable data either from storage or while in transit.
- Secondly, IoT integration in critical sectors such as healthcare and infrastructure introduces severe risks if compromised (Abomhara & König, 2015). For instance, an IoT security breach in healthcare could result in unauthorized access to patient data or even manipulation of medical devices, posing life-threatening dangers.

This study aims to address the urgent need for a secure IoT framework. Without proper security, personal and sensitive data collected and shared across IoT networks face significant risks (Sicari et al., 2015). The exponential growth of IoT-generated data increases the potential for devastating breaches, with over 90% of IoT devices deemed vulnerable to cyberattacks due to inadequate security measures (Biswas et al., 2018). This lack of protection exposes critical information, such as location data, financial records, and medical histories, to cyber threats.

Additionally, attacks on IoT systems managing critical infrastructure—such as energy, transportation, and healthcare—can endanger public safety (Roman et al., 2018). High-profile incidents, such as the 2016 Distributed Denial of Service (DDoS) attack on DNS provider Dyn using IoT devices (Kolias et al., 2017) and the Stuxnet worm targeting Iran's nuclear facilities in 2010 (Falliere et al., 2011), illustrate the disruptive potential of IoT vulnerabilities. Moreover, unsecured IoT devices pose significant physical safety risks. A survey found that over 80% of organizations acknowledged that cyberattacks on IoT medical devices could directly endanger human lives (Ponemon Institute, 2018). Similarly, the hijacking of IoT components in vehicles, industrial systems, and public infrastructure could lead to physical damage, injuries, or loss of life. A secure IoT framework is necessary to mitigate these risks and ensure public safety.

Given the immense security, economic, and social risks associated with IoT vulnerabilities, developing a comprehensive IoT security framework is an urgent priority. Establishing standardized best practices will help address existing security concerns, guide responsible IoT development, and mitigate threats to individuals and organizations. The objective of this study is to develop a robust IoT security framework that addresses the diverse and evolving security challenges inherent in IoT environments. The specific objectives include:

a) Conducting a thorough review of existing IoT security frameworks and guidelines to assess their strengths, weaknesses, and limitations.
b) Designing and implementing an innovative IoT security framework based on insights gained from the literature review, ensuring it is tailored to the unique security needs of IoT environments.

2. LITERATURE REVIEW

The increasing connectivity of devices, systems, and people through IoT has significantly transformed daily life and work processes. In 2020, an estimated 15.1 billion IoT devices were in use worldwide, with projections suggesting this number will exceed 29 billion by 2030 (Lionel, 2023). However, as IoT adoption expands, so do the associated security risks. One of the most pressing concerns in IoT is its vulnerability to cyber threats. As more devices connect to the internet, the number of potential attack targets for cybercriminals grows exponentially. This has heightened concerns regarding IoT security and the need for effective frameworks to protect IoT networks and devices.

Several IoT security frameworks have been proposed, each with its advantages and limitations. For example, the National Institute of Standards and Technology (NIST) has developed a framework emphasizing the security of IoT devices and networks while safeguarding sensitive data (NIST, 2024). Similarly, the International Organization for Standardization (ISO) has introduced a framework that underscores the importance of risk assessment and security implementation (ISO, 2022). Figure 1 illustrates the historical and projected growth of IoT devices worldwide.

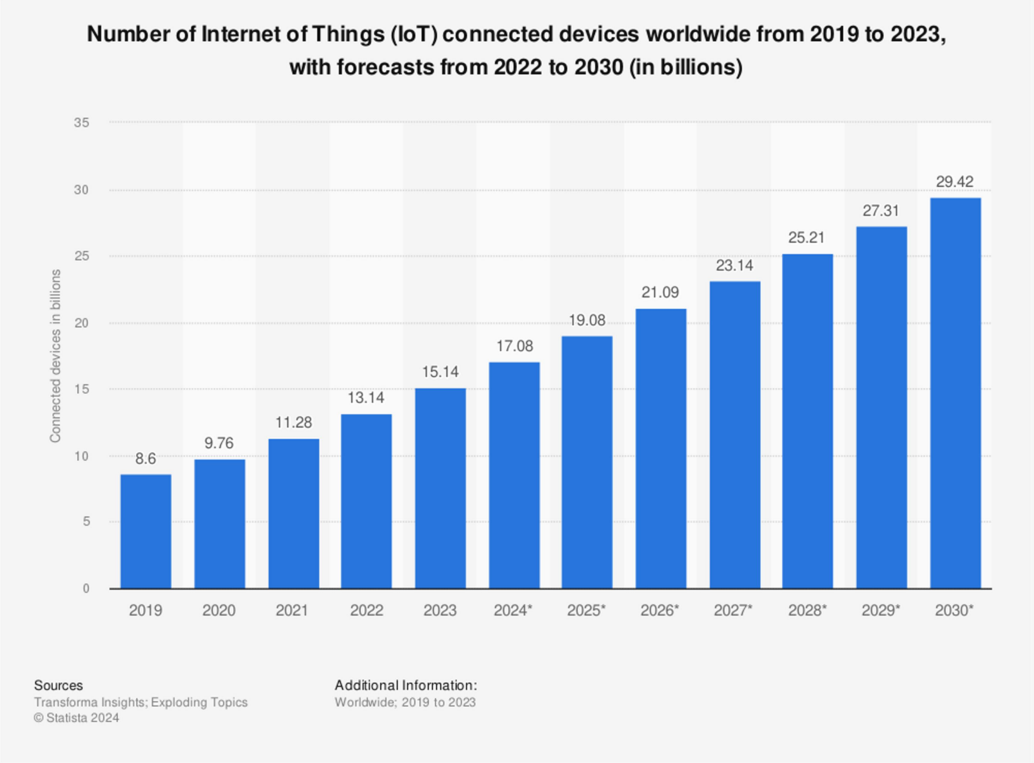

Figure 1 - IoT Devices Forecasts by (source: Statista)

The purpose of this literature review is to provide an overview of the current state of IoT security frameworks, highlighting their strengths and weaknesses while identifying areas that require further research and development. By examining existing studies on IoT security frameworks, this review aims to enhance the understanding of challenges and opportunities in this field and contribute to the development of more robust and effective security solutions. The Internet of Things (IoT) refers to a network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and internet connectivity, enabling them to collect and exchange data (Greengard, 2024). IoT encompasses various "smart" devices that function similarly to computers, allowing them to connect to the internet or communicate wirelessly. These devices range from simple smart home products, such as thermostats, to wearables like smartwatches and clothing, as well as complex industrial equipment and transportation systems (Appiah & Kwao, 2023). As IoT adoption accelerates, the world is becoming increasingly interconnected at an unprecedented pace.

IoT Applications and Industries

The applications of IoT are vast and diverse, with a significant impact across industries such as manufacturing, transportation, healthcare, and agriculture (Rajiv, 2020). Industrial IoT (IIoT) refers to the integration of complex machinery with networked sensors and software, enabling automation and data-driven decision-making. IIoT applications are widely used in manufacturing, mining, agriculture, energy management, healthcare, and transportation, driving Industry 4.0—an era of advanced automation and data exchange in manufacturing (Neuron, 2023). Figure 2 illustrates how IoT enhances smart manufacturing processes.

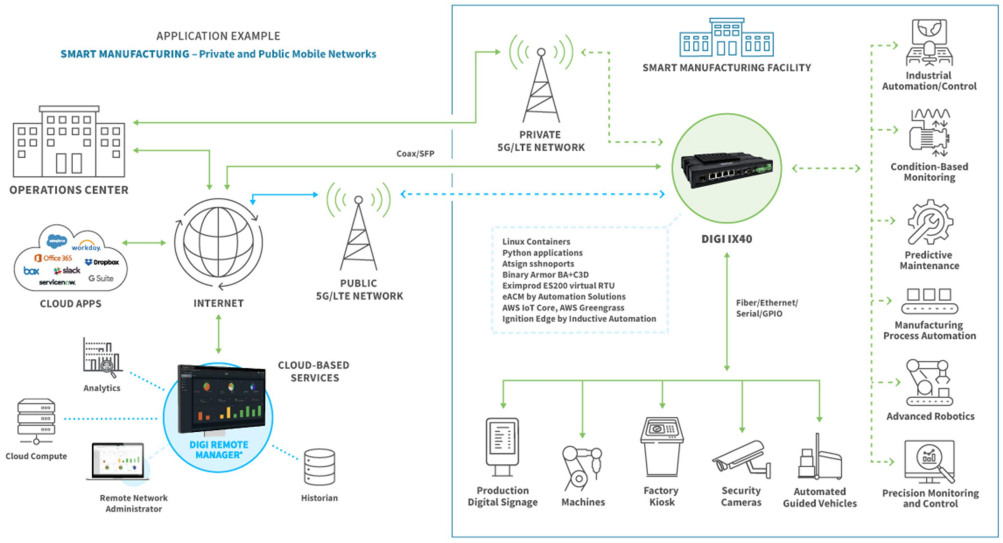

Figure 2 - Smart Manufacturing in Practice

The Industrial Internet of Things (IIoT) involves deploying sensors and smart machines to capture and transmit data, monitor temperature, flow, and volume changes, automate processes for efficiency, accuracy, and safety, and ensure data reaches the right individuals for analysis and decision-making. Additionally, IIoT ensures that all these processes operate reliably and securely on schedule (Quinn, 2023).

3. IoT SECURITY FRAMEWORKS

Several studies have addressed the growing security threats within the IoT paradigm. Some approaches focus on specific layers, while others pursue end-to-end security solutions. One analysis categorized risks by architecture, data, communication, and applications (Kozlov, Veijalainen & Ali, 2012). The study noted that vulnerabilities emerge as more devices become "smart" and interconnected. Identified threats include poor device authentication, lack of encryption allowing data interception, and an extensive attack surface due to numerous endpoints. Similarly, another survey by Granjal, Monteiro, and Silva (2015) discussed security issues related to IoT protocols.

Abduvaliyev et al. (2013) analyzed key management systems and cryptographic algorithms while comparing intrusion detection systems, with a specific focus on wireless networks. The study explored unique security challenges posed by wireless technologies and the IoT. Mitchell and Chen (2014) similarly categorized and summarized various intrusion detection methods tailored for wireless environments, assessing misuse detection techniques reliant on predefined signatures and anomaly detection approaches that monitor normal usage patterns. Their study evaluated knowledge-based, behavior-based, and hybrid intrusion detection systems across factors such as centralization, resource usage, and detection accuracy. The survey further examined intrusion detection solutions for wireless LANs and wireless sensor networks, commonly used in IoT infrastructure.

Additionally, research has evaluated encryption techniques to preserve privacy and data security within fog computing, where data processing and storage are decentralized. Sicari et al. (2015) reviewed research contributions addressing security, confidentiality, integrity, privacy, and access control, including security within middleware architectures. Building on this, Roman, Lopez, and Mambo (2018) explored security considerations in edge computing-based frameworks, such as mobile edge computing, mobile cloud computing, and fog computing. Their work delved into identity and authentication, access control, trust management, fault tolerance, network security, and forensic capabilities in decentralized computing paradigms. Stoyanova et al. (2020) provided an overview of IoT forensics, emphasizing the need for standardization. They argued that standardizing forensic processes is crucial for high-quality forensic reporting across jurisdictions and adherence to cybersecurity best practices.

4. IMPORTANCE OF IOT SECURITY

The rise of the Internet of Things (IoT) has transformed various aspects of life, offering convenience, efficiency, and productivity. However, IoT security has become a critical concern with implications for personal and national security, economic stability, and ethical considerations.

a) **Impact on Personal and National Security:** The proliferation of IoT devices makes them prime targets for cyberattacks due to inadequate security measures (Alaba, Othman, & Hashem, 2017). Attacks can result in personal data breaches, device hijacking for malicious purposes, and disruption of critical infrastructure (Cui et al., 2018). The impact on national security is even more severe, as IoT-based attacks can infiltrate sensitive government systems or disrupt essential services (Sadhu, Yanambaka, & Abdelgawad, 2022). Strengthening IoT security is crucial to mitigating these risks.

b) **Economic Implications:** IoT security breaches can have significant financial consequences for businesses relying on these technologies. Companies may suffer losses due to data breaches, system downtime, and remediation costs (Mehrnezhad et al., 2016). Additionally, reputational damage resulting from security incidents can erode consumer trust and reduce revenue (Laghari et al., 2021). The broader economic impact extends to industries, governments, and consumers (Yan et al., 2010). Implementing strong IoT security measures can help prevent these potentially devastating financial losses.

c) **Ethical Considerations:** The widespread use of IoT devices raises ethical concerns related to privacy and data protection. As these devices collect and transmit vast amounts of personal data, risks of misuse or unauthorized access arise (Alaba, Othman, & Hashem, 2017). Moreover, IoT-enabled surveillance and potential erosion of individual autonomy require careful consideration (Cui et al., 2018). Ensuring ethical IoT development and deployment is essential to maintaining public trust and safeguarding individual rights (Yan et al., 2010).

Addressing IoT security challenges is essential for unlocking the full potential of this technology and ensuring a secure, sustainable future. Developing a robust IoT security framework protects sensitive information, prevents financial losses, and maintains business continuity. Ethical considerations related to privacy, data security, and user trust must also be prioritized.

4.1 Consequences of IoT Security Breaches

The rapid expansion of IoT has transformed various industries, enabling unprecedented levels of connectivity. However, this increased connectivity has introduced significant security risks. IoT security breaches pose serious threats to individuals, organizations, and society. In recent years, several high-profile IoT security breaches have gained attention. In 2021, a vulnerability in the Verkada security camera system allowed hackers to access thousands of surveillance feeds, exposing sensitive information from offices, hospitals, and schools.

IoT security incidents can lead to substantial financial losses, with an average cyber loss of $1.56 million per incident (Statista, 2022). Breaches compromise the confidentiality, integrity, and availability of IoT systems, resulting in data theft, system disruptions, and potential physical harm to connected devices (Kumar, Vealey, & Srivastava, 2016). Additionally, vulnerabilities in a single IoT device can be exploited to infiltrate entire networks, jeopardizing sensitive data, critical infrastructure, and even national security (Baldini et al., 2018).

As society becomes increasingly reliant on IoT, the consequences of security breaches can be widespread. Malicious actors can exploit IoT vulnerabilities to launch large-scale attacks, such as Distributed Denial-of-Service (DDoS) attacks, which disrupt essential services and infrastructure (Makhdoom et al., 2019). Furthermore, unauthorized access to personal information, such as location, health data, and home security systems, can lead to privacy violations and physical harm. IoT breaches in sectors like healthcare, transportation, and energy pose risks to human lives and disrupt critical services (Baldini et al., 2018).

As the frequency of IoT security incidents continues to rise, it is imperative to implement robust security measures and effective frameworks to mitigate these risks. Understanding the different aspects of IoT security breaches and their impact on individuals, organizations, and society is crucial for developing comprehensive security solutions.

5. CONCLUSION

The advent of the Internet of Things has led to significant advancements, enhancing convenience, efficiency, and productivity for users. However, increased connectivity and the widespread adoption of IoT devices have raised serious security concerns. Establishing strong IoT security frameworks is critical for safeguarding sensitive information, ensuring data integrity, preventing unauthorized access, and protecting critical systems. This research highlights the necessity of such frameworks by critically evaluating existing IoT security solutions, proposing an innovative design for secure IoT system implementation, and advocating for responsible deployment.

Additionally, the paper reviews current IoT security systems, identifying strengths, limitations, and areas requiring further research. Failure to implement adequate security measures can lead to personal data breaches, privacy violations, and safety risks associated with compromised IoT-based control systems. The implications of unattended security flaws in IoT systems extend to individual well-being, national security, economic stability, and ethical concerns. To mitigate these risks, an all-inclusive IoT security framework must be developed and implemented. Stakeholders must remain informed about potential IoT security breaches and their consequences, ensuring proactive measures to protect individuals, organizations, and society at large.

REFERENCES

Abduvaliyev, A., Pathan, A. S., Zhou, J., Roman, R., & Wong, W. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials.

Abomhara, K., & König, S. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility.

Alaba, F. A., Othman, M., & Hashem, I. A. T. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications.

Appiah Osei, B., & Kwao-Boateng, E. (2023). Critical Review on Internet of Things (IoT): Evolution and Components Perspectives. IntechOpen. doi: 10.5772/intechopen.109283

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the Internet of Things. Science and engineering ethics, 24(3), 905-925.

Biswas, K., Muthukkumarasamy, V., & Sarker, V. K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411. https://doi.org/10.1016/j.future.2017.08.017

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. IEEE Access, 6, 19884-19894. https://doi.org/10.1109/ACCESS.2018.2853985

Dorri, A., Moustafa, N., & Choo, K.-K. R. (2021). Blockchain for IoT Security: A Survey. IEEE Communications Surveys & Tutorials, 24(2), 1153-1188. European Union. (2016). General Data Protection Regulation. https://gdpr-info.eu/

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet dossier. White paper, Symantec Corp., Security Response, 5, 29.

Fang, L., & Dong, Y. (2023). Definition, Challenges and Future Research for Internet of Things. Journal of Computing and Natural Science.

Goumagias, N., Whalley, J., Dilaver, O., & Cunningham, J. (2021). Making sense of the internet of things: a critical review of internet of things definitions between 2005 and 2019. Internet Research, 31(5), 1583-1610.

Granjal, J., Monteiro, E., & Sá Silva, J. (2015). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials.

Greengard, S. (2024). Internet of Things. Encyclopedia Britannica. https://www.britannica.com/science/Internet-of-Things

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

Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. Proceedings of the 7th International Conference on Body Area Networks.

Kumar, S., Vealey, T., & Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. pp. 5772-5781. doi:10.1109/HICSS.2016.714

Laghari, A.A., Wu, K., Laghari, R.A., Ali, M., & Khan, A.A. (2021). A Review and State of Art of Internet of Things (IoT). Archives of Computational Methods in Engineering, 29, 1395 - 1413.

Lionel Sujay Vailshery. (2023). IoT connected devices worldwide 2019-2030. Retrieved May 17, 2024, from [https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/]

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.

Makwana, P. P., Shukla, A., & Patel, P. (2022). Secure Communication for Internet of Things (IoT) Using Physically Unclonable Function (PUF). Sensors (Switzerland), 22(15), 5513.

Mehrnezhad, M., Toreini, E., Shahandashti, S.F., & Hao, F. (2016). Stealing PINs via mobile sensors: actual risk versus user perception. International Journal of Information Security, 17, 291 - 313.

Mitchell, R., & Chen, I. (2014). A survey of intrusion detection in wireless network applications. Computer Communications.

Mittal, S., França, F. M., & Thingalaya, A. (2022). Machine Learning for Heterogeneous IoT Devices: A Survey. ACM Computing Surveys, 55(2), 1-37.

National Institute of Standards and Technology. (2024). NIST Cybersecurity for IoT Program. Retrieved May 17, 2024, from https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

Neuron Team. (2023). 18 Industrial IoT Applications and Why You Need Them. https://www.emqx.com/en/blog/industrial-iot-applications

NIST. (2024). The CSF 1.1 Five Functions. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions.

Ponemon Institute. (2018, October). Cost of a Data Breach Study: Global Overview. IBM. https://www.ibm.com/downloads/cas/ZYKLN2E3

Quinn Jones. (2023). What Is Industrial IoT (IIoT)? Definition, Use Cases and Application Examples. https://www.digi.com/blog/post/what-is-industrial-iot-definition-use-cases

Rad, E. M. (2023). A Survey on Security of Internet of Things (IoT) Devices. Journal of Network and Computer Applications, 202, 103354.

Rajiv. (2020). Applications of Industrial Internet of Things (IIoT). https://www.rfpage.com/applications-of-industrial-internet-of-things/

Roman R., Lopez J., & Mambo M. (2018) Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges, Future Generation Computer Systems.

Roman, R., Najera, P., & Lopez, J. (2018). Features, requirements, and challenges for the internet of robotic things. In 2018 IEEE International Conference on Robotics and Automation (ICRA) (pp. 1-9). IEEE. https://doi.org/10.1109/ICRA.2018.8460557

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors (Basel, Switzerland), 22(19), 7433. https://doi.org/10.3390/s22197433

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

Silva, Silva, Neto, Lemos, Neto, & Esposito. (2020). A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. Sensors.

Stana, A., & Hasani, S. (2018). The rise of internet of thing and the risk of threats. Interdisciplinary Journal of Research and Development.

Statista. (2022). Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E.K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE Communications Surveys & Tutorials, 22, 1191-1221.

Xu, L., Zhao, S., Min, G., et al. (2023). Lightweight Privacy-Preserving Authentication for Secure and Efficient Data Aggregation in Industrial IoT. IEEE Transactions on Industrial Informatics, 19(2), 1222-1232

Yan, H., Huo, H., Xu, Y., & Gidlund, M. (2010). Wireless sensor network-based E-health system-implementation and experimental results. IEEE Transactions on Consumer Electronics, 56(4), 2288-2295.