j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions

Zaid A. Alsarray *[1], Sanaa Ahmed Kadhim[2]

[1&2] *College of Biomedical Informatics, University of Information Technology and Communications, Baghdad, Iraq.*

zaid.ali-bmic@uoitc.edu.iq

Abstract The Internet of Things (IoT) has become a transformational strength in various fields, including health services, production and urban infrastructure. Although it enables automation and data exchange in real time, it also introduces sufficient risks that cannot be ignored. This article makes a comprehensive review of existing literature to detect the most pressure related challenges associated with IoT, including security weaknesses, privacy considerations, inter -Boundaries and questions of stability. This emphasizes how the growing number interacted equipment expands the surface of the cyber-attacks, often increased by old firmware, weak encryption and incompatible standards. In response, recent research has suggested integration of blockchain, artificial intelligence and slightly cryptography as a possible solution. However, practical purposes are interrupted by the lack of energy and scalable, the requirement for adaptive structure. The study also emphasized the role of new technologies such as edge calculation and 5G to remove delay and reliability problems. In addition, the data protection and generation -related moral and regulatory complications discuss. By synthesizing insights from recent studies, the paper suggests future research directions, aimed at developing energy networks, safe and standardized IoT ecosystem.

Crossref 10.36371/port.2025.4.5

Keywords: *Internet of Things, Cybersecurity, Interoperability, Edge Computing, Data Privacy, Blockchain, Energy Efficiency, Machine Learning*

1. INTRODUCTION

The Internet of Things (IoT) is defined as a system of interconnected devices that communicate and share information through internet-based platforms. This connectivity improves automation and streamlines various everyday functions. IoT technology involves embedding sensors and software into common objects, allowing them to function independently and transmit real-time data for analysis and informed decision-making. Its importance in modern life is evident in multiple dimensions, as IoT applications range widely from smart home devices to wearable health monitors—all seamlessly connected via the internet.(Jose J et al., 2024; Weber & Weber, 2016). The Internet of Things (IoT) is an emergent technology perceived to have a huge influence on numerous domains such as healthcare, industrialization or smart city. IoT facilitates device-device communication, leading to better efficiency, productivity and experience. This article provides an overview of the impact of IoT on these sectors, addressing its advantages and challenges. With the help of IoT, real-time monitoring of patients are done using wearables leading to better care and proactive medication.(Adeoye & Adams, 2024; Patel et al., 2024) In addition, devices connected to the Internet of Things networks enhance disease management and patient engagement. (Ahluwalia et al., 2024). Moreover, the Internet of Things plays a crucial role in the industry as the Internet of Things improves manufacturing processes, reducing downtime and enhancing supply chain efficiency. (Kamble & Kulkarni, 2024; Patel et al., 2024). And cost reduction by streamlining operations, industries can achieve significant cost savings (Ahluwalia et al., 2024). In addition smart cities' IoT come with the role of a Resource Management: IoT applications for traffic, energy and water concerns are managing resources and energy for the planification and management of cities in a sustainable way. (Kamble & Kulkarni, 2024). Also with real-time data analytics helps cities to efficiently serve their citizens this will improved public services. (Ahluwalia et al., 2024) Considering security concerns, the interconnected nature of smart city technologies raises significant cybersecurity issues. (Kamble & Kulkarni, 2024). The security risks associated with the Internet of Things (IoT) are numerous, stemming from the rapid proliferation of connected devices and their inherent vulnerabilities. With the growing importance of IoT applications across many sectors, including healthcare and transportation, the need for robust security features is paramount. IoT systems face significant threats due to their heterogeneous nature, insufficient security measures, and vulnerability to cyberattacks. (Ntayagabiri et al., 2024). IoT architecture has security risks present at all levels including physical components through to applications which demand specific security approaches.(Richa, 2021). Also the protection of sensitive data requires effective management because breaches result in significant privacy violations(Sebestyen et al., 2024). IoT security strategies encompass a wide array of methodologies that continuously develop in response to the specific challenges created by the

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

expansion of connected devices. Security strategies now combine multiple protection methods with resource optimization and artificial intelligence technology to enhance defense mechanisms. Intrusion Detection Systems (IDS) are designed to detect suspicious network activities and generate immediate alerts alongside responses to potential threats(Szymoniak et al., 2025). Anomaly Detection systems that employ machine learning techniques detect abnormal patterns which strengthen threat detection functionalities.(Said et al., 2024). Moreover secure authentication of devices is essential to block unauthorized access and maintain network communication for only legitimate devices.(Ntayagabiri et al., 2024). Resource Optimization Strategies form an essential aspect of IoT security by employing Lightweight Cryptographic Algorithms which deliver strong protection while conserving resources for devices with limited processing power alongside Adaptive Security Mechanisms which modify security protocols according to operational context and available resources to maintain effective protection and performance.(Rozlomii et al., 2025). In addition, AI technology, including deep learning and machine learning, is used to detect deviations and predict weaknesses, by improving the safety currency of the IoT system significantly, blockage technology is also used, where this technology is detected to ensure identification management and secure data integrity on the IoT. (Said et al., 2024; Sebestyen et al., 2024) . Internet of Things (IoT) presents several research intervals and future instructions in various domains, including health services, industrial applications and cyber security. It is important to identify these intervals to promote IoT technologies and ensure their effective implementation. The following sections designed main areas for future research. The first differences are interoperability problems: Lack of standardized contours in IoT, especially in the Industrial Internet of Things (IIOT), prevents uninterrupted integration and communication between equipment (Cuozzo et al., 2024). In addition to cyber security weaknesses, where current fazing techniques for the IoT system are inadequate, firmware and hardware must develop new methods for addressing weaknesses.(Touqir & Haas, 2024). Morever, privacy and data protection are where the Internet of Medical Things (IOMT) faces important challenges with patient data person protection, which requires advanced cryptographic solutions and blockage chain technology.(Al Khatib et al., 2024)

2. REVIEW of PREVIOUS STUDIES

The fast growing Internet of Things (IoT) has created remarkable advancements to a variety of industries. With these improvements, there are given concomitant dangers, questions, and risks that need serious scrutiny. This chapter presents an organized analysis of literature on confined risks and challenge of IoT and Gap analysis of IoT Risk and Challenges with Security, Privacy, Interoperability, Scalability, Regulations, and Sustainability as key dimensions. The goal is to discern trends in existing studies, bring forth challenges, and provide recommendations for further investigation.

2.1 Security and Privacy Risks

IoT systems process vast sensitive data, exposing them to privacy breaches and cyber threats due to weak encryption and unauthorized access. Bhamare et al. (2024) stand out by proposing block chain and machine learning integration, which provides critical multi-layered security to defend against evolving threats.(Bhamare et al., 2024). IoT systems are experiencing significant risks in respect to privacy and security specifically that of securing sensitive healthcare and industrial data from breaches. Patel et al., (2024) offered a series of solutions such as block chain for secure data exchanges, as well as, analytics to collect predictive threat analysis derived from artificial intelligence to improve data integrity and proactive protection in IoT environments. (Patel et al., 2024). Default passwords and firmware that have not been updated put IoT devices at serious risk of being exploited for malware attacks. A critical example is malware, the Mirai botnet as Mirai, as explained in the paper, exploits Internet of Things devices, using a botnet to execute large scale distributed denial of service (DDos) attacks,. Owed to several risk factors in the IoT ecosystem, the paper recommends several security measures for mitigating Internet of Things scanners and their use for botnet activites, such as using strong passwords and routinely updating the current firmware installed. Overall, additional methods of defence was offered for IoT attack risk, including the configuration of traffic filters and disabling telnet services by closing TCP 23. Collectively, they discussed methods to mitigate risks associated with IoT exploitation, which should appear to be effective for preventing device from hijacking for use in botnets.(Pravylo & Averkiiev, 2024).

Various methods for identifying and protecting against botnet attacks have been suggested, including machine learning-based approaches and suggested better secure practices. Using the IoT-POT dataset, machine learning models including K-Nearest Neighbor, Logistic Regression, Decision Tree and Random Forest can detect Mirai botnet activity by looking at patterns in the network traffic.(Sharma & Babbar, 2024). Besides that Catboost, an implementation of a gradient-boosting algorithm, performed optimally in detecting botnet attacks, achieving an accuracy rate of 99.49% relative to alternative methods such as SVM and Logistic Regression.(Rasheed & Alnabhan, 2024).Weak-encryption standards grossly risk data confidentiality in the Internet of Things (IoT) by exposing sensitive information to unauthorized access and modification. Lightweight Security Algorithm (LSA) proposed the encryption algorithm that protects WSN security in IoT and consumes very little power to complete. It achieves 99% security using a mere five rounds of encryption.(Mahlake et al., 2023). Similarly, deficiencies in the execution of lightweight encryption standards can inadvertently create access flaws, which expose to systematic attacks.(Aljaafari et al., 2021). Consequently, applying highly secure encryption algorithms like Twofish provides a level of security vital for protecting data confidentiality and integrity with respect to transmission.(N et al., 2023). Also, Lightweight

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

cryptographic solutions may be designed for constrained devices while giving appropriate consideration to security requirements and performance requirements.(Garah et al., 2023).

According to(Bonaventura et al., 2024) exploitation of non-calibrated IoT devices such as Tapo smart bulbs and plugs can lead to acquisition of personal credentials including user emails and network passwords. This provided attackers with access to the complete IoT ecosystem for that residence. These exploitable flaws were acknowledged by implementing a process of firmware updates, TLS encryption, and secure configuration channels like Bluetooth. (Vojković et al., 2020) indicate smart homes, which rely on IoT technology, are susceptible to breaches that can expose personal data, such as household habits, to unauthorized third parties without user consent so, they advocate for amendments to current legislation and greater user awareness as key mitigation approaches. A review of previous cyberattacks on IoT networks show that many of these breaches happened due to poor security. Lee highlights that layered defenses such as whitelisting, data diodes, device authentication, and automated updates can help alleviate these threats. (Lee, 2023). The cases mentioned above demonstrate the complexity and severity of risks associated with IoT systems, it is essential to also point out the recent development in security technologies, including blockchain and machine learning, which may greatly assist in reducing these risks.(Sahu & Mazumdar, 2024).

2.2 Interoperability and Standardization Issues

The lack of a unified protocol for conversation among IoT devices presents substantial demanding situations in reaching interoperability and seamless integration across various systems. Benomar et al proposes a gateway-primarily based gadget integrating Stack4Things and DeXMS to evolve diverse protocols into RESTful HTTP offerings. It is made web accessible by utilizing dynamic DNS and reverse proxy, to ensure the gateway can be accessed even behind NATs. (Benomar et al., 2024). Also Nurgaliyev et al also suggests a multi-protocol IoT gateway approach that adapts the message formats and protocols into a unified standard to enable data exchange. (Nurgaliyev et al., 2024). Unified Communication Protocols was proposed as a solution for implementing unified protocols and data formats to provide compatibility and scalability, as well as improve data exchange between middleware systems. (Liu, 2024). In addition to using gateways that transform and expose IoT device capabilities as RESTful APIs can help to bridge different protocols promoting interoperability(Xun, 2024).

Compatibility problems in IoT integration impede the effective communication and data exchange that various systems require. Likewise, as IoT technologies advance and evolve, ensuring interoperability is imperative to achieving seamless and effective integration. Adequately addressing these challenges will be paramount to optimizing performance of the various systems; systems that incorporate models based on temporal action logic solve complex compatibility problems earlier in the development process, resulting in more stable systems. (Timenko et al., 2024). Furthermore, leveraging cloud computing can increase the interoperability of intelligent transportation systems by connecting IoT platforms and connected vehicles. (Shukla et al., 2024)

Standards setting organizations such as the IEEE, ITU, and ISO are key in defining standards for IoT to achieve interoperability, security, and quality, across heterogeneous IoT applications. This study will employ a t-test statistical analysis, comparing standard price and page quantity to gauge the complexity and accessibility of the project. The study will reveal no significance difference in the t-test results, for both standards groups.(Gaborović et al., 2022). Additionally, the ITU has a notable role in establishing global telecommunications standards to ensure that IOT devices can communicate properly across networks.(Dickerson et al., 2021). The ISO also places an emphasis on core foundational standards which enable IoT technologies to integrate into different sectors and thereby promote quality and safety in deploying IoT systems.(Coallier, 2022).

2.3 Scalability and Reliability Issues

The scalability and reliability issues with the Internet of Things (IoT) are significant challenges to the performance of IoT systems and their usefulness to achieve a function. As IoT networks scale and adopt more devices, and more devices generate more data and information, these networks may struggle in maintaining communication among devices and/or managing the vast amount of data being collected. Solutions to address the key issues of scalability and reliability will take a multifaceted approach, such as improving communication protocols, improving management of data, and improved security use of Software Defined Networks (SDN) provides improved resource utilization. All of this will lead to improved efficiencies and improvements in scalability of IoT networks.(Luntovskyy & Globa, 2019) Even traditional centrally managed systems will lead to bottlenecks for either human operators or other network autonomies; therefore, some solutions such as mesh, multi-hop networks, and edge computing are proposed to improve scalability.(Dickson & Ijeoma Peace OKECHUKWU, 2024). However, protocols such as MQTT may also run into scalability problems with devices limited to a single broker and so clustering and federated strategies can be more successful with MQTT protocols in scalable situations. (Spohn, 2022). While many devices experience high failure rates in IoT operations which would cause disruptions to normal performance; therefore reliability modeling would help to inform performance. Further to that, any delays to data transmissions as a result of unreliable devices in IOT networks will be untenable and thus efficient communication protocols can only be effective to get real-time information. Hence, a layered analysis approach using fault tree models, dynamic fault trees, and binary decision diagrams

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

(BDD) are proposed to quantify the reliability of the IoT network and to help guide improvements in reliability. The concept is successfully demonstrated through an extended case study about CHISS in a real world IoT situations.(Singh et al., 2024).

Cloud Infrastructure manages large IoT data using age calculation, smart storage algorithms and advanced analysis. This integrated approach effectively handles challenges such as scalability, delay and resource management. Rbeee architecture increases this by distributing treatment work near IoT units through Architecture Edge Computing. It reduces delays and bandwidth use, and ensures safe, energy efficient and responsible data processing. (Rajendra Mahto & Dr. Nidhi Mishra, 2024). In addition to real -time treatment: By removing the data to edge devices it may be instant treatment, which is important for applications that require real -time reactions.(Edje et al., 2023). Cloud infrastructure adapters Data storage with scalable algorithms that effectively manage data from 1 million IoT units, these algorithms increase performance and reduce the delay, ensure credibility for real -time application.(Deepthi et al., 2024).

Edge is crucial for data processing and 5G IoTs, and offers increased data processing and high-speed connection. Their integration supports real -time applications by providing communication with low bonding, high bandwidth. Data for data processing processes near the source reduces significant delays for smart cities and autonomous systems.(Kolapo et al., 2024). Also 5G-edge architecture can have significant performance benefits, such as an increase of 260% in throughput and a decline of 71.3% in response time compared to cloud-based solutions.(da Silva et al., 2025). The ultra-low latency and high speeds of 5G enables seamless IoT device operation and increase the system's efficiency. In addition, 5G supports large -scale device connection, which is important for the growing IoT ecosystem. (Salman et al., n.d.).Moreover There are challenges such as data security, resource management and service quality. To address these, solutions that promoted security protocols and intelligent resource planning are necessary. In addition, monitoring of multidimensional service quality ensures reliable and effective system performance.(Li & Cao, 2024)

2.4 Ethical and Regulatory Challenges

The rapid development of IoT devices increases serious concerns about privacy, data collection and consent. These devices are often connected to individual devices without the approval of clear users, collecting data quietly. In addition, users are usually ignored or incorrect, causing accidental exposure data. This lack of openness reduces the user's awareness and control of their personal information. To address this, Chang et al UTCID introduce individual privacy assistant (PPA), which evaluates privacy risk using the Entropy-based model.(Chang et al., 2024). This condition requires the development of technologies and outlined privacy savings to protect user information while maintaining the functionality. In addition to privacy preservation techniques, including cryptographic methods and anonymization, it is necessary for securing data during transmission and processing.(Goel et al., 2024).

Moreover Some regulators and technical solutions were also introduced, such as tailored protection technologies such as IoT Inspector; Increase user confidence and adoption through individual messages based on individual regulator focus.(Ghaiumy Anaraky et al., 2024). Also data protection rules such as GDPR and CCPA are important for managing IoT person protection, users determine clear standards for data protection. These laws protect personal information by compulsory and enter data protection principles directly into IoT units. In particular, GDPR manufacturers require implementing strong security measures and privacy-for-design practice.(Ebbers & Friedewald, 2023a). In addition to the compliance mechanism, such as the PACTA scheme, utilize block chain and trusted execution environments (TEE) to increase data person protection and verify compliance effectively.(Zhang et al., 2023). CCPA and Consumer Rights on the other hands emphasizes transparency; The CCPA emphasizes transparency, which means it's important for companies to disclose how they collect data to promote trust of consumers on IoT technologies. Alongside these regulations, there are still challenges around compliance and keeping pace with our changing technology which can tighten the grip of the existing legal stances and their frameworks.(Benedicta Ehimuan et al., 2024). In addition, continued research needs to surge to reshape these laws to support new technologies that will be used in the future to continue to protect user rights in IoT usages .(Ebbers & Friedewald, 2023b).

Legal concerns regarding big data and predictive analytics within both the IoT's privacy, security, and regulatory compliance sectors remain the overall consideration. The growing data collection of IoT devices means a need for provided substantial legal frameworks, particularly within e-commerce or financially based sectors, which require safeguards over personal data throughout collection, transmission, and storage processes. Moreover, given the different levels of security offered between different devices, the absence of a common security design for a technical device presents a challenge for data protection in itself .(Volynets et al., 2025). Moreover, Predictive analytics typically involves the processing of personal data, which may result in a privacy breach if mishandled.(Mühlhoff & Ruschemeier, 2024). Furthermore, the interconnectedness of IoT devices creates vulnerabilities and risks for users; a breach in one device means compromise for the entire system and network, making security measures important.(Satchithanantham, 2024). As well, there is an urgent need for changing regulations that evolve alongside technology and the expansion of data analytics.(Zahra, 2025).

2.5 Energy Consumption and Sustainability Issues

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

The environmental impacts are significant from IoT devices as they produce e-waste that contains hazardous materials which will eventually leak into the ground, leading to soil and water contamination when disposed of incorrectly. The production and operation of IoT devices also requires a lot of energy and therefore produces a substantial carbon output. (Kumar et al., 2025) recognized a range of environmental and social risks in relation to poor disposal of e-waste whilst the authors recommended "enhanced recycling, refurbishment, and secure and safe disposal of e-waste as well as positioning relevant stakeholders to address this concern0.(Kumar et al., 2025). Also sometimes resource depletion occurs as a result of using scarce resources: The involvement of scarce materials for production is contributing to resource depletion which also spurs economic upheaval.(Miura et al., 2024). Energy Consumption also includes production footprint: The carbon footprint that may be associated with production of IoT devices may be higher than the operational phase. Moreover, Growing on increasing network demand: Along with having IoT through an existing network solution could increase power consumption to over 15%.(Cappelle et al., 2024). This demonstrates that using energy efficient designs and renewable energy sources could lessen these issues.(Zayn & Miran, 2024).

Energy-efficient technologies such as LPWAN (Low-Power Wide Area Network) technology (e.g. LoRa and NB-IoT) contribute significantly to IoT efficiency by supporting multiple devices over large areas with very little available power, which is especially appropriate technology for smart cities. One of the benefits of LPWAN technology is that it supports wide area coverage and ecosystem scalability without requiring the user to charge the device more than necessary.(Igwebuike & Girma, 2024). LPWAN support low-power protocols for a network of devices that typically operate on batteries for long periods and with limited maintenance and other protocol protocols like particle swarm optimization take advantage of protocols to reduce energy consumption by minimizing the amount of data packets sent.(Tripathi & Kuthe, 2024). One of the most significant applications of LPWAN technology from the IoT is generally environmental monitoring. More specifically LPWANs enable the deployment of sensor networks for measuring vital environmental parameters which is an important metric of any smart city management framework, or modern smart city. (Karaush & Patlaienko, 2024). In addition to cost-effectiveness: The use of LPWAN technologies is economically viable, which suits them for large-scale IoT distribution.(Igwebuike & Girma, 2024). While LPWANs provides significant benefits in energy savings and efficiency, challenges such as covering blind spots remain. Innovative solutions such as nature -inspired relay selections are developed to solve these problems, ensure strong connection for battery -powered equipment.(Strzoda & Grochla, 2024).

Staaf (2025) draws attention to the environmental issues associated with battery-powered IoT devices, including their contribution to electronic waste and maintenance. The author promotes self-powered IoT sensors that include the potential to harvest ambient energy (solar, kinetic, thermal, etc.) as sustainable remediation, and he argues how those with the developments are environmentally conscious and lead to savings in overall costs. RISE has developed energy-harvesting sensors in naturalistic simulations with positive outcomes for the medical, industrial and urban applications. (Staaf, 2025). In addition, Integrating AI with IoT enhances decision-making and operational efficiency in sectors like smart cities and healthcare. AI-driven analytics also optimize energy use and cut emissions, supporting sustainability objectives.(Sehito et al., 2024). Gupta and Sharma (2024) investigated the challenge of adding stability into smart cities by targeting carbon reduction, efficient use of resources and waste minimization. They benefit from IoT, AI and renewable energy in the circular economy. The study uses quantitative matrix to guide politics and innovation against long -term environmental goals.(Gupta & Sharma, 2024). Furthermore, Ishola (2024) attempts a "Green IoT" approach that includes energy-efficient technologies, sustainable design to further align IoT development with global sustainability goals. Specific challenges of energy consumption and global standards, are still of critical need.(Ishola, 2024).

3. SUMMARIZATION ANALYSIS

The results obtained from previous researches, there methods used, basic scope with the limitations and challenges are shown in table (1) below:

Table (1): *summary of previous work*

Reference	Basic scope	Method	Key Result	Limitation/Challenge
Bhamare et al., 2024	Security & Privacy	Blockchain, Fog Computing, ML	Need multi-layered security	**High energy demands, scalability limitations**
Sharma & Babbar, 2024; Rasheed & Alnabhan, 2024	Security & Privacy	ML models (KNN, CatBoost)	Detect botnets ~99% accuracy	**Depends on data quality**
Mahlake et al., 2023	Security & Privacy	Lightweight encryption	99% security with minimal power	**Vulnerable if poorly implemented**

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

Bonaventura et al., 2024; Lee, 2023	Security & Privacy	Firmware updates, layered defenses	Mitigate DDoS, botnet risks	**User non-compliance in updates**
Benomar et al., 2024	Interoperability	Gateway-based integration	Adapt diverse protocols	**Complexity behind NAT/firewall**
Nurgaliyev et al., 2024	Interoperability	Multi-protocol gateway	Unify message formats	**Protocol conversion overhead**
Liu, 2024	Interoperability	Unified communication protocols	Enhance compatibility, scalability	**Standard adoption challenges**
Luntovskyy & Globa, 2019	Scalability & Reliability	Software Defined Networks (SDN)	Improve resource utilization	**Potential network complexity**
Dickson & Ijeoma, 2024	Scalability & Reliability	Mesh networks, edge computing	Enhance scalability, reduce bottlenecks	**Infrastructure, deployment costs**
da Silva et al., 2025	Scalability & Reliability	5G-edge architecture	260% throughput gain, 71.3% latency reduction	**Needs massive infrastructure upgrade**
Chang et al., 2024	Ethical & Regulatory	Entropy-based privacy assistant	Evaluate privacy risks	**User awareness, adoption**
Ebbers & Friedewald, 2023	Ethical & Regulatory	GDPR, privacy by design	Mandate robust security, consent	**Compliance complexity, evolving laws**
Igwebuike & Girma, 2024	Energy & Sustainability	Low-Power Wide Area Networks (LPWAN)	Extend battery life, efficient coverage	**Coverage blind spots**
Staaf, 2025	Energy & Sustainability	Self-powered IoT sensors	Harvest ambient energy, cut costs	**Technology maturity, cost barriers**

4. Current Risks and Challenges of the Internet of Things (IoT)

The Internet of Things (IoT) continues its rapid expansion, connecting billions of devices and revolutionizing industries. However, this widespread adoption also brings a host of significant risks and challenges that are constantly evolving. As of mid-2025 table 2 summarizing the key risks and challenges of the Internet of Things (IoT).

Table 2 *: Category, key challenges of Internet of Things (IoT)*

N	Category	Key Challenges and Descriptions
1	Security Vulnerabilities	**Key Challenges:** Ineffective or absent built-**built-in security measures**, lack of continuous updates, complexity of multi-layered device security. **Specific Risks:** Cyberattacks, hacking, data breaches, botnet formation (DDoS attacks), malware infection, physical tampering, and vulnerabilities originating from the supply chain [71--76].
2	Privacy Concerns	Key Risks: Massive volume of data collected, often without explicit consent; challenges in guaranteeing proper storage, usage, and sharing of personal data. Specific Concerns: Potential for unauthorized access to data, sensitive information being exposed due to inadequate security measures, and insufficient controls for user data privacy [77-82].
3	Interoperability	Key Challenges: Fragmented technology landscape, absence of universal standards, creating interoperability hurdles. Specific Concerns: Inconsistent data formats, lack of seamless device communication, vendor lock-in, and reliance on complex middleware, impeding scalability and data exchange. Visually Meaningful Image Encryption (VMIE) is a cutting-edge technique that protects sensitive visual information by embedding it into a seemingly innocent "cover" image. Unlike traditional encryption, which produces chaotic noise, VMIE aims to create an output that looks like a regular, harmless image, making the hidden data much less likely to be detected or intercepted by attackers [83-88].
4	Scalability and Management	Key Challenges: Effectively managing huge volumes of distinct devices and their extensive data. Specific Concerns: Complex device monitoring and configuration, the demands on existing network infrastructure, limited resources on devices affecting features, and maintaining efficient data load across potentially fluctuating workloads [89-94].

Zaid A. Alsarray, Sanaa Ahmed Kadhim. 2025, Risks and Challenges of the Internet of Things: An Analytical Review of Previous Studies and Future Research Directions. *Journal port Science Research*, 8(4), pp.357-368. https://doi.org/10.36371/port.2025.4.5

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

5	Regulatory and Compliance Landscape	Key Challenges: Navigating the complex and changing landscape of regional regulatory demands and complex global sourcing requirements Specific Concerns: Compliance burden; liability issues for device faults; compliance with complex regulations; penalties including large fines and restricted market access. [95-105].

5. FUTURE DIRECTIONS

In future research, priority should be given to the development of AI models that are not only resistant to adversarial threats but are also tailored to operate within the constrained computational capacities of IoT environments. Equally important is the creation of lightweight and energy-efficient encryption mechanisms that can uphold robust security standards without placing excessive demands on device resources. Furthermore, there is a pressing need for coordinated international initiatives aimed at standardizing interoperability protocols and implementing real-world pilot programs to evaluate the effectiveness of integrated security frameworks.

6. CONCLUSION

The paper discloses that IoT devices are more susceptible to attacks owing to the presence of obsolete firmware, poor encryption and non-compliance with interoperation, where AI-powered models such as CatBoost can yield up to 99.49% performance in detecting botnet threats. Although new technologies, such as block chain and fog computing, have improved data validity with Martínez-Pérez et al: An enhanced security protocol for IoT fog- and cloud-based applications 6 real-time detection of threats, there are still severe difficulties in implementing it on lightweight IoT devices. For example, 5G-edge architectures yielded a 260% higher throughput and 71.3 x lower latency, but at the cost of expensive and slow infrastructure upgrades Limitations span from user non-compliance with firmware updates to energy requirements for AI and encryption operations, to the complexity of being compliant (e.g., GDPR, CCPA). Disadvantages also include environmental factors, like e-waste. And increased network energy consumption (more than 15% improvement when IoT is included) Additional developments are required on adversarial robustness on AI, lightweight encryption and global interoperability standards need to be defined. Actions that could lessen risks are enforcing strong passwords, updating firmware, and moving to layered security architectures that combine AI, encryption, and regulation.

REFERENCES

[1] Adeoye, S., & Adams, R. (2024). *Revolutionizing Healthcare : The Impact and Future of the Internet of Things (IoT) in the Health Sector*. *4*(10), 127–143. https://doi.org/ 10.47760/ cognizance .2024 .v04i10.009

[2] Ahluwalia, A., Garg, V., Kapoor, S., & Gupta, L. (2024). The Internet of Things (IoT): Transformations and Challenges in the Modern World. *African Journal of Biological Sciences*, *6*(3), 764–769. https://doi.org/10.48047/afjbs.6.3.2024.764-769

[3] Al Khatib, I., Shamayleh, A., & Ndiaye, M. (2024). Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. *Informatics*, *11*(3), 47. https://doi.org/10.3390/informatics11030047

[4] Aljaafari, F., Menezes, R., Mustafa, M. A., & Cordeiro, L. C. (2021). *Finding Security Vulnerabilities in IoT Cryptographic Protocol and Concurrent Implementations*. 1–16.

[5] Benedicta Ehimuan, Ogugua Chimezie, Ob, Onyinyechi Vivian Akagha, Oluwatosin Reis, & Bisola Beatrice Oguejiofor. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

[6] Benomar, Z., Garofalo, M., Georgantas, N., Longo, F., Merlino, G., Puliafito, A., Benomar, Z., Garofalo, M., Georgantas, N., Longo, F., Merlino, G., Benomar, Z., Garofalo, M., Georgantas, N., & Longo, F. (2024). *Bridging IoT Protocols with the Web of Things : A Path to Enhanced Interoperability To cite this version : HAL Id : hal-04708266 Bridging IoT Protocols with the Web of Things : A Path to Enhanced Interoperability*.

[7] Bhamare, H., Vidhate, A., & Padiya, P. (2024). *P rivacy And Security Issues In Iot Systems*. *14*, 1352–1365.

[8] Bonaventura, D., Esposito, S., & Bella, G. (2024). The IoT Breaches your Household Again. *ArXiv Preprint ArXiv:2407.12159*.

[9] Cappelle, J., Van der Perre, L., Fitzgerald, E., Ravyts, S., Gajda, W., De Smedt, V., Cox, B., & Callebaut, G. (2024). IoT on the Road to Sustainability: Vehicle or Bandit? *ArXiv Preprint ArXiv:2405.20706*.

[10] Chang, K. C., Niu, H., Kim, B., & Barber, S. (2024). IoT Privacy Risks Revealed. *Entropy*, *26*(7). https://doi.org/10.3390/e26070561

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

[11] Coallier, F. (2022). IoT Standardization Strategies in ISO/IEC JTC 1/SC 41. *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, 1–6.

[12] Cuozzo, G., Testi, E., Riolo, S., Miuccio, L., Cena, G., Pasolini, G., De Nardis, L., Panno, D., Chiani, M., & Di Benedetto, M.-G. (2024). Research Directions and Modeling Guidelines for Industrial Internet of Things Applications. *ArXiv Preprint ArXiv:2410.02610*.

[13] da Silva, M. V. B., Barbosa, M., Queiroz, A., & Dias, K. L. (2025). A 5G-Edge Architecture for Computational Offloading of Computer Vision Applications. *ArXiv Preprint ArXiv:2501.04267*.

[14] Deepthi, K. J., Balakrishnan, T. S., Krishnan, P., & Ebenezar, U. S. (2024). Optimized Data Storage Algorithm of IoT Based on Cloud Computing in Distributed System. *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, 1–5.

[15] Dickerson, K., García-Castro, R., Kostelnik, P., & Paralič, M. (2021). Standards for the IoT. In C. Zivkovic, Y. Guan, & C. Grimm (Eds.), *IoT Platforms, Use Cases, Privacy, and Business Models: With Hands-on Examples Based on the VICINITY Platform* (pp. 125–147). Springer International Publishing. https://doi.org/10.1007/978-3-030-45316-9_6

[16] Dickson, S. M., & Ijeoma Peace OKECHUKWU. (2024). Internet of Things (IoT) Data Communication Challenges, and Solutions. *Journal of Digital Learning and Distance Education*, *2*(11), 803–808. https://doi.org/10.56778/jdlde.v2i11.226

[17] Ebbers, F., & Friedewald, M. (2023a). *Responses of the European IoT Ecosystem to the European General Data Protection Regulation*. 1–18.

[18] Ebbers, F., & Friedewald, M. (2023b). *Responses of the European IoT Ecosystem to the European General Data Protection Regulation*.

[19] Edje, A. E., Abd Latiff, M. S., & Chan, W. H. (2023). IoT data analytic algorithms on edge-cloud infrastructure: A review. *Digital Communications and Networks*, *9*(6), 1486–1515.

[20] Gaborović, A., Karić, K., Blagojević, M., & Plašić, J. (2022). *Comparative analysis of ISO/IEC and IEEE standards in the field of Internet of Things*.

[21] Garah, A., Mbarek, N., & Kirgizov, S. (2023). IoT Data Confidentiality Self-Management. *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 395–400.

[22] Ghaiumy Anaraky, R., Li, Y., Cho, H., Huang, D. Y., Byrne, K. A., Knijnenburg, B., & Nov, O. (2024). Personalizing Privacy Protection With Individuals' Regulatory Focus: Would You Preserve or Enhance Your Information Privacy? *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1–17.

[23] Goel, P. K., Singh, G., Chattopadhyay, S., Vishwakarma, P., Jain, A., & Aeri, M. (2024). Privacy-Preserving Techniques for Data Sharing in the Era of IoT. *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, 1053–1058.

[24] Gupta, S., & Sharma, P. (2024). Sustainability Integration in Smart Cities: Future Generation Smart Systems. *Available at SSRN 5077694*.

[25] Igwebuike, C., & Girma, A. (2024). Analysis of Low-Power Wide-Area Network (LPWAN) Internet of Things (IoT) Telemetry System with Wireline Solution Approach Recommendation. *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*, 1–6.

[26] Ishola, A. (2024). IoT applications in sustainability and sustainable community development. *World Journal of Advanced Research and Reviews _ Awaiting DOI*.

[27] Jose J, M. D., Kumar, D. D. V., & Jayakeerthi, M. (2024). Iot in the Modern World. *Futuristic Trends in Computing Technologies and Data Sciences Volume 3 Book 8*, *3*, 284–290. https://doi.org/10.58532/v3bkct8p4ch2

[28] Kamble, N. N., & Kulkarni, D. A. (2024). Internet of Things (Iot) and Smart World. In *Futuristic Trends in Physical Sciences Volume 3 Book 1* (Vol. 3). https://doi.org/10.58532/v3bkps1ch13

[29] Karaush, Y., & Patlaienko, M. (2024). Evaluating IoT Low Power Wide Area Networks for Smart City Solutions. *2024 32nd National Conference with International Participation (TELECOM)*, 1–4.

[30] Kolapo, R., Kawu, F. M., Abdulmalik, A. D., Edem, U. A., & Atisi, M. (2024). *Edge computing : Revolutionizing data processing for IoT applications*. *13*(02), 23–29.

[31] Kumar, Y., Kumar, P., & Kumar, B. (2025). Impact Assessment of E-Waste: Environment and Society. *Global Waste Management*, 115–144.

[32] Lee, M. (2023). *An Empirical Survey on the Cybersecurity of the Industrial Internet of Things An Empirical Survey on the Cybersecurity of the Industrial Internet of Things*.

[33] Li, Z., & Cao, K. (2024). *Application and Challenge of Edge Computing Based on 5G Communication in Information and Communication Systems*. *8*(6), 39–45.

[34] Liu, Z. (2024). Compatibility and optimization Strategy of Multiple Network Protocols in the Internet of Things Installation and Debugging Training Bench. *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, 1–6.

[35] Luntovskyy, A., & Globa, L. (2019). Performance, reliability and scalability for IoT. *2019 International Conference on Information and Digital Technologies (IDT)*, 316–321.

[36] Mahlake, N., Mathonsi, T. E., Du Plessis, D., & Muchenje, T. (2023). A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. *J. Commun.*, *18*(1), 47–57.

[37] Miura, N., Taguchi, H., Watanabe, K., Nohara, M., Makita, T., Tanabe, M., Wakimoto, T., Kumagai, S., Nosaka, H., & Aratake, A. (2024). 17.4 Environmentally-Friendly Disposable Circuit and Battery System for Reducing Impact of E-Wastes. *2024 IEEE International Solid-State Circuits Conference (ISSCC)*, *67*, 320–322.

[38] Mühlhoff, R., & Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology*, *16*(1), 261–292.

[39] N, A. K., Ramesh, D. D., S, D. P. H., R, D. P., & G., V. B. (2023). Securing Iot Data Transmission: A Comprehensive Approach Integrating Two-Fish Encryption With Wireless Smart Energy Systems And Iot Cloud Services. *Migration Letters*, *21*(S1), 972–993. https://doi.org/10.59670/ml.v20i3.7269

[40] Ntayagabiri, J. P., Bentaleb, Y., Ndikumagenge, J., & Makhtoum, H. E. L. (2024). *A Comprehensive Approach to Protocols and Security in Internet of Things Technology*.

[41] Nurgaliyev, K., Tokhmetov, A., & Tanchenko, L. (2024). an Analysis of the Heterogeneous Iot Device Network Interaction in a Cyber-Physical System. *Scientific Journal of Astana IT University*, 53–68. https://doi.org/10.37943/16enna6243

[42] Patel, S., Patidar, P. K., & Patidar, M. (2024). *IoT Applications in Healthcare and Industry : Current State , Challenges , and Future Perspectives*. 89–96. https://doi.org/10.48175/IJARSCT-22614

[43] Pravylo, V., & Averkiiev, Y. (2024). Analysing Malicious Software Supporting Ddos Attacks on Iot Networks. *Information and Telecommunication Sciences*, *0*(1), 50–54. https://doi.org/ 10.20535/ 2411-2976.12024.50-54

[44] Rajendra Mahto, & Dr. Nidhi Mishra. (2024). An Investigation on Handling IoT Big Data with RBSEE Architecture. *Journal of Advances in Science and Technology*, *21*(1), 97–104. https://doi.org/10.29070/j4f6hq17

[45] Rasheed, A., & Alnabhan, M. (2024). Detection of Botnet Attacks on IoT Using AI. *2024 International Jordanian Cybersecurity Conference (IJCC)*, 7–13.

[46] Richa, E. (2021). IoT: Security Issues and Challenges. *Smart Innovation, Systems and Technologies*, *196*(12), 87–96. https://doi.org/10.1007/978-981-15-7062-9_9

[47] Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Innovative resource-saving security strategies for IoT devices. *Journal of Edge Computing*.

[48] Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, *7*(May), 1–16. https://doi.org/10.3389/frai.2024.1397480

[49] Said, N. M. M., Ali, S. M., Shaik, N., Begum, K. M. J., Shaban, A. A. A. E., & Samuel, B. E. (2024). Analysis of Internet of Things to Enhance Security Using Artificial Intelligence based Algorithm. *Journal of Internet Services and Information Security*, *14*(4), 590–604. https://doi.org/10.58346/JISIS.2024.I4.037

[50] Salman, A. S., Mahmoud, A., Yaseen, A. H., Ahmed, O. S., & Abdullah, M. Y. (n.d.). *The synergistic impact of 5g on internet of things innovation and growth*.

[51] Satchithanantham, U. (2024). Significant Security Challenges in IOT Analytics. *International Journal of Communication and Information Technology*, *5*(1), 01–05. https://doi.org/ 10.33545/ 2707661x.2024.v5.i1a.71

[52] Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2024). *Security in the Internet of Things : Identifying and Analysing Critical Categories Security in the Internet of Things : Identifying and Analysing Critical Categories*. 0–30. https://doi.org/ 10.20944/ preprints202412.2512.v1

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

[53] Sehito, N., Yang, S., Larik, R. S. A., Kamal, M. M., Alwabli, A., & Ullah, I. (2024). Artificial Intelligence (AI) and Internet of Things (IoT) Applications in Sustainable Technology. In *Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies* (pp. 227–246). Springer.

[54] Sharma, A., & Babbar, H. (2024). IoT-POT: Machine Learning-based Detection of Mirai Botnet Attacks in IoT. *2024 First International Conference on Innovations in Communications, Electrical and Computer Engineering (ICICEC)*, 1–6.

[55] Shukla, R., Choudhary, A. K., Kumar, V. S., Tyagi, P., Mutharasan, A., Kumar, S., & Gupta, S. K. (2024). Understanding integration issues in intelligent transportation systems with IoT platforms, cloud computing, and connected vehicles. *Journal of Autonomous Intelligence*, *7*(4), 1–13. https://doi.org/10.32629/jai.v7i4.1043

[56] Singh, K., Yadav, M., Singh, Y., Barak, D., Saini, A., & Moreira, F. (2024). Reliability on the Internet of Things with designing approach for exploratory analysis. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1382347

[57] Spohn, M. A. (2022). On MQTT Scalability in the Internet of Things: Issues, Solutions, and Future Directions. *Journal of Electronics and Electrical Engineering*, *1*(1), 4. https://doi.org/10.37256/jeee.1120221687

[58] Staaf, H. (2025). *The future of green tech : Self-powered IoT sensors*. *January*, 1–5.

[59] Strzoda, A., & Grochla, K. (2024). A Nature-Inspired Approach to Energy-Efficient Relay Selection in Low-Power Wide-Area Networks (LPWAN). *Sensors*, *24*(11), 3348.

[60] Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and Security Mechanisms in the Internet of Things: A Review. *Applied Sciences (2076-3417)*, *15*(2).

[61] Timenko, A. V., Shkarupylo, V. V., Kulykovska, N. A., & Hrushko, S. S. (2024). Study of the method of controlling the compatibility of Internet of Things devices based on the MQTT application layer protocol. *Herald of Advanced Information Technology*, *7*(1), 48–58. https://doi.org/10.15276/hait.07.2024.4

[62] Touqir, A., & Haas, O. (2024). *Systematic Review of Fuzzing in IoT : Evaluating Techniques , Vulnerabilities , and Research Gaps*. 1–30.

[63] Tripathi, D. R., & Kuthe, B. S. (2024). *Optimizing IOT Network Performance : A Study on Low-Power Wide-Area Network (LPWAN) Technologies for Smart City Applications*. *October*.

[64] Vojković, G., Milenković, M., & Katulić, T. (2020). IoT and smart home data breach risks from the perspective of data protection and information security law. *Business Systems Research: International Journal of the Society for Advancing Innovation and Research in Economy*, *11*(3), 167–185.

[65] Volynets, V., Popov, A., Pushkar, T., Frolov, M., & Babarytskyi, O. (2025). Legal Aspects of Using the Internet of Things (Iot) in Electronic Commerce. *Journal of Lifestyle and SDG'S Review*, *5*(2), 1–17. https://doi.org/10.47172/2965-730X.SDGsReview. v5.n02. pe03657

[66] Weber, R. H., & Weber, R. (2016). Internet of Things Archives | Internet of Things. *Cisco*, *2019*(July 2016), 1–47.

[67] Xun, L. (2024). Bridging IoT Protocols with the Web of Things: A Path to Enhanced Interoperability. *International Journal of High Speed Electronics and Systems*, 2540049.

[68] Zahra, Y. (2025). Regulating AI in Legal Practice: Challenges and Opportunities. *Journal of Computer Science Application and Engineering (JOSAPEN)*, *3*(1), 10–15.

[69] Zayn, M., & Miran, K. (2024). Harmony in Connectivity: Toward a Sustainable Future with Green Internet. *International Journal for Research in Applied Science and Engineering Technology*, *12*(2), 1363–1367. https://doi.org/10.22214/ijraset.2024.58599

[70] Zhang, Y., Yang, J., Lei, H., Bao, Z., Lu, N., Shi, W., & Chen, B. (2023). PACTA: An IoT data privacy regulation compliance scheme using TEE and blockchain. *IEEE Internet of Things Journal*, *11*(5), 8882–8893.

[71] Jaafar Ahmed Abdulsaheb, Raghad Mohanned Nafea, Waleed Ameen Mahmoud Al-Jawher, Mohammed Lateef Hayyawi "IoT Based Smart Parking System" Authors Publication date 2024/6/28, Journal Journal Port Science Research, Volume 7, Issue 3, Pages . 196-203, 2024.

[72] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher "Uruk 4D discrete chaotic map for secure communication applications" Journal Port Science Research, Volume 5, Issue 3, Pages 131-142, 2023.

[73] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher "Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos" Journal of Electronic Imaging, Volume 32, Issue 4, Pages 043038-043038, 2023.

[74] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher "WAM 3D discrete chaotic map for secure communication applications" International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages45-54, 2022.

[75] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher "A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet–Fourier Transforms" Journal of Cyber Security and Mobility, Pages 435-464, 2023.

[76] Qutaiba K Abed, Waleed A Mahmoud Al-Jawher "A Robust Image Encryption Scheme Based on Block Compressive Sensing and Wavelet Transform" International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 7-13, 2022.

[77] Hamid M Hasan, Waleed A Mahmoud Al-Jawher, Majid A Alwan "3-d face recognition using improved 3d mixed transform" Journal International Journal of Biometrics and Bioinformatics (IJBB), Volume 6, Issue 1, Pages 278-290, 2012.

[78] Hamid M Hasan, AL Jouhar, Majid A Alwan "Face recognition using improved FFT based radon by PSO and PCA techniques" International Journal of Image Processing (IJIP), Volume 6, Issue 1, Pages 26-37, 2012.

[79] Waleed A Mahmoud, Afrah Loay Mohammed Rasheed " 3D Image Denoising by Using 3D Multiwavelet" AL-Mustansiriya J. Sci, Volume 21, Issue 7, Pages 108-136, 2010.

[80] AHM Al-Helali, WA Mahmmoud, HA Ali "'A Fast personal palmprint authentication Based on 3d-multi Wavelet Transformation" TRANSNATIONAL JOURNAL OF SCIENCE AND TECHNOLOGY, Volume 2, Issue 8, 2012.

[81] Waleed A Mahmoud Al-Jawher, Sarah H Awad "A proposed brain tumor detection algorithm using Multi wavelet Transform (MWT)" Materials Today: Proceedings, Volume 65, Pages 2731-2737, 2022.

[82] W. A. Mahmoud, J J. Stephan and A. A. Razzak "Facial Expression Recognition Using Fast Walidlet Hybrid Transform" Journal port Science Research و Volume3, No:1, Pages 59-69, 2020.

[83] Walid Amin Mahmoud "Computation of wavelet and multiwavelet transforms using fast fourier transform" Journal Port Science Research, Volume 4, Issue 2. Pages 111-117, 2021.

[84] Zahraa A Hasan, Suha M Hadi, Waleed A Mahmoud "Time domain speech scrambler based on particle swarm optimization" Pollack Periodica, Volume 18, Issue 1, Pages 161-166, 2023.

[85] Rasha Ali Dihin, Waleed A Mahmoud Al-Jawher, Ebtesam N AlShemmary "Diabetic retinopathy image classification using shift window transformer" International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 23-29, 2022.

[86] [86] Ebtesam N. AlShemmary and Waleed A. Mahmoud Al-Jawher Rasha Ali Dihin "Automated Binary Classification of Diabetic Retinopathy by SWIN Transformer" Journal of Al-Qadisiyah for computer science and mathematics (JQCM), Volume 15,Issue 1, Pages 169-178, 2023.

[87] Zahraa A Hasan, Suha M Hadi, Waleed A Mahmoud "Speech scrambler with multiwavelet, Arnold Transform and particle swarm optimization" Pollack Periodica, Volume 18, Issue 3, Pages 125-131, 2023.

[88] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher "An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain" International Journal of Computers and Applications, Volume 46, Issue 5, Pages 324-337, 2024.

[89] Rasha Ali Dihin, Ebtesam N AlShemmary, Waleed AM Al-Jawher "Wavelet-Attention Swin for Automatic Diabetic Retinopathy Classification" Baghdad Science Journal, Volume 21, Issue 8, Pages 2741-2741, 2024.

[90] Lubna K Alazzawi, Ali M Elkateeb, Aiyappa Ramesh, Waleed Aljuhar, "Scalability analysis for wireless sensor networks routing protocols" 22nd International Conference on Advanced Information Networking and Applications-Workshops (aina workshops 2008), Pages 139-144, 2008.

[91] Waleed Al-Jawhar, Abbas Hasan Kattoush, Sulaiman M Abbas, Ali T Shaheen "A high performance parallel Radon based OFDM transceiver design and simulation" Digital Signal Processing, Volume 18, Issue 6, Pages 907-918, 2008.

[92] Maryam I Mousa Al-Khuzaay, Waleed A Mahmoud Al-Jawher "New Proposed Mixed Transforms: CAW and FAW and Their Application in Medical Image Classification" International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 15-21, 2022.

[93] AHM Al-Heladi, WA Mahmoud, HA Hali, AF Fadhel "Multispectral Image Fusion using Walidlet Transform" Advances in Modelling and Analysis B, Volume 52, Issue 1-2, Pages 1-20, 2009.

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 4. 2025

[94] Qutaiba K Abed, Waleed A Mahmoud Al-Jawher "Optimized color image encryption using arnold transform, URUK chaotic map and GWO algorithm" Journal Port Science Research, Volume 7, Issue 3, Pages, . 219-236, 2024.

[95] Salman Waleed A. Mahmud Al-Jouhar, Dr. Talib M. Jawad Abbas Al-Talib, R. HamudiA. "Fingerprint Image Recognition Using Walidlet Transform" Australian Journal of Basic and Applied Sciences, Australia, 2012.

[96] Haqi Khalid, Shaiful Jahari Hashim, Fazirulhisyam Hashim, Waleed Ameen Mahmoud Al-Jawher, Muhammad Akmal Chaudhary, Hamza HM Altarturi "Raven: Robust anonymous vehicular end-to-end encryption and efficient mutual authentication for post-quantum intelligent transportation systems" IEEE Transactions on Intelligent Transportation Systems, 2024.

[97] Waleed A Mahmoud Al-Jawher, Shaimaa A Shaaban "K-Mean Based Hyper-Metaheuristic Grey Wolf and Cuckoo Search Optimizers for Automatic MRI Medical Image Clustering" Journal Port Science Research, Volume 7, Issue 5, Pages 109-120, 2024.

[98] Jane Jaleel Stephan and A. A. W. Razzak W. A. Mahmoud "Facial Expression Recognition from Video Sequence Using Self Organizing Feature Map" Journal port Science Research و TRANSACTION ON ENGINEERING, TECHNOLOGY AND THEIR APPLICATIONS, Volume 4, Issue 2, 2021.

[99] Walid A Mahmoud, Majed E Alneby, Wael H Zayer "Multiwavelet Transform and Multi-Dimension -Two Activation Function Wavelet Network Using for Person Identification" IJCCCE, Volume 11, Issue 1, Pages 46-61, 2011.

[100] Waleed Ameen Mahmoud, Ommama Razzak "Speech recognition using new structure for 3D neural network" 2010, University of Technology, 1st Computer Conference, Pages . 161-171, ttps://cs.uotechnology.edu.iq/index.php/112-about-dept-en/394-conf-2010

[101] A. Barsoum and Entather Mahos Waleed. A. .Mahmoud "Fuzzy Wavenet (FWN) classifier for medical images" Al-Khwarizmi Engineering Journal, Volume 1, Issue 2, Pages 1-13, 2005.

[102] Waleed A. Mahmoud, Ahmed S Hadi "Systolic Array for Realization of Discrete Wavelet Transform" Journal of Engineering, Volume 13, Issue 02, Pages 1368-1377, 2007.

[103] W. A. Mahmoud & I.K. Ibraheem "Image Denoising Using Stationary Wavelet Transform" Signals, Inf. Patt. Proc. & Class, .Volume 46, Issue 4, Pages 1-18, 2003.

[104] WA Mahmoud, IA Al-Akialy "A Tabulated Method of Computation Multiwavelet Transform" Journal of AL-Rafidain University College for Sciences, Volume 15, Issue 1, Pages 161-170, 2004.

[105] Saadi Mohammed Saadi, Waleed Al-Jawher "Enhancing image authenticity: A new approach for binary fake image classification using DWT and swin transformer" Global Journal of Engineering and Technology Advances, Volume 19, Issue 3, Pages 1-10, 2024.

[106] Abbas Hasan Kattoush, W Al-Jawhar, A Ghodayyah "Multiwavelet computed Radon-based OFDM transceiver designed and simulation under different channel conditions" Journal of Information & Computing Science, Volume 5, Issue 2, Pages 133-145, 2010.