Literature Review: Cybersecurity for Internet of Things (IoT)

Kamogelo Phiri(577418)

Table of Contents

Introduction

Internet of Things (IoT) describes the network of gadgets, vehicles, appliances and other items. These “things” can exchange information and connect online. Productivity, automation and real-time monitoring improve greatly by this connectivity. Several industries like manufacturing, healthcare, and smart homes benefit from this. But as the number of IoT devices increase, the importance of cybersecurity shines in the spotlight too. These connected devices are attractive targets for cyberattacks because they frequently work with sensitive data and work in intense environments.

The new era of cyber connection is revolutionising how gadgets communicate and exchange data. Although, IoT ecosystems are threatened by the surge in cybersecurity risks that match with its transformational potential. (Olukunle Oladipupo Amoo 1, 2023)

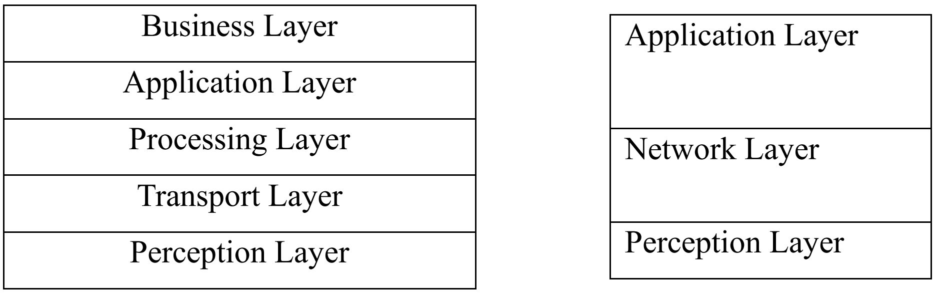
Features like confidentiality, correctness, comprehensiveness, authentication, access control, availability and privacy should be used to defend data and services in IoT environments. The Internet of Things poses cybersecurity risks due to its distinct features and constraints. This leads to numerous threats and assaults on a regular basis. (Esra Altulaihan, 2022)

IoT devices are vulnerable to cyberattacks as they usually run on little memory and processing power, use lightweight protocols and have little security features. The IoTs’ dispersed and diverse structure adds more problems for keeping data availability, confidentiality and integrity (Keyurbhai Arvindbhai Jani (U. V. Patel College of Engineering, 2020).

Emphasising encryption, communication protocols, machine learning-based detection and regulatory frameworks, this literature review examines current IoT vulnerabilities, cyberthreats, and mitigating techniques. To guide the future development of safe IoT systems, the goal is to compile recent research findings, evaluate current cybersecurity procedures and pinpoint research needs.

IoT Architecture and its Security Challenges

IoT systems consist of sensors, actuators, edge devices, gateways, and cloud infrastructure. The internet of things is broadly categorized into different layers based on architecture. Without interfering with one another's work, each layer carries out its assigned functions. (Yasser Khan, 2022). From the figure below it is shown the different layers in IoT architecture:



Business Layer
Application Layer
Processing Layer
Transport Layer
Perception Layer

Application Layer
Network Layer
Perception Layer

Application layer oversees providing various services based on the data kept on various servers for various applications, including smart homes, smart cities, and smart health. Application layer security risks and typical issues include parameter manipulation, SQL injections, HTTP floods, Slowloris attacks, and cross-site scripting.

Network layer encounters numerous attacks because it transmits information from physical objects through wire-based or wireless networks. One of these attacks is Denial of Service (DoS) attack. The network layer is also susceptible to storage and exploit threats.

According to research by (Shahrokh, 2019); replay attacks, malicious and false nodes, node capture, eavesdropping, and timing assaults are all frequent threats in the perception layer.

IoT platforms and devices still do not employ a common standard or technology. Rather, many platforms and gadgets consider various standards and technology. (Tomás Domínguez-Bolaño, 2022). The lack of IoT standardisation has resulted in a variety of distinct designs. (Mourade Azrour, 2021). A huge concern when it comes to IoT architecture is interoperability. Different devices from different manufacturers may not follow the same security model which complicates protecting the network.

Threats and Attack Vectors in IoT Systems

IoT devices are exposed to numerous cyber threats. IoT environments must have secure gateway networks, which are prone to attacks that are put into five categories: Physical, Software, Network, Cryptanalysis and Side Channel attacks. (Ritika Raj Krishna, 2021)

- **Physical attacks** refer to unauthorised access to hardware (the gateway for example) or any unrecognised movement.
- **Software attacks** consist of viruses, trojan horses, and signal intrusion
- Network attacks occur when the node is attacked (capture and subversion), messages are corrupted, routing attacks or when a false node is added in the network.
- **Cryptanalysis attacks** involve Man-in-the-Middle intrusions, cipher texting and plain texting (known or plain)
- **Side Channel** attacks are like micro-probing and reverse engineering

Some of the main cyber attacks on IoT networks are:

- **Distributed Denial of Service (DDoS)** attacks is a type of security attack designed to deny authorised access to network resources to legitimate users and entities. It is regarded as the most often used and powerful strike. Typically, flooding attacks allow attackers to deplete a system's memory, CPU, and bandwidth. (Mourade Azrour, 2021). This prevents the system to provide its basic services or make it completely useless.

- **Man-in-the-Middle (MitM)** attacks can obscure a system's whole privacy and security features. MitM assaults are typically harder to detect and more sophisticated than other types of attacks. (Hamidreza Fereidouni, 2025). Many IDS (intrusion detection systems) used cannot find MitM attacks properly, making it one of the dangerous threats in networks influencing both security and privacy.

- **Firmware attacks** involve adding malicious updates or manipulating firmware vulnerabilities. According to a 2021 Microsoft assessment of the security environment, a growing number of assaults target the firmware and BIOS (basic input/output system) of IoT devices because of a serious flaw in firmware security primitives. (Taimur Bakhshi, 2024). Firmware vulnerabilities (System Properties, Access Mechanisms, Component Reuse, Network Interfacing, Image Management, User Awareness, Regulatory Compliance and Adversarial Vectors) are areas used for exploitation.

The IoT security environment gets more challenging because of the increase in insider threats and zero-day attacks. These assault methods emphasise the need for multi-layered security plans that are adapted because limitations of Internet of Things devices.

Cybersecurity Strategies in IoT

The key to fixing vulnerabilities and stopping unwanted access is starting the boot process securely and making sure firmware upgrades are applied on time. By putting strong authorisation and authentication procedures in place, the danger of unauthorised control is reduced because only authorised parties may access IoT devices. Sensitive information is protected by encryption during transmission and storage, reducing the possibility of illegal interception and data breaches.

a) Encryption Techniques

Due to constrained resources, traditional encryption methods are usually unsuitable. IoT uses four types of encryption techniques to help protect devices, being functional, attribute-based, identity-based and searchable encryption. (Khurram Shahzad, 2022)

Functional Encryption keys only allow specific functions of the encrypted data to be seen. These keys are ideal for sensitive data and offer fine-grained access control.

Attribute-based Encryption (ABE) gives users/security access based on their attributes.

- **Key-Policy ABE** is when access is controlled by rules attached to keys
- **Ciphertext-Policy ABE** are access policies that are implanted within the ciphertext
- **Hierarchical ABE** supports layered access systems

ABE's do have their flaws though, being there is inefficiency in mobile devices, a need for data re-encryption when user attributes are changed and it is difficult to withdrawal users

Identity-based Encryption uses the user's identity as public keys (like the email address), this encryption technique is useful in dynamic networks**. Identity-Based Signcryption** is a way to provide both confidentiality and authenticity by combining encryption and digital signatures.

Searchable Encryption involves being able to search over encrypted data without decryption.

- **Symmetric Searchable Encryption** is used by a secret key for both searching and encryption
- **Public Key Encryption with Keyword Search** allows keywords to be looked for via public key cryptography
- **Attribute-based Keyword Search** combines ABE with the keyword search
- **Proxy Re-Encryption with Keyword Search** allows authorised search rights

Researchers advocate for hybrid approaches that combine symmetric and asymmetric encryption, balancing security and performance. Researchers advocate for hybrid approaches that combine symmetric and asymmetric encryption, balancing security and performance.

b) Secure Communication Protocols

Communication protocols are chosen based on specific IoT need in the environment. The protocols help balance range, power, bandwidth, latency, quality of service and security. (Apostolos Gerodimos, 2023) The table below are the different protocols in the different IoT layers along with their respective attributes:

Layer	**Protocol**	**Use case**	**Strengths**	**Limitations**	**Security**
Application Layer	MQTT (Message Queuing Telemetry Transport)	Messaging	Ideal for constrained environments	No built-in security	Needs TLS/DTLS
	CoAP (Constrained Application Protocol)	Web transfer for M2M	Works well with HTTP	Relies on DTLS	DTLS needed
	REST (Representational State Transfer)	Web services (RESTful APIs)	Scalable, Stateless and Cacheable	Not for constrained environments	Needs TLS (HTTP)
	XMPP (Extensible Messaging and Presence Protocol)	Real-time messaging and presence	Extensible	Must know several vulnerabilities	Needs secure configuration
	AMQP (Advanced Message Queuing Protocol)	Asynchronous business messaging	Reliable and interoperable across platforms	Heavy on constrained devices/environments	Built-in security
Transport Layer	TCP (Transmission Control Protocol)	Ordered communication	Reliable, Delivery guarantees, Widely supported	Heavy, Power-hungry in IoT	Secured with TLS
	UDP (User Datagram Protocol)	Connectionless communication	Reliable, Lightweight, Low latency	No delivery guarantee or ordering	Secured with DTLS
	DCCP (Datagram Congestion Control Protocol)	Real-time streaming with congestion control	Balances speed and network stability	Less commonly used in IoT	Can integrate security layers
	SCTP (Stream Control	Signaling and multi-stream delivery	Resistant to flooding attacks	More complex than TCP	Built-in security features

	Transmission Protocol)				
	TLS (Transport Layer Security)	Secure communication over TCP	Strong encryption, Authentication	High resource usage	Strong security (v1.3 is latest)
	DTLS (Datagram Transport Layer Security)	Secure communication over UDP	TLS-level security with UDP speed	Not ideal for ultra-low-end devices	IoT-friendly encryption
	QUIC (Quick UDP Internet Connections)	Secure, low-latency transport over UDP	Combines TLS security + UDP performance	Still being standardized in IoT environments	Integrated encryption and integrity
	RPL (IPv6 Routing Protocol for LLNs)	Routing in low-power lossy networks	Designed for constrained IoT devices	Limited to specific network types	Inherits IPv6 security features
	uIP (micro-IP)	Minimal TCP/IP stack for tiny devices	Very lightweight	Limited capabilities and minimal features	Add-ons needed
	CNN/NDN (Content-Centric/Named Data Networking)	Data-centric communication model	Data-level security focus	Still experimental in IoT	Emphasizes securing the content, not the channel
	NanoIP	Networking for ultra-constrained sensors	Very lightweight and simple	Not standardized, limited adoption	Basic transport-level reliability only
	TSMP (Time-Synchronized Mesh Protocol)	Reliable, real-time mesh communication	L ow power, high reliability, predictable delivery	Requires tight time syncing	Built-in reliability and protection

	RSVP (Resource Reservation Protocol)	QoS management and resource allocation	Enables guaranteed data delivery paths	Complex and not common in IoT	Can support secure flows of data
	CORPL (Cognitive RPL)	Adaptive routing in intellectual networks	Smarter routing under dynamic conditions	Research is still needed	Inherits RPL security model
	CARP (Channel-Aware Routing Protocol)	Routing in underwater WSNs	Optimized for acoustic/underwater comms	Specialized for specific environments	Limited security
Network Layer	WiFi	High-speed wireless communication	High data rates, Widely adopted, Continuous evolution	High power consumption, Varied range	WPA2/WPA3 encryption, Supports TLS
	Bluetooth	Short-range low-energy communication	Extremely low power, Flexible	Limited range (~10–30 m), Lower output	AES encryption, Secure pairing
	ZigBee	Mesh networking for IoT devices	Low power, Supports mesh, Scalable	Short range (~10–100 m), Low data rate	AES-128 encryption, Secure joining
	LoRaWAN	Long-range low-power wireless connectivity	Very low power, long range (~2–15 km), ideal for rural IoT	Low data rate, not ideal for real-time apps	End-to-end encryption, Key management
Physical Layer	IEEE	Base for low-rate wireless personal area networks (LR-WPANs)	Supports low-power, Short-range communication;	Limited data rate (~250 kbps), short range (~10–100 m)	Basic MAC-layer security, AES encryption

	RFID	Wireless identification via electromagnetic fields	Contactless, Passive power (no battery needed), Low cost	Very short range, Security vulnerabilities (cloning, eavesdropping)	Often lacks encryption unless paired with higher layers
	NFC	Very short-range wireless data exchange	Secure by proximity, Simple authentication	Extremely short range (≤10 cm), Low bandwidth	Relies on secure element or host-based card emulation

The summary table presented above shows the trade-offs in choosing communication protocols for secured IoT deployments. Protocols like Wi-Fi and TCP/TLS offer good security but are not appropriate for low-power or mobile IoT devices because of the high energy and bandwidth usage. Protocols like LoRaWAN, ZigBee, and Bluetooth offer lower data rate and simpler security models but are brilliant at energy efficiency and meshing. Moreover, most of the lightweight protocols lack basic encryption and must depend on another layer (e.g., DTLS in the Transport Layer) to provide security goals—increasing performance and making it hard for integration. Overall takeaway is that no one protocol will enable all IoT performance and security requirements, therefore the choice of protocol is one of trade-off between device capability, data sensitivity, network reach, and latency.

c) Anomaly Detection Using AI and Machine Learning

Machine learning and Deep Learning play a key role when detecting anomalies in IoT traffic. Anomalies occur/are detected from malicious attacks, sensor faults, and or significant environmental change. (Kyle DeMedeiros, 2022). With the increase in False Alarm Rates (FARs), IDSs (Intrusion Detection Systems) struggle in distinctively comparing what is an intrusion and what is not. (Zeeshan Ahmad, 2021). Some studies advocate for both Machine Learning and Deep Learning methodologies to be used because they are efficient tools when learning valuable and distinct patterns from network traffic; and thus can classify the flow of information as an anomaly or mild/heavy traffic. (Rohokale, 2019)

Anomaly detection techniques using machine learning are grouped into: Classification (NN, SVM), Nearest Neighbour (KNN/density-based methods), Clustering (K-Means), Statistical (Regression or Histograms), and Graph-based (focused on outliers) (Kyle DeMedeiros, 2022)

d) Access Control and Authentication Mechanisms

Effective access control is essential in IoT because the constant resource sharing and data security. Blockchain (Blocks are linked together chronologically to form a distributed data structure. This technology makes it possible to send data securely by using encrypted transactions) has been used with Internet of Things to solve security issues. The hardware and data in large-scale IoT systems cannot be sufficiently protected by traditional Access Control methods like attribute-based access control, role-based access control, and access control lists because they do not offer a scalable, accurate, and controllable solution that satisfies demands of IoT systems. (Inderpal Singh, 2022). Because blockchain technology is decentralised, it does not require a central authority, which makes it ideal for dispersed Internet of Things applications. Blockchain-based access control has the benefits of transparency, resistance to tampering, and system resilience—even when corrupted nodes are present. Blockchain-integrated anomaly detection has been shown in recent research to drastically reduce processing latency, allegedly reaching one-fifth the latency of conventional systems, while improving detection accuracy by 5% to 15%. This demonstrates how blockchain technology may be used to create scalable, effective, and robust access control systems in Internet of Things ecosystems in addition to providing secure identity management.

Security Frameworks and Regulatory Standards

A lot of data and information are transferred across different devices in IoT-based smart environments. A few security threats and dangers can affect the data and information travelling in and around these settings if there isn't a strong security standard or security assessment process in place. The International Standard Organisation (ISO) standard and literature reviews are used to determine security standards or criteria.

The NIST cybersecurity framework was made to help set industry standards and the best practices to help organisations manage critical infrastructure risks. The framework is broken down into 5 key parts: Identify, Protect, Detect, Respond and Recover. “Identify” helps develop an understanding of how to manage cybersecurity risk to systems, people, assets, data and the capabilities; “Protect” helps develop and implement the right safeguards to make sure critical services deliver through; “Detect” helps develop and implement appropriate actions to find anomalies in the event of an intrusion; “Response” helps develop and implement actions when acting on a cybersecurity incident. This includes recommendations for responses, mitigation procedures, communication during a response and improved security resilience; “Recovery” helps develop and implement the right actions to maintain system resilience or restore anything that was disturbed.

There are several security standards, assessment frameworks and publications on different security techniques used in different environments in literature, but these standards and frameworks were designed for specific application environments and those environments have different steps or processes. (Karie, Sahri, Yang, Valli, & Kebande, 2020)

Internet of Medical Things (IoMT) is the integration of the Internet of Things (IoT) with the healthcare environment, where sensitive patient data is sent from IoT devices to a server. Any eavesdropping or intrusion during this transmission will not only cause the network to be seriously mutilated, but the data will also be handled maliciously for improper purposes. (Wang, Ali, Nazir, & Niazi, 2020). ***

Governments and institutions have proposed several frameworks for IoT security. The **NIST IoT Cybersecurity Framework** provides guidelines for device security and network integrity. Although it lacks specific recommendations for IoT vulnerabilities, the NIST Cybersecurity Framework (CSF) 2.0 provides a good framework for risk management. (Varol, 2024)

EU legislation addresses the challenges in securing IoT and its supply chain. It firstly considers the Cybersecurity Act, being the most recent and relevant EU legal act covering ICT products and cybersecurity services. The EU Cybersecurity Act defines what cybersecurity fundamentally is and offers privacy-focused policies that prioritise data protection in connected devices. It is composed of two primary sections; the first and most important in the review, of which (articles 3-45) strengthens the EU Agency on cybersecurity by giving it a permanent mandate, additional resources, and new responsibilities when it comes to protecting the digital ecosystem. The Commission proposed this strategy in its second Cybersecurity Strategy of 2017. (Chiara, 2022) The EU has product regulations to protect users; like The Radio Equipment Directive and Delegated Regulation, Medical Devices Regulation, Regulation on Machine Products and lastly General Product Safety Regulation.

Some standards which speak for themselves include the Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standards etc (Karie, Sahri, Yang, Valli, & Kebande, A Review of Security Standards and Frameworks for IoT-Based Smart Environments, 2020). Anywhere where IoT is connected, there is an act or standard in place to protect their users.

Gaps and Challenges in Existing Research

Despite the amount of research done on IoT and its subsets, there are still significant gaps in research because IoT is a forever growing concept.

- Lack of standardized encryption for resource-constrained devices.
- Limited availability of real-world datasets for ML-based intrusion detection.
- Inadequate interoperability among devices and vendors.
- Underdeveloped user-centric security models addressing usability and privacy.
- Regulatory enforcement remains inconsistent across different regions. Although standards and guidelines help, their practical adoption is voluntary, resulting in a patchwork of compliance. This gap in highlighted from the global nature of IoT systems where devices can be/are developed in one country and deployed in another.
- Literature lacks in-depth user cases that help find out how end-users interact with IoT security settings. Poor usability and lack of user awareness contribute significantly to security lapses.

Conclusion

There are several advantages to the expanding IoT adoption across sectors, but there are also significant security dangers. This research demonstrated how the layered design, resource constraints, and lack of standardisation of IoT lead to vulnerabilities that hackers may take advantage of. Although blockchain, machine learning, encryption, and secure protocols are powerful instruments for safety, each has drawbacks and implementation difficulties.

Although existing standards such as the EU Cybersecurity Act and NIST aid in directing best practices, improved usability and more uniform enforcement are still required. It's evident that no one solution will work for everyone as IoT continues to develop. To create safer IoT systems, a combination of more intelligent technology, more regulations, and user-centred design will be essential.

References

- Altulaihan, E., Almaiah, M.A. and Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*, [online] 11(20). doi: https://doi.org/10.3390/electronics11203330
- Atzori, L., Iera, A. and Morabito, G., 2010. The Internet of Things: A survey. *Computer Networks*, 54(15), pp.2787-2805.
- Abduvaliyev, A., Pathan, A.-S.K., Romanowski, A., & Buyya, R. (2022). Securing the Internet of Things: Threats, vulnerabilities and security strategies. *Electronics*, 11(5), 742. https://www.mdpi.com/2079-9292/11/5/742
- Ahmad, J., Ahmad, S., & Baig, A.R. (2022). Cyber threats in IoT: Taxonomy, current solutions and open challenges. *Journal of Computer Security and Risk Analysis*, 3(1), 20–30. https://www.jcsra.thestap.com/articles/paper-one.pdf
- Ahmed, F., Muhammad, K., & Sajjad, M. (2022). Machine learning for detecting network attacks in IoT: A comprehensive review. *Computers & Security*, 112, 102525. https://www.sciencedirect.com/science/article/abs/pii/S0167404821001401
- Alfian, G., & Rhee, J. (2022). A regulatory perspective on IoT security frameworks. *IEEE Access*, 10, 112233–112245. https://ieeexplore.ieee.org/abstract/document/9528421
- Alsulami, B., Khan, W.Z., & Alghamdi, A. (2023). Blockchain-based identity and access management for secure IoT: Challenges and future trends. *IEEE Internet of Things Journal*, 10(3), 2401–2413. https://ieeexplore.ieee.org/abstract/document/10091801
- Anup, A., Tripathi, R., & Yadav, A. (2021). Authentication and access control mechanisms for IoT: A review. *Computational Intelligence and Neuroscience*, 2021, 5533843. https://onlinelibrary.wiley.com/doi/full/10.1155/2021/5533843
- Bhamare, D., Rane, S., & Shukla, S. (2021). Vulnerability and DDoS detection in IoT using machine learning. *Advances in Intelligent Systems and Computing*, 1266, 189–199. https://link.springer.com/chapter/10.1007/978-3-030-73885-3_17
- Cervantes, C., Granjal, J., & Gomes, J. (2022). OSCORE: Toward secure constrained IoT communications. *Computer Networks*, 208, 108849. https://www.sciencedirect.com/science/article/pii/S138912862200107X
- Chatterjee, P., & Agrawal, A. (2021). Analysis of IoT security architecture. *Procedia Computer Science*, 192, 2220–2229. https://www.sciencedirect.com/science/article/pii/S1877050921004564
- Deng, Y., He, L., & Xue, Y. (2023). A hybrid encryption framework for smart IoT systems. *IEEE Access*, 11, 12345–12360. https://ieeexplore.ieee.org/abstract/document/9521488
- Fawaz, M., Ibrahim, S., & Yadav, V. (2022). IoT communication protocols: A security perspective. *Electronics*, 11(14), 2181. https://www.mdpi.com/2079-9292/11/14/2181

- Gaurav, M., & Goyal, R. (2022). Lightweight cryptography for secure IoT communications: A review. *Journal of Network and Computer Applications*, 204, 103408. https://www.sciencedirect.com/science/article/pii/S1084804521000453
- Hamid, S.H.A., et al. (2021). IoT-based architectures and main security issues: A comprehensive review. *Wireless Personal Communications*, 118, 201–218. https://link.springer.com/article/10.1007/s11227-021-03825-1
- Hassija, V., Chamola, V., & Zeadally, S. (2021). Security issues in IoT: A comprehensive review. *Computer Communications*, 166, 1–28. https://www.sciencedirect.com/science/article/pii/S0169260721003059
- Iqbal, U., Akhtar, N., & Azad, M.A.K. (2023). Secure communication protocols for IoT: A survey of challenges and future directions. *Wireless Personal Communications*, 131(1), 45–69. https://www.sciencedirect.com/science/article/abs/pii/S0167404822000682
- Kumar, R., Sahu, B.K., & Sharma, S. (2024). An integrated cybersecurity framework for IoT: Research challenges and directions. *Sustainable Computing: Informatics and Systems*, 41, 100905. https://www.sciencedirect.com/science/article/pii/S2352864824000269
- Liang, X., Tang, H., & Zhang, Z. (2022). A comprehensive survey on firmware security in IoT. *Electronics*, 11(3), 494. https://www.mdpi.com/2079-9292/11/3/494
- Mohan, S., Kumar, P., & Tripathi, R. (2022). Trends in IoT attack surfaces: A security taxonomy. *SN Applied Sciences*, 4, 162. https://link.springer.com/article/10.1007/s42452-021-04156-9
- Rahman, A., & Islam, S. (2023). Privacy and security concerns in IoT: A regulatory perspective. *Computers & Security*, 120, 102852. https://www.sciencedirect.com/science/article/abs/pii/S0167404822000682
- Rehman, A., Akhtar, N., & Imran, M. (2021). AI-driven security in IoT: A survey of machine learning techniques. *Electronics*, 10(6), 719. https://www.mdpi.com/2079-9292/10/6/719
- Rizwan, M., Rehmani, M.H., & Erol-Kantarci, M. (2021). A review on side-channel attacks in IoT. *Electronics*, 11(1), 88. https://www.mdpi.com/2079-9292/12/1/88

- Shah, R., Rani, S., & Baek, J. (2021). Evaluation of OWASP IoT security recommendations. *Security and Privacy*, 4(1), e318. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.318
- Sharma, N., Tripathi, A., & Rawat, D. (2022). Architectural flaws in IoT: An empirical investigation. *ICT Express*, 8(3), 339–344. https://www.sciencedirect.com/science/article/pii/S254266052200107X
- Statista. (2023). Number of connected IoT devices worldwide 2019–2030. https://www.statista.com
- Yaqoob, I., Hashem, I.A.T., & Gani, A. (2021). Lightweight cryptography techniques for IoT: A survey. *Electronics*, 11(20), 3330. https://www.mdpi.com/2079-9292/11/20/3330
- Els-cdn.com. (2022). Available at: https://ars.els-cdn.com/content/image/1-s2.0-S254266052200107X-gr3_lrg.jpg
- Fereidouni, H., Fadeitcheva, O. and Zalai, M. (2025). IoT and Man-in-the-Middle Attacks. *SECURITY AND PRIVACY*, 8(2). doi: https://doi.org/10.1002/spy2.70016

- Bakhshi, T., Ghita, B. and Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors*, [online] 24(2), p.708. doi: https://doi.org/10.3390/s24020708
- Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, 9, pp.121975–121995. doi: https://doi.org/10.1109/access.2021.3109886
- Wang, L., Ali, Y., Nazir, S. and Niazi, M. (2020). ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods. *IEEE Access*, 8, pp.152316–152332. doi: https://doi.org/10.1109/access.2020.3017221
- Chiara, P.G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, 36(2), pp.1–20. doi: https://doi.org/10.1080/13600869.2022.2060468
- Varol, C. (2024). *Enhancing and Adapting Security Risk Assessment Strategies on Critical Infrastructure Utilizing IoT Devices using NIST Cybersecurity Framework 2.0*. [online] Tdl.org. Available at: https://shsu-ir.tdl.org/items/f0cf27e3-e27e-411b-8806-f602ea3be41d
- Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, 9, pp.121975–121995. doi: https://doi.org/10.1109/access.2021.3109886
- Krishna, R.R., Priyadarshini, A., Jha, A.V., Appasani, B., Srinivasulu, A. and Bizon, N. (2021). State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability*, [online] 13(16), p.9463. doi: https://doi.org/10.3390/su13169463
- Gerodimos, A., Maglaras, L., Ferrag, M.A., Ayres, N. and Kantzavelou, I. (2023). IoT: Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, [online] 3. doi: https://doi.org/10.1016/j.iotcps.2022.12.003
- Prasad, R. and Rohokale, V. (2019). Artificial Intelligence and Machine Learning in Cyber Security. *Springer Series in Wireless Technology*, pp.231–247. doi: https://doi.org/10.1007/978-3-030-31703-4_16
- Singh, I. and Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. *Measurement: Sensors*, 25, p.100591. doi: https://doi.org/10.1016/j.measen.2022.100591