Multidisciplinary Reviews

CONFERENCE PAPER
Published Online: April 27, 2024
https://doi.org/10.31893/multirev.2023ss063

Interdisciplinary Advances in Engineering, Science, and Technology

From protocols to countermeasures: A comprehensive survey into IoT safety

Jaimine Vaishnav[a] | **Ramachandran Thulasiram**[b] | **Ritesh Kumar**[c] | **Pratik Pandey**[d]

[a]ATLAS SkillTech University, Mumbai, Maharashtra, India, Department of ISME.
[b]JAIN (Deemed-to-be University), Ramanagara District, Karnataka, India, Department of Mechanical Engineering.
[c]Maharishi University of Information Technology, Lucknow, India, Maharishi School of Engineering and Technology.
[d]Vivekananda Global University, Jaipur, India, Department of Computer Science & Engineering.

Abstract The Internet of Things (IoT) has become a field with enormous potential, effect, and development with the emergence of smart cities, smart houses, and intelligent objects. Computer Information System Company (Cisco Inc). Projects that there will be 51 billion devices which are connected by 2021. However, the majority of those IoT gadgets are simple to alter and attack. These IoT devices are generally more susceptible to assaults than other types of endpoints such as desktops, mobile phones, or tablets because of their limitations in terms of storage, computing, and networking capability. The main IoT security concerns are presented and addressed in this study. Along with the methods utilized for connection, interaction, and administration, we examine and classify common security concerns about the IoT layers of architecture. In addition to the most recent assaults, challenges and innovative approaches, we describe the security necessities of the IoT. In addition, we connect and tabulate IoT safety problems with current literature-based remedies. Above all, we explore that blockchain technology, the software that powers Bitcoin, can play a major role in enabling the resolution of numerous IoT security issues. Difficulties along with unresolved research issues related to IoT security are also listed in this study.

Keywords: data security, IoT protocols, network security, IoT security, blockchain

1. Introduction

The IoT, which connects systems and gadgets to improve convenience and efficiency which is constantly expanding and changing our modern environment (Hassan et al 2020). However, there have become significant concerns about the safety and security of IoT ecosystems as a result of this exponential expansion (Abba Ari et al 2024). Data security, device honesty and user confidentiality are merely some of the issues that must be resolved to protect these networked systems (Rahmani et al 2022). Strong policies and countermeasures are critical to thwarting any vulnerabilities that can result in breaches of information, privacy violations or property damage (Guo et al 2021).

It is essential to use safe communication procedures, such as Message Queuing Telemetry Transport (MQTT) and Transport Layer Security (TLS), to encrypt data during transfer and ensure the privacy of data shared among equipment (Shammar and Zahary 2020). Device authorization, which uses techniques such as Public Key Infrastructure (PKI) and token-based identification to confirm the true nature of devices which is essential to avoid unwanted access (Kalaria et al 2021). Delivering security fixes on time requires regular firmware and software upgrades, made possible by Over-the-Air (OTA) protocols and code signatures (Ahmad et al 2021). Using filters and systems for intrusion detection (IDS) in conjunction with network segmentation methods such as VLANs helps segregate IoT devices from essential infrastructure, reducing the possible impact of security breaches (Haseeb et al 2020). Furthermore, protecting user data and enhancing confidentiality can be achieved by using end-to-end encryption and privacy by design (Haji et al 2020 and MohdAman et al 2021).

Physical security features that help to protect IoT ecosystems from tampering and unwanted access include tamper detection and secure boot with hardware-based protection (Ali et al 2020). A thorough approach that incorporates these procedures and countermeasures is necessary in this dynamic environment to successfully navigate the changing IoT safety problems (Pancaroglu and Sen 2021; Ju et al 2023). As technology develops, a safe and reliable IoT ecosystem must be sustained by implementing the latest security measures (Gaba et al 2020). The objective is Protocols to Countermeasures are pre-planned approaches that emphasize methodical reactions and security measures to reduce risks and guarantee resilience and protection (Ahmed 2022).

2. IoT design and security concerns

IoT devices, considering their small dimensions and computational constraints, give individuals direct accessibility to information and resources by connecting to the internet through gateways.

2.1. IoT standards and protocols

An organized infrastructure is shown in Figure 1, which illustrates the standard The IoT methods that are utilized for gadgets with hardware, software and communications, routing and redirection keys and identity (Garai et al 2022). The recent algorithms for "Low Rate Wireless Personal Area Networks (LR-WPANs) and low power wide-area-network (LPWANs)" are also included, along with their corresponding specifications.

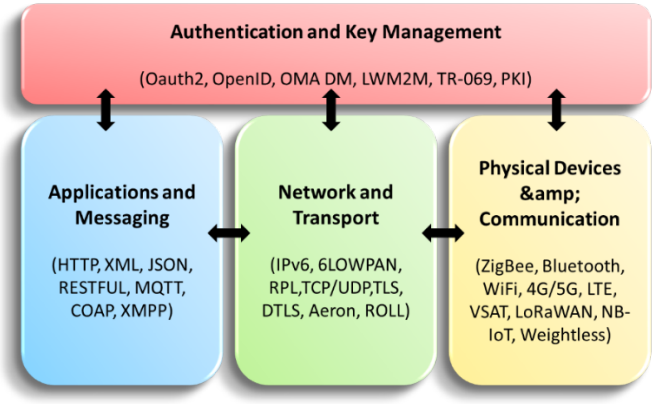

Figure 1 Standardized IoT protocols and standards.

According to the "IEEE specification 802.15.4, LR-WPANs has two low-level portions: the Physical Layer and the Medium Access Control (MAC) layer". For transportable networks to function properly, bandwidth adjustments and data transfer speeds must be made at the network layer. The MAC layer specifications cover access to channels and synchronization methods. The moderate minimum transmissions unit (MTU) specified by IEEE requires the addition of an IPv6 adaptation layer across the connection layer to improve the sensor node's ability to communicate across Low-Power Wireless Personal Area Network (6LoWPAN). A distinct IPv6 network address is assigned to each single IoT device. It is possible to implement 6LoWPAN settings by utilizing the Routing Protocol for Low-Power and Lossy Networks (RPL) (Patel and Shah 2020). The RPL standard allows for both one-way and two-way interaction, as well as point-to-point traffic.

Applications built for the IoT use "User Datagram Protocol (UDP)" for communication instead of "Transmission Control Protocol (TCP)" because of the smaller payload (SRHIR et al 2023). UDP is simpler and more efficient. On top of that, to make better use of the restricted payload capacity, it is possible to compress the UDP header. "6LoWPAN uses the Internet Control Message Protocol (ICMP)" for messages that control these neighborhood identification and inaccessible destination specifications. The "constrained Application Protocol (CoAP)" offers a design for small appliances that are request-response oriented but influenced systems that are present in limited environments (Li et al 2021). The CoAP protocol allows for the asynchronous transmission of messages and the provision of HTTP mapping for the access of IoT resources through HTTP.

The IoT devices can communicate over long distances according to the LPWAN. It enables devices with limited power to communicate, compared to a portable WAN, which needs a bigger battery to operate an increased bit-rate at a lower bit-rate. In a system of battery-powered things, LPWAN supports different data speeds through the application of LoRaWAN protocols for gateway-to-end product connectivity (Alhaidari and Alqahtani 2020). In addition, NB-IoT is a 3GPP innovation that uses LTE frequencies to provide coverage inside and enable LPWAN connectivity. To accommodate low-power, bidirectional, and unidirectional LPWAN interactions, the Weightless protocol employs three distinct standards.

2.2. Needs for IoT Security

Several factors and mechanisms, detailed below, itmust be considered for an IoT implementation to be secure.

2.2.1 Integrity, data privacy and confidentiality

Data confidentiality is crucial in the IoT, as it requires multiple network connections. Privacy can be compromised by infiltrating networks, devices, and malicious parties altering stored information.

2.2.2. Accounting, Authentication, and Authorization

Authentication is crucial for secure IoT communication, requiring device identification before accessing protected functions. Developing a used system for authentication is challenging in heterogeneous settings. Authorization procedures

ensure authorized access, and a reliable setting ensures safe communication through resource utilization, auditing, and monitoring.

2.2.3. Service accessibility

Denial-of-service attacks targeting IoT devices can undermine the quality of service (QoS) provided to customers, using methods like replay assaults, sinkhole assaults, and jamming opponents.

2.2.4. Energy-related effectiveness

IoT devices, with limited resources and storage, can be vulnerable to attacks that increase energy consumption by flooding the internet with pointless or fraudulent applications.

2.3. Singular sources of failures

The explosion of different networks for IoT infrastructure could lead to a large number of weak points that could compromise the IoT's essential functions. It is imperative to develop an appropriate environment for an extensive amount of IoT devices and provide failsafe alternatives for network establishment

3. Sorting security challenges into categories

It is essential to handle safety issues at multiple levels due to the wide range of gadgets and machinery that are part of the Internet of Things paradigm, ranging from enormous high-end servers to tiny embedded systems chips. A classification of IoT security issues is shown in Figure 2, which includes hyperlinks to articles addressing each issue. In light of the IoT deployment methodology described below, we assess potential safety risks.

Figure 2 An index of security-related materials and topics. High-level security-related concerns; Intermediate-level security-related concerns; Low-level security-related concerns

4. Solutions for IoT security

IoT security challenges involve faults in various parts, including hardware, software, network parts, applications and physical equipment. Countermeasures target flaws at various stages, but are complex due to various protocols. This study explores popular security methods from recent literature.

4.1. Low-level security countermeasures

In sensing networks with wireless connections, deliberate interference that results in message collisions or channel floods is known as jamming (Bout et al 2020). Among the techniques used for detection are statistics comparisons with personalized threshold values, signal strength monitoring, and noise-like signal extraction. A different approach measures the proportion of packets that have been delivered effectively and verifies the consistency of node positions and signal quality (Yan et al 2023).

Cryptographic characteristics, error correction coding, channel surfing (moving between frequencies), and geographical getaways (shifting position) are some techniques to stop interruption (Mendez Mena 2021). A suggested architecture adds fake noise to signals, establishes a minimum data rate to prevent absorbing to, and improves the safety of IoT devices during installation. Intentional nodes use fake MAC values in Sybil attacks to trick and drain resources (Dogan-Tusha et al 2023). Signal strength measurements and the deployment of detector nodes to determine the sender's position during the communication are examples of detection techniques (Tomic and Beko 2022). The method is predicated on being appropriate for stable networking. Other approaches analyze signal intensity to identify MAC address-based impersonating operations or utilize estimation of channels to identify Sybil assaults (Shrivastava et al 2021). Physically unsafe devices have vulnerable utilities and interfaces to the outside. According to Ferrara et al 2021 instructions, equipment-based solutions including Trusted Platform Modules should be used, testing tools should be turned off, and extraneous hardware connections should be avoided. By breaking up clusters, minimizing communication over long distances to save energy, and utilizing a 5-layer system for the detection of intrusions, a structure fights sleep deprivation attacks (Mishra and Paul 2020). For improved security, detection systems for intrusions are incorporated into cluster managers and nodes at various layers.

4.2. Intermediate-level security countermeasures

The integration of timestamp and nonce options into cracked packets is how 6LoWPAN combats replay assaults resulting from packet segmentation (Rudra et al 2020). Timestamp choices are essential for unidirectional packets, whereas nonce variables safeguard bi-directional transmissions (Lenders et al 2021). Marketing materials only react to recent queries according to nonce, and a 64-bit timestamp eliminates pointless ads and redirection (Prathapchandran et al 2021). Sequential IPv6 packet transmission is ensured by content chaining, and the procedure is authenticated by fragment contents. Encrypting data, key development, authentication, and reliable neighbour identification are covered by the safety framework (Lenders et al 2021). Secure neighbourhood identification can be accomplished with the use of "Elliptic Curve Cryptography (ECC)". Nodes are identified during neighbourhood identification by ECC available signatures.

There are security concerns with the IPv6 “Routing Protocol for Low-Power and Lossy Networks (RPL)”. By employing MAC and hashing algorithms to authenticate versions and rank numerals, “Version Number and Rank Authentication (VeRA)” protects against hostile efforts. Directional Acyclic Graphs (DAGs) are shielded from unwanted nodes by defenses against attacks that manipulate node rankings (Garai et al 2022). Integrated authentication and failover are necessary to prevent sinkhole attacks in low-power lossy networking. Protection is improved by multilayered wireless networks of sensors, neighborbehavior evaluation, and dynamic source routing (DSR) trust levels.“Encapsulating Security Payload (ESP) and Compressed Authentication Header (AH)” secure communications for IPv6 networks utilizing 6LoWPAN. Security in IoT applications for Smart Cities is addressed by initiatives like BUTLER, ARMOUR, and RERUM. Transport-level end-to-end security suggests techniques for header reduction. 6LoWPAN key administration is handled using compacted IKEv2, and end-to-end HTTP-CoAP confidentiality is provided by TLS-PSK (Challa and Rao 2022). New approaches defend against Sybil and sinkhole attacks, and secure communication structures strengthen the reliability, privacy and dependability of Internet of Things systems. To summarize, a variety of methods like as cryptography, authentication and encryption are used to safeguard low-power lossy networks (Shrivastava et al 2021). Research is done to address new threats and make sure IoT systems are reliable.

4.3. High-level security countermeasures

The proposed security methods for internet-connected “CoAP-based Low-power and Lossy Networks (LLNs)” protect against various threats. Integrating TLS and DTLS provides end-to-end security for LLNs against internet threats (Omar et al 2022). The computation cost for mapping “Transport layers security (TLS)” and DTLS on resource-constrained devices may be difficult. Another way addsSecurityOn, SecurityToken, and SecurityEncap to CoAP. SecurityOn secures CoAP communications at the application level, SecurityToken identifies and authorizes, and SecurityEncap transmits data for authentication and replay protection using Advanced Encryption Standard (AES)(Gupta et al 2021). Security models for IoT on IP networks use 6LBRs for message filtration and TLS-“Datagram Transport Level Security (DTLS)” tunnels for endwise security. The energy-

efficient solution uses a “Mirror Proxy (MP) and Resource Directory” for server representation and public key cryptography for data update authentication (Wang et al 2022). (Ferrara et al 2021) suggests discouraging weak passwords, checking interfaces for vulnerabilities, using HTTPS, and updating software to secure IoT. TLS and SASL authentication and encryption in VIRTUS middleware ensure data integrity and authorized user access (Prathapchandran et al 2021). A semantic framework uses Triple Space Computing to ensure diverse implementation interactions. An AAA-enabled middleware server filters data in heterogeneous IoT environments and uses a web portal for service access. Various security architectures recommend AES encryption, safe message exchange, and open authentication for IoT connectivity (Sanders and Yau 2021). These ideas strengthen LLN and IoT ecosystem security against various threats and weaknesses.

5. Blockchain solutions for IoT security

Industry and research anticipate blockchain technology to significantly impact IoT device management, control, and security. The use of blockchain-based technologies to provide efficient security remedies for current IoT security issues is examined in this part (Manaserh 2020). In addition to discussing open IoT security issues that a blockchain may be able to solve, this part explains blockchain technology. We also review the research on blockchain-based fixes for security vulnerabilities in the IoT.

5.1. Background

Asset and transaction data is maintained on a peer-to-peer network via a decentralized blockchain. Data authenticity and integrity are established using elliptic curve cryptography using SHA-256 processing. A digital representation of the preceding block and transaction information is included in every timestamped and verified network block. Eliminating the need for central control or Verified Third Parties, miners ensure confidentiality by using minority decisions to verify operations in an accessible database. Miners validate Bitcoin blocks using a proof-of-work process, generating an immutable record after consensus. Privacy and access control differ with permissioned (private) or permission-less (public) blockchains. Blockchains have a block header including version number, timestamp, block size, and transaction count. The specifics of the transaction are contained in the block's body, while the current block hashing value is included in the Merkle root field (Daneel and Hoff 2020).

The proof-of-work algorithm's nonce field modifies difficulty goals to preserve blocktimes. Ethereum developed smart contracts, making Bitcoin and Ethereum popular blockchain applications. Smart contracts, implemented on Ethereum Virtual Machines (EVM), define contract terms. Ethereum executes smart contracts using a blockchain state and Ether. Smart contracts have accounts, addresses, executable code and Ether balances. Ethereum'sblockchain state saves big amounts, although BitTorrent or IPFS can be used. Smart contracts are used in cryptocurrencies, trading, supply chains, autonomous transactions, and digital identification (Mighan et al 2022). New blockchain platforms like Hyperledger, Eris, Stellar, Ripple, and Tendermint have expanded their application cases. SafeShare offers bitcoin blockchain insurance, and IBM's Hyperledger Fabric platform is used in banks, supply chains, and freight shipping without cryptocurrency. Blockchain's widespread use shows its potential to disrupt many industries.A Blockchain's typical design structure is shown in Figure 3.

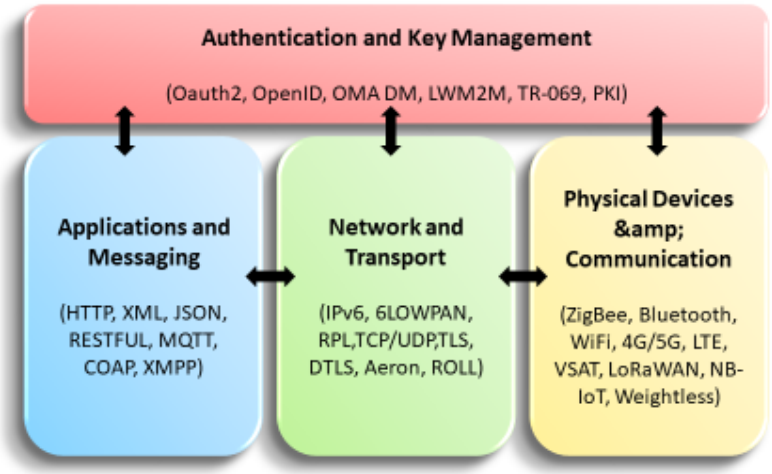

Figure 3 Blockchain design structure.

5.2. Possible Blockchain Solutions

This article highlights the importance of blockchain technology, particularly smart contracts, in IoT device administration, control, security, address space, identity management, data authentication, secure communications, and governance benefits.

5.2.1. Addressing Field

The "Elliptic Curve Digital Signature Algorithm" generates an address field of one sixty bits for network authentication, reducing identity conflicts and improving IoT adaptability by providing 4.2 billion addresses more than IPv6 and eliminating the need for an IANA.

5.2.2. Governance and Identity of Things (IDoT)

IoT problems include managing ownership changes and device interactions. Blockchain provides surveillance, responsibility observing, and reliable identification verification to address these issues. Trust Chain uses blockchain to provide distributed integrity. Blockchain's decentralized management, governance, and tracking of IoT devices' supply chains and lifecycles ensures transparency and reliability. IoT devices connected to the blockchain network ensure data authenticity and integrity by cryptographically proofing and signing data by the real sender. Blockchain ledgers securely and transparently record all transactions (Shrivastava et al 2021). This fundamental architecture boosts IoT ecosystem security. Compared to more traditional methods such as "Role Based Access Management (RBAC) or OAuth 2.0", managing access is made simpler by the decentralized authorization and authentication regulations established by blockchain smart contracts. Conventional agreements include conditions, time limitations, and accessibility guidelines for ownership of information and administration while safeguarding confidentiality. Rights for software or hardware upgrades, IoT device resets, keypair provisioning, and ownership changes are specified. Traditional IoT protocols lack inherent security, necessitating DTLS or TLS layers for secure connection. By giving IoT devices unique GUIDs and asymmetric key pairs, blockchain replaces these complicated protocols. This simplification minimizes computational and memory requirements, making lightweight IoT security methods possible. Blockchain offers reliable distributed organization, surveillance, and management at every point in an IoT device's lifecycle throughout the supply route, as illustrated in Figure 4.

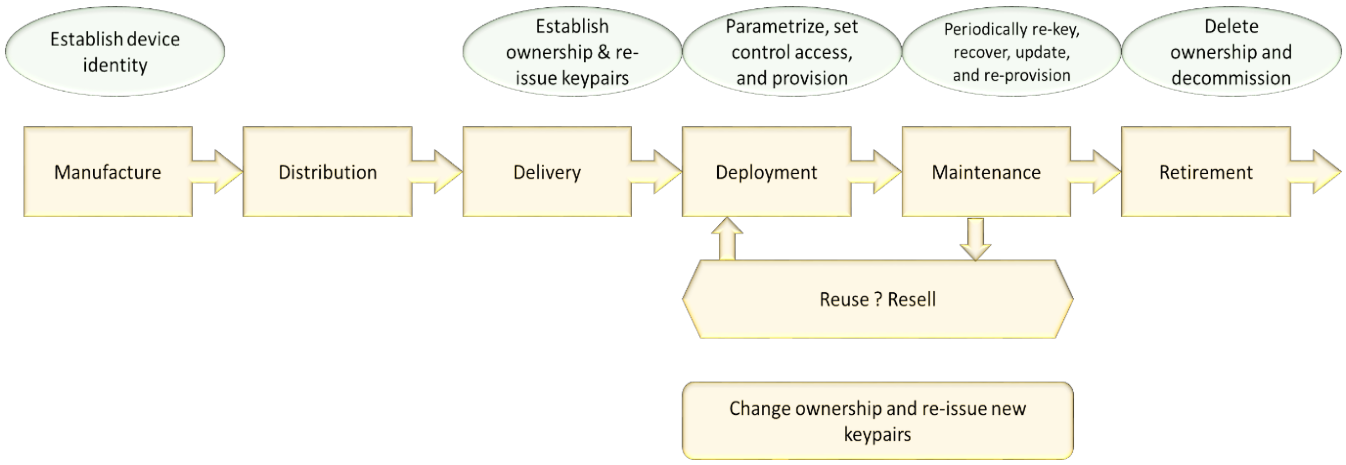

Figure 4 Lifecycle security administration for IoT devices.

5.3. Work on Blockchain and IoT

The research on blockchain and IoT security focuses on improving IoT functioning through 18 application cases, including four IoT-specific ones. Blockchain can address issues like ownership, authentication, authorization, governance, and privacy (Kumar et al 2020). It can also facilitate communication between IIoT devices, the cloud, and the blockchain network. Blockchain networks can aid IoT in billing, e-trade, shipping, supply chain management, and energy trading (Alam 2021). Smart contracts and IoT asset tracking can enhance IoT security, functionality, and efficiency.

6. Constraints and research directions

The challenges of securing Internet of Things devices are covered in this section.

6.1. Resource constraints

IoT's resource constraints make difficult to provide a reliable security system. To implement effective protocols, energy efficiency and lightweight procedures must be improved, while enhancing energy harvesting systems.

6.2. Distinctive apparatuses

The implementation of a multi-layer security structure is necessary for diverse equipment, which can range from powerful servers to tiny, low-power electronics with monitors. Whenever the services are offered to end users, the structure

must adjust to the assets that are available. It should decide the security techniques to utilize the IoT tiers. The analysis needed for an adaptive security system depends on a standardized set of resources that must be used in IoT designs.

6.3. Protocol compatibility for protection

The international IoT security framework requires collaboration between protocols at different layers to standardize safety requirements at each level using structural restrictions assessment.

6.4. Singular sources of failures

IoT's heterogeneous systems increase failure risk, necessitating further research to ensure component availability for essential applications. Implementing standards and processes can provide redundancy while balancing costs and infrastructure dependability.

6.5. Weaknesses in software and hardware

Low-cost and low-power devices increase vulnerability to hardware defects in IoT design. Confirming security techniques in equipment, navigation, and packet handling is crucial for preventing and fixing vulnerabilities post-deployment.

6.6. Dependable management and upgrades

The research on secure software administration for IoT devices is a major unresolved issue, with concerns about governance, data privacy, and scaling. Blockchain-based technology could help, but challenges include scaling, effectiveness, and key collisions.

6.7. Weaknesses in blockchain

Blockchain technologies, despite their robust IoT security, are vulnerable to attacks (Wang et al 2022). Hackers can compromise consensus systems and internet credentials, necessitating the development of effective methods to secure transactional confidentiality and prevent race assaults.

7. Final considerations

This study examines the security concerns of IoT devices, focusing on middle, high, and low-level layers. It provides the main security concerns, groups them according to the IoT tiers, and outlines suggested scholarly approaches. A presentation of a parametric analysis of IoT threats and security mechanisms is provided, with a focus on possible links to blockchain solutions. To create dependable and easily accessible IoT security solutions, researchers need to concentrate on these obstacles and address both known problems and open research topics to create a global strategy. In the future, the scope will involve developing IoT device capabilities for increased security, setting international standards, and encouraging the creation of safe equipment.

Ethical Considerations

Not Applicable.

Conflict of Interest

The authors declare no conflict of interest.

Funding

The current review did not receive any financial support.

References

Abba Ari, A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Mohamadou, A. & Gueroui, A.M., (2024). Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, 20(1/2), 119-141.

Ahmad T, & Zhang D, (2021). Using the Internet of things in smart energy systems and networks. *Sustainable Cities and Society,* 68, 102783.https://doi.org/10.1016/j.scs.2021.102783

Ahmed N, (2022) March. MPaS: A micro-services-based publish/subscribe middleware system model for IoT. *In 2022 5th Conference on Cloud and Internet of Things (CIoT)*, 220-225. IEEE. 10.1109/CIoT53061.2022.9766670

Alam T, (2021) IBchain: Internet of things and blockchain integration approach for secure communication in smart cities. *Informatica,* 45(3). 10.31449/inf.v45i3.3573

Alhaidari FA, & Alqahtani EJ, (2020). Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey. *J. Commun,* 15, 14-30.

Ali M, Nadeem M, Siddique A, Ahmad S & Ijaz A, (2020). Addressing Sinkhole Attacks in Wireless Sensor Networks—A Review. *Int J Sci. Technol Res (IJSTR),* 9, 406-411.

Bout E, Loscri V. & Gallais A, (2020 September). Energy and Distance evaluation for Jamming Attacks in wireless networks. *In 2020 IEEE/ACM 24thInternational Symposium on Distributed Simulation and Real-Time Applications (DS-RT),* 1-5. IEEE.https://doi.org/10.1109/DS-RT50469.2020.9213652

Challa R, & Rao KS, (2022) Resource-Based Attacks Security Using RPL Protocol in Internet of Things. *Ingenierie des Systemesd'Information*, 27, 165.

Daneel S, & Hoff, B., (2020). Blockchain and Distributed Ledger Technologies.

Dogan-Tusha S, Althunibat S, & Qaraqe M, (2023). Doppler Shift-based Sybil Attack Detection for Mobile IoT Networks. *IEEE Internet of Things Journal.* 10.1109/JIOT.2023.3288040

Ferrara P, Mandal AK, Cortesi A & Spoto F, (2021). Static analysis for discovering IoT vulnerabilities*. International Journal on Software Tools for Technology Transfer,* 23, 71-88. https://doi.org/10.1007/s10009-020-00592-x

Gaba GS, Kumar G, Monga H, Kim TH & Kumar P, (2020). Robust and lightweight mutual authentication scheme in distributed smart environments. *IEEE Access,* 8, 69722-69733.https://doi.org/10.1109/ACCESS.2020.2986480

Garai A, Sen S & Chandra P, (2022). IOT Securities: A Review. AJEC.

Guo Q, Xie H, Li Y, Ma W, & Zhang C, (2021). Social bots detection via fusing bert and graph convolutional networks. *Symmetry* 14, 30.https://doi.org/10.3390/sym14010030

Gupta M, Jain S & Patel RB, (2021). Security issues in the Internet of Things Principles challenges taxonomy. *In Recent Innovations in Computing Proceedings of ICRIC* 2020, 651-667. Springer Singapore.https://doi.org/10.1007/978-981-15-8297-4_52

Haji LM, Ahmad OM, Zeebaree SR, Dino HI, Zebari RR & Shukur HM, (2020). Impact of Cloud computing and the internet of things on the future internet. *Technology Reports of Kansai University*, 62, 2179-2190.

Haseeb K, Almogren A, Ud Din I, Islam N & Altameem A, (2020). SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. *Sensors*, 20(9), 2468.https://doi.org/10.3390/s20092468

Hassan R, Qamar F, Hasan MK, Aman AHM & Ahmed AS, (2020). Internet of Things and its applications. *A comprehensivesurvey. Symmetry*, 12,10, 1674.https://doi.org/10.3390/sym12101674

Ju Y, Liu W, Yang, M, Liu L, Pei Q, Zhang N, Ota K, Dong M & Leung VC, (2023). Physical Layer Security in Full-Duplex Millimeter Wave Communication Systems. *IEEE Transactions on Vehicular Technology*.https://doi.org/10.1109/TVT.2023.3320907

Kalaria R, Kayes ASM, Rahayu W & Pardede E, (2021). A Secure Mutual authentication approach to fog computing environment. *Computers & security*, 111, 102483.https://doi.org/10.1016/j.cose.2021.102483

Kumar T, Harjula E, Ejaz M, Manzoor A, Porambage P, Ahmad I, Liyanage M, Braeken A & Ylianttila M, (2020). BlockEdge: blockchain-edge framework for industrial IoT networks. *IEEE Access,* 8, 154166-154185.https://doi.org/10.1109/ACCESS.2020.3017891

Lenders MS, Schmidt TC, & Wählisch M, (2021). Fragment forwarding in lossy networks. *IEEE Access,* 9, 143969 143987.https://doi.org/10.1109/ACCESS.2021.3121557

Li X, Liu B, Zheng X, Duan H, Li Q & Huang Y (2021) June. Fast IPv6 network periphery discovery and security implications. *In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),* 88-100. IEEE.https://doi.org/10.1109/DSN48987.2021.00025

Manaserh AAS, (2020). A Relationship Between Bitcoin And Foreign Exchange Rates: A Quantitative Research On Bitcoin,And Selected Foreign Exchanges. *YayımlanmamışYüksekLisansTezi)*. İstanbul Aydın Üniversitesi, İstanbul.

Mendez Mena DM, (2021). Blockchain-based security framework for the Internet of things and home networks (Doctoral dissertation, Purdue University Graduate School).

Mighan SN, Mišić J & Mišić VB, (2022), December On block delivery time in Ethereum network. *In GLOBECOM 2022-2022 IEEE Global Communications Conference*, 2867-2872. 10.1109/GLOBECOM48099.2022.10001081

Mishra S, & Paul A, (2020) October. A critical analysis of attack detection schemes in IoT and open challenges. *In 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON),* 57-62. IEEE.https://doi.org/10.1109/GUCON48875.2020.9231077

MohdAman AH, Shaari N & Ibrahim R, (2021). Internet of Things energy system: Smart applications technologyadvancement and open issues*. International Journal of Energy Research,* 45, 8389-8419.https://doi.org/10.1002/er.6451

Omar YA & Goyal SB, (2022). Blockchain for Enhancing Security of IoT Devices. *In Internet of Things: Security and Privacy in Cyberspace,* 235-270. Singapore: Springer Nature Singapore.https://doi.org/10.1007/978-981-19-1585-7_11

Pancaroglu, D. & Sen, S., (2021). Load balancing for RPL-based Internet of Things: A review. *Ad Hoc Networks,* 116, 102491.https://doi.org/10.1016/j.adhoc.2021.102491

Patel BH & Shah P, (2020). RPL routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation. *TELKOMNIKA (Telecommunication Computing Electronics and Control),* 18, 1849-1856. 10.12928/telkomnika.v18i4.15768

Prathapchandran K. & Rutravigneshwaran P, (2021 May). Trust Based Security Mechanisms for Resource-Constrained Internet of Things-A Review. *In Journal of Physics: Conference Series,* 1850(1), 012042. IOP Publishing.DOI 10.1088/1742-6596/1850/1/012042

Rahmani AM, Bayramov S. & KianiKalejahi B, (2022). Internet of Things applications: opportunities and threats. *WirelessPersonal Communications*, 122, 451-476. 10.1007/s11277-021-08907-0

Rudra B, (2020). Impact of Blockchain on Internet of Things Security. *Cryptocurrencies and Blockchain Technology Applications*, 99, 127. 10.1002/9781119621201.ch6

Sanders K & Yau S S (2021 December) An Effective Approach to Protecting Low-Power and Lossy IoT Networks Against Blackhole Attacks. I*n 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, 65-72. 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00025

Shammar EA & Zahary AT, (2020). The Internet of Things (IoT). a survey of techniques operating systems and trends*. Library Hi Tech*, 38, 5-66.10.1108/LHT-12-2018-0200

Shrivastava R, Tiwary A. & Yadav P, (2021), January. Challenges Block Chain Technology Using IOT for Improving Personal and Physical Safety-Review. *In 2021 International Conference on Advances in Technology, Management & Education (ICATME),* 238-243. IEEE. 10.1109/ICATME50232.2021.9732730

SRHIR A, MAZRI T & BENBRAHIM M, (2023). Security in the IoT: State-of-the-art issues solutions and challenges. *International Journal of Advanced Computer Science and Applications.* 14.DOI: 10.14569/IJACSA.2023.0140507

Tomic S & Beko M, (2022) Detecting Distance-Spoofing Attacks in Arbitrarily-Deployed Wireless Networks. *IEEE Transactions on Vehicular Technology,* 71(4), 4383-4395. 10.1109/TVT.2022.3148199

Wang T, Hua H, Wei Z & Cao J, (2022). Challenges of blockchain in new generation energy systems and future outlooks. *International Journal of Electrical Power & Energy Systems,* 135, 107499. 10.1016/j.ijepes.2021.107499

Yan B, Yao P, Yang T, Zhou B & Yang Q, (2023). Game-Theoretical Model for Dynamic Defense Resource Allocation in Cyber-Physical Poer Systems under Distributed Denial of Service Attacks. *Journal of Modern Power Systems and Clean Energy.* 10.35833/MPCE.2022.000524