Fortifying IoT against crimpling cyber-attacks: a systematic review

Usman Tariq

Irfan Ahmed

Muhammad Attique Khan

Ali Kashif Bashir

University of
Kerbala

Fortifying IoT against crimpling cyber-attacks: a systematic review

Abstract

The rapid growth and increasing demand for Internet of Things (IoT) devices in our everyday lives create exciting opportunities for human involvement, data integration, and seamless automation. This fully interconnected ecosystem considerably impacts crucial aspects of our lives, such as transportation, healthcare, energy management, and urban infrastructure. However, alongside the immense benefits, the widespread adoption of IoT also brings a complex web of security threats that can influence society, policy, and infrastructure conditions. IoT devices are particularly vulnerable to security violations, and industrial routines face potentially damaging vulnerabilities. To ensure a trustworthy and robust security framework, it is crucial to tackle the diverse challenges involved. This survey paper aims to aid researchers by categorizing attacks and vulnerabilities based on their targets. It provides a detailed analysis of attack methods and proposes effective countermeasures for each attack category. The paper also highlights case studies of critical IoT applications, showcasing security solutions. In addition to traditional cryptographic approaches, this work explores emerging technologies like Quantum Crypto Physical Unclonable Functions (QC-PUFs) and blockchain, discussing their pros and cons in securing IoT environments. The research identifies and examines attacks, vulnerabilities, and security measures and endeavors to impact the overall understanding of IoT security. The insights and findings presented here will serve as a valuable resource for researchers, guiding the development of resilient security mechanisms to ensure the trustworthy and safe operation of IoT ecosystems.

Keywords

Creative Commons License

REVIEW ARTICLE

Fortifying IoT Against Crimpling Cyber-attacks: A Systematic Review

Usman Tariq [a,*], Irfan Ahmed [b], Muhammad Attique Khan [c], Ali Kashif Bashir [d]

[a] Department of Management Information Systems, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia
[b] Department of Computer Science, College of Engineering, Virginia Commonwealth University, Richmond, VA, 23284, USA
[c] Department of Computer Science, HITEC University, Taxila, Pakistan
[d] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, M156BH, UK

Abstract

The rapid growth and increasing demand for Internet of Things (IoT) devices in our everyday lives create exciting opportunities for human involvement, data integration, and seamless automation. This fully interconnected ecosystem considerably impacts crucial aspects of our lives, such as transportation, healthcare, energy management, and urban infrastructure. However, alongside the immense benefits, the widespread adoption of IoT also brings a complex web of security threats that can influence society, policy, and infrastructure conditions. IoT devices are particularly vulnerable to security violations, and industrial routines face potentially damaging vulnerabilities. To ensure a trustworthy and robust security framework, it is crucial to tackle the diverse challenges involved. This survey paper aims to aid researchers by categorizing attacks and vulnerabilities based on their targets. It provides a detailed analysis of attack methods and proposes effective countermeasures for each attack category. The paper also highlights case studies of critical IoT applications, showcasing security solutions. In addition to traditional cryptographic approaches, this work explores emerging technologies like Quantum Crypto Physical Unclonable Functions (QC-PUFs) and blockchain, discussing their pros and cons in securing IoT environments. The research identifies and examines attacks, vulnerabilities, and security measures and endeavors to impact the overall understanding of IoT security. The insights and findings presented here will serve as a valuable resource for researchers, guiding the development of resilient security mechanisms to ensure the trustworthy and safe operation of IoT ecosystems.

Keywords: Internet of things, Cyber security, Anomaly detection, Systematic literature review, Machine learning (ML), Blockchain

1. Introduction

The realm of IoT security encompasses a broad range of strategies, tools, processes, systems, and methods aimed at safeguarding the entirety of the Internet of Things. It involves protecting physical components, applications, data, and network fixtures to guarantee the availability, integrity, and confidentiality of IoT ecosystems. Security challenges are abundant due to the continuous discovery of numerous vulnerabilities within IoT systems. Robust IoT security entails a holistic approach to protection, encompassing measures such as component hardening, continuous monitoring, firmware updates, access management, proactive threat response, and active vulnerability remediation. The significance of IoT security cannot be understated, as these sprawling and vulnerable systems represent highly attractive attack vectors.

IoT security vulnerabilities are pervasive across a wide range of domains, including vehicles, smart grids, watches, and smart home devices. For instance, researchers have identified webcams with glaring security flaws [1], easily exploitable for unauthorized network access. Similarly, smartwatches have been found to harbor vulnerabilities enabling

hackers to track wearers' locations and eavesdrop on their conversations [2]. These examples underscore the pressing need to comprehensively and proactively address IoT security concerns.

1.1. IoT security challenges

Securing IoT environments presents many challenges owing to the distinctive characteristics of IoT devices and systems. The absence of standardized regulations and a lack of awareness regarding inherent risks significantly compound the complexity of IoT security. Key challenges encompass limited visibility and control over deployed devices, the intricate integration of diverse IoT devices into existing security frameworks, vulnerabilities stemming from open-source code in firmware, the sheer volume of data generated by IoT systems, inadequate vulnerability testing practices, unresolved vulnerabilities, susceptible APIs, and the prevalence of weak passwords. Effectively addressing these challenges necessitate implementing specific security measures, including API security, meticulous device inventory management, continuous software updates, robust encryption for data at rest and in transit, multi-factor authentication, comprehensive network security provisions, and diligent vulnerability patching.

1.2. IoT adoption use case

In today's world, the widespread adoption of IoT devices necessitates implementing robust measures for connectivity, management, and control. To achieve this, three fundamental steps are essential. Firstly, the process of discovering and classifying each connected object enables rapid identification and automated provisioning based on device type and the application of appropriate configuration policies. Secondly, the network infrastructure can be effectively segmented into dedicated virtual networks, ensuring the separation of services and applications to optimize functionality and enhance security. Lastly, continuous monitoring of device behaviors enables real-time inventory management and prompt response in the event of deviations. By adhering to these steps, cybersecurity researchers can significantly enhance the usability of their IoT devices, promoting efficient operation, timely detection of anomalies, and proactive device management and security practices.

Multiple fundamental elements are essential for enabling the functionality of IoT. Identification, a crucial element, plays a significant role in naming and matching services to their respective demands. IoT devices utilize sensing capabilities to capture data and transmit it to the cloud or databases for analysis. Communication serves as a binding force, enabling seamless interaction among diverse objects to provide targeted digital services. Various communication protocols [3] such as Wireless Fidelity (WiFi), Bluetooth, Zigbee, Message Queuing Telemetry Transport (MQTT), Institute of Electrical and Electronics Engineers (IEEE) 802.15.4, Object Linking and Embedding for Process Control Unified Architecture (OPC-UA), Near Field Communication (NFC), Z-wave, Long Range Wide Area Network (LoRaWAN), SigFox, and Long-Term Evolution Advanced (LTE-Advanced) are utilized for facilitating these interactions. Hardware components, including microcontrollers, microprocessors, Field-programmable gate arrays (FPGAs), and system-on-chip (SoCs) handle processing tasks, while software functions and processing systems form the intelligent core of IoT. The eventual objective of IoT is to render services accessible anytime, anywhere, and to anyone.

1.3. Impact of device specification in IoT anomaly detection

With reference to Table 1, it is evident that the specifications of IoT devices and network infrastructure significantly impact the capability of anomaly detection and the effectiveness of cyber defense in IoT systems. The CPU clock speed and cache size of devices determine their processing power and ability to manage real-time anomaly detection algorithms. A higher clock speed and larger cache enable faster processing and analysis of data, improving the responsiveness of anomaly detection systems. The availability of sufficient RAM and flash memory allows for storing and processing large volumes of data, facilitating comprehensive anomaly detection, and enhancing the system's defense capabilities. The presence of cameras and audio/video support enables the capture and analysis of multimedia data, enriching the anomaly detection process. Supported protocols play a vital role in facilitating communication and data exchange between IoT devices and the detection system, enhancing the system's ability to monitor and identify anomalies. The instruction size, available registers, memory access type, and instruction set architectures influence the execution efficiency and computational capabilities of anomaly detection algorithms. Compliance with applicable IoT standards ensures interoperability and compatibility, enabling seamless integration of different devices and systems for a robust cyber defense mechanism in IoT environments. Hence, careful consideration

Table 1. IoT Device cataloging with reinforced computer peripherals.

Devices	CPU	Clock	Cache	RAM	Flash	Supported Protocols	Instruction Size	Available Registers	Memory Access Type	Instruction Set Architectures
Raspberry Pi 4	Broadcom BCM2711	1.5 GHz	512 KB	4 GB	16 GB	Wi-Fi, Bluetooth	32 bits	16	Memory Mapped	ARMv8-A
Arduino Uno	Atmel ATmega328P	16 MHz	2 KB	2 KB	32 KB	UART, I2C	16 bits	32	Memory Mapped	AVR
ESP32	Tensilica Xtensa LX6	240 MHz	512 KB	520 KB	4 MB	Wi-Fi, Bluetooth	32 bits	16	Memory Mapped	Xtensa LX6
BeagleBone Black	Texas Instruments AM335x	1 GHz	256 KB	512 MB	4 GB	Ethernet, UART	32 bits	32	DDR3	ARMv7-A
NVIDIA Jetson Nano	Quad-core ARM Cortex-A57	1.43 GHz	2 MB L2	4 GB	16 GB eMMC	Ethernet, USB	64 bits	32	LPDDR4	ARMv8-A
Intel Edison	Intel Atom	500 MHz	512 KB L2	1 GB	4 GB eMMC	Wi-Fi, Bluetooth	32 bits	16	DDR3	x86
Particle Argon	Nordic Semiconductor	64 MHz	256 KB	128 KB	1 MB	Wi-Fi, Bluetooth	32 bits	16	Memory Mapped	ARM Cortex-M4
Microchip PIC32	MIPS32 M4K	80 MHz	32 KB	128 KB	512 KB	UART, SPI, I2C	16 bits	32	Memory Mapped	MIPS32
Adafruit Feather M0	Atmel SAMD21	48 MHz	256 KB	32 KB	256 KB	UART, SPI, I2C	32 bits	16	Memory Mapped	ARM Cortex-M0+

of IoT device and network specifications is crucial for developing effective anomaly detection systems and strengthening the overall cybersecurity posture in IoT deployments.

1.4. Generalized IoT layered-architecture

The generalized architecture of an IoT system entails four layers: Perception, Network, Processing, and Application. In the Perception layer, nodes such as conveyor systems, surveillance cameras, Global Positioning System (GPS) modules, Radio-frequency Identification (RFID) scanners, and manufacturing robots are liable for supervising the settings and aggregation of sensory data. The Network layer comprises communication systems [4] like WiFi, Bluetooth, Zigbee, Long-Term Evolution (LTE), and protocols like Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), facilitating the transfer of data to the subsequent Processing layer. Within the Processing layer, cloud servers and databases handle tasks such as data analysis, computation, decision-making, and the storage of vast amounts of information. Ultimately, the Application layer caters to the distinctive requirements of end-users, delivering tailored services based on their requirements and preferences.

1.5. Deviations or anomalies in IoT setting

Anomaly detection focuses on data, device & network changes, revealing previously unknown threats and communication patterns that have not yet been documented in threat databases or operate covertly, causing gradual shifts. By analyzing existing IoT devices, network communication and infrastructure, an effective anomaly detection can provide administrators with a comprehensive network mapping that offers valuable insights. This includes identifying devices and clients within the network, establishing connections and hierarchies between devices (such as master/slave relationships), monitoring data packets and their content, identifying utilized protocols, and analyzing the frequency of specific communication patterns. Through this approach, IoT enabler-establishments can become eligible to effectively detect and address deviations or anomalies, enabling proactive mitigation of potential security risks and ensuring the stability and integrity of the network.

1.6. Research contributions

This research paper significantly contributes to the domain knowledge of IoT vulnerabilities,

anomalies, risks, threats, and security features. Firstly, it provides a comprehensive review of the existing literature, synthesizing the current understanding of IoT security issues and highlighting the key vulnerabilities and threats that can conciliate the integrity and confidentiality of IoT systems. This review serves as a valuable resource for researchers and practitioners seeking to gain a holistic understanding of the security challenges in the IoT domain.

Secondly, the paper presents the results of a comprehensive system generated anomaly spread and identification survey conducted among experts and practitioners in the field. The survey data offers insights into real-world experiences and practices regarding IoT security, shedding light on the most common anomalies and risks encountered. By analyzing the survey responses, the research paper identifies trends, patterns, and emerging concerns in the IoT security backdrop, informing future research directions and best practices.

Furthermore, the research paper proposes a systematic framework for assessing and mitigating IoT vulnerabilities and risks. It provides a structured approach that the cybersecurity scientific community can adopt to identify potential threats, evaluate their impact, and implement appropriate security measures. The framework considers both technical aspects (such as encryption, authentication, and access control) and non-technical factors (such as policy and governance) to create a comprehensive security strategy.

Lastly, the paper evaluates the effectiveness of existing security features and protocols in mitigating IoT risks. It examines the strengths and limitations of commonly used security mechanisms and proposes enhancements to address the identified gaps. By critically assessing the current state of security features, the research paper guides the development and implementation of more robust and resilient security solutions for IoT environments.

We, the authors, believe that the findings of this research paper will empower IoT infrastructure handlers and researchers to better understand, address, and mitigate the vulnerabilities and risks associated with IoT deployments.

1.7. Paper organization

Section 2 provides a detailed explanation of the 'Procedural Research Method' and its rationale for utilizing a systematic methodology in evaluating security challenges within the jurisdiction of IoT. This approach aims to establish a comprehensive threat taxonomy to thoroughly understand the

subject matter. In Section 3, the research delves into the 'Security background, terminology, and objectives', offering valuable insights into the contextual aspects of the study. Section 4 presents 'Key Applicable Recommendations', proposing lightweight, scalable, and effective cyber-shields for IoT cyber-defense. Finally, Section 5 serves as the conclusion, highlighting the study's limitations and providing recommendations for future research directions. This sequential organization of sections ensures a coherent and logical flow of information, enhancing the overall structure and readability of the research paper.

2. Procedural research method

This research paper employed a systematic methodology to assess the security challenges in the realm of IoT and construct a comprehensive threat taxonomy. A meticulous literature search was conducted using pertinent keywords, such as "IoT" and "security," across renowned publication databases including Elsevier, IEEE, ACM, Springer, IET, MDPI, Wiley and etc. This process yielded a wide array of survey papers, providing a solid foundation for comprehending the IoT security landscape. Leveraging their own expertise in the security field [5], the authors carefully examined and selected pertinent topics crucial to network security. Fig. 1 illustrates the research dispersal data with respect to subject area. Investigating from diverse sources of research journals and considering diverse subjects is important for IoT cyber security research survey as it allows for a comprehensive and multidisciplinary understanding of the complex challenges and potential solutions. Drawing from various fields such as computer science, decision science, engineering, material science, mathematics, machine learning, artificial intelligence (AI), and more ensures a holistic approach to address the multifaceted aspects of IoT security, fostering innovative ideas and robust methodologies to mitigate risks and safeguard IoT systems effectively. In our examination of dissimilar procedural research methods, including Scoping Review, Integrative Review, Realist Review, and Quantitative Synthesis, we aimed to ensure the effectiveness and accuracy of our furnished analysis. Upon careful consideration, we found that the gold standard in evidence synthesis is a systematic review. This method provides a rigorous and transparent approach to gather, assess, and analyze existing literature, following a predefined protocol to minimize bias and ensure reproducibility. Contrasting the Scoping Review, which focuses on mapping available literature to

(a) Dispersal of researches based on the year of publication.

(b) Research dispersal based on journals.

Fig. 1. Research distribution statistics.

identify key concepts and gaps but lacks the depth and comprehensive analysis, Integrative Review synthesizes diverse research methodologies but may not exhibit the same level of methodological rigor. Realist Review, while exploring underlying mechanisms, may be limited in generalizability compared to the broad scope of a systematic review. Whereas, Quantitative Synthesis may lack the qualitative depth and context provided by the systematic review, which thoroughly examines both quantitative and qualitative evidence. Overall, the meticulous and comprehensive approach of the systematic review ensures the generation of robust and reliable findings.

To gain a deeper understanding of the primary studies and identify shared patterns, an analysis was conducted to examine the prevalence, frequency, and occurrence of keywords across the complete set of

studies. This comprehensive examination aimed to identify recurring themes and topics within the selected studies and shed light on the focus and emphasis of the research. The findings, illustrated in Table 2, revealed a growing interest and emphasis on safeguarding IoT devices against cyber-attacks, providing valuable insights into the prevailing trends and interests in this area of research. This analysis provides a broader perspective and highlights significant aspects related to the primary topic of interest.

It is evident that the IoT has witnessed a remarkable growth trajectory, with a substantial number of connected devices already in use and an anticipated doubling by 2025 (i.e., as illustrated in Fig. 2) [6,7]. This rapid expansion has resulted in diverse applications across various domains, such as the Industrial Internet of Things (IIoT), facilitating enhanced communication and optimization of production processes among machines. Another noteworthy domain is the Internet of Medical Things (IoMT), focusing on healthcare applications like remote patient monitoring and personalized health tracking. Likewise, IoT plays a pivotal role in the evolution of Smart Cities, enabling efficient management of traffic and waste disposal while unlocking the potential of data-driven governance. The integration of IoT devices in smart homes has also revolutionized daily life, with interconnected appliances such as thermostats, televisions, and security systems. However, the widespread deployment of IoT devices raises legitimate concerns regarding security and privacy, necessitating the implementation of robust measures to mitigate risks and safeguard sensitive data.

3. Security background, terminology, and objectives

In the perspective of IoT security, several key objectives play a crucial role in safeguarding IoT devices and systems. These objectives include integrity, authentication, confidentiality, privacy, availability, authorization, non-repudiation, identification, reliability, freshness, access control methods, and soundness. Ensuring data integrity is essential to prevent unauthorized modification or destruction of data during transmission, storage, and processing. Authentication and authorization are crucial in verifying the identities of entities within the IoT system and ensuring that they have the appropriate permissions to access resources. Confidentiality protects sensitive information from unauthorized disclosure, both during transference and storage. Privacy becomes a significant concern in handling and processing data, ensuring that the

rights of individuals regarding the use of personal information are respected. Availability focuses on the system's operational state and capability to deliver required services. Additionally, non-repudiation prevents entities from denying their actions, enabling the resolution of potential conflicts within the system. These security objectives highlight the comprehensive measures required to address the unique challenges and vulnerabilities posed by IoT systems. Table 3 provides an overview of IoT security objectives, corresponding attack types, and anomaly detection techniques. It offers insights into the layers involved, ML methods utilized, detection accuracy, datasets used, and relevant references for further exploration. Incorporating quantitative analysis into our research on IoT security was crucial to providing a data-driven and objective assessment of the identified vulnerabilities and potential solutions. By utilizing a relevant dataset encompassing various aspects of IoT security, such as the frequency and types of cyber-attacks, the effectiveness of different cryptographic algorithms, and the performance of existing security protocols, we could derive valuable insights and meaningful conclusions. This quantitative analysis enabled us to measure the impact and significance of security measures, identify trends and patterns in cyber-attacks, and assess the overall effectiveness of IoT security strategies.

Table 4 consolidates and expands crucial information on ML models employed in the context of IoT security for detecting and mitigating cyber-attacks. It is evident that the ML models leverage various techniques like anomaly detection, behavior analysis, pattern recognition, and signature-based detection to identify and classify abnormal activities and malicious patterns within the IoT environment. The advantages of these models include high accuracy, real-time detection, scalability, and adaptability to evolving attack patterns. However, they also face challenges such as false positives, computational complexity, dataset requirements, and susceptibility to adversarial attacks.

3.1. Machine learning for IoT security

In reference to Tables 3 and 4, the machine learning and deep learning techniques, derived from artificial intelligence, play a vital role in detecting malware and malevolent network traffic within IoT systems. Traditional attack discovery systems rely on predefined strategies and feature sets to identify and classify network attacks, resulting in limitations when it comes to detecting new attack types and being restricted to specific

Table 2. Analysis of keywords in primary studies.

Keywords	Count	Keywords	Count
Internet of Things (IoT)	724	Cyber-attacks	609
Wireless Sensor Networks (WSNs)	427	Denial-of-Service (DoS)	578
Secure Routing	255	Trustworthiness	651
Edge Computing	310	Cloud Computing	318
Scalability	645	Machine Learning	595
Artificial Intelligence	607	Deep Learning	487
Neural Networks	496	Supervised Learning	477
Unsupervised Learning	545	Reinforcement Learning	268
Dimensionality Reduction	271	Feature Extraction	542
Transfer Learning	732	Model Selection & Evaluation	445
Autoencoder	273	Ensemble Learning	257
Convolutional Neural Networks	335	Adversarial Networks	620
Data Augmentation	421	Active Learning	715
Anomaly Detection	732	Semi-Supervised Learning	319
Lightweight Cryptography	246	Encryption and Decryption	715
Authentication	543	Key Exchange	615
Secure Communication	677	Resource-Constrained Devices	609
Energy Efficiency	405	Memory Efficiency	307
Hardware & Software Implementation	246	Lightweight Authentication Protocol	294
Resistance to Differential Power Analysis (DPA)	212	Performance Analysis of Lightweight Cryptographic Algorithms	215
Blockchain	725	Distributed Ledger	494
Consensus Mechanisms	483	Decentralization	357
Peer-to-Peer (P2P) Network	570	Immutable	369
Transparency	231	Private/Public/Permissioned Blockchain	699
Proof of Work (PoW)	377	Proof of Stake (PoS)	573
Proof of Authority (PoA)	716	Byzantine Fault Tolerance (BFT)	287
Scalability	398	Interoperability	624
Cross-Chain Communication	606	Zero-Knowledge Proofs	501
Blockchain Governance	316	Blockchain Intermediaries	492
Consensus Algorithms	547	Blockchain Adoption	623
Blockchain IoT Security Use Cases	298	Applied Protocols	674

scenarios [14]. However, this limitation can be overcome by employing ML algorithms that learn from previous experiences rather than relying on predetermined rules. Recent research [4,8,11−13] has successfully applied and supported the efficacy of ML algorithms in bolstering IoT security. These studies demonstrate that machine learning algorithms can adapt to the dynamic behaviors of IoT
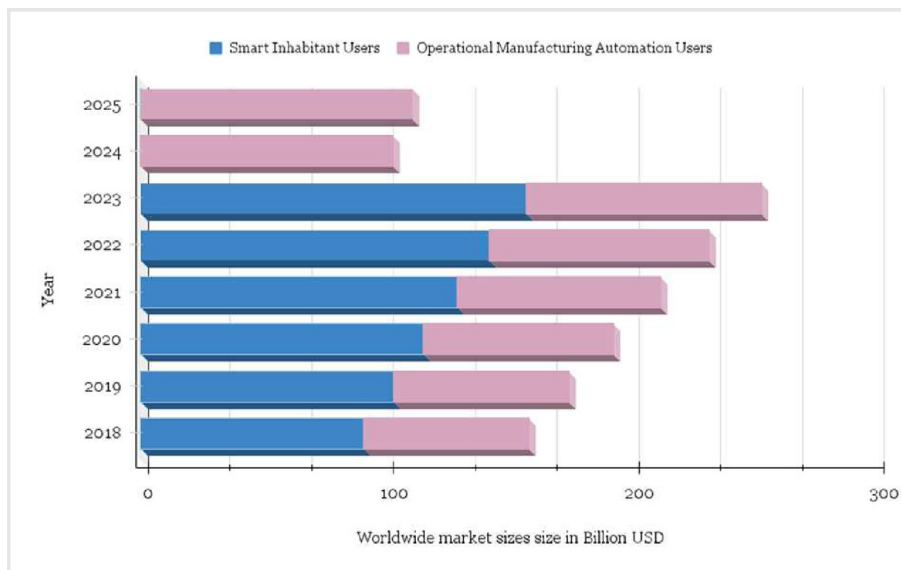

Fig. 2. IoT market size (year 2018−2025).

systems without compelling manual intrusion. By continuously monitoring network behavior, machine learning algorithms can swiftly detect various IoT attacks at an early stage, making them well-suited for IoT devices with limited resources.

3.1.1. Supervised ML

Supervised ML algorithms play a crucial role in accomplishing specific tasks by training ML models using a learning procedure and a training dataset. These algorithms classify the output based on the acquired training knowledge. Supervised learning involves two primary processes: classification and regression. Classification algorithms excel in categorizing output based on input data, enabling tasks such as determining the authenticity of information or distinguishing between real and fake entities. Prominent supervised ML classifiers include Support Vector Machine (SVM) [15], Naive Bayes (NB) [16], K-Nearest Neighbor (KNN) [17], and Random Forest (RF) [18]. SVM, for example, has gained significant adoption in the field of IoT security, effectively classifying diverse attacks such as DoS/DDoS, privacy fortification, IoT botnet recognition, and encoding attacks. Although SVM demonstrates high classification accuracy, it has limitations, such as a propensity for over-generalization, deliberate convergence rapidity, and sensitivity to local extrema.

Another widely used supervised ML-based classification algorithm in IoT security is Random Forest (RF). RF constructs a collection of decision trees, and the classification and prediction accuracy improve as the number of trees in the model increases. RF has been successfully employed in various IoT security tasks, including irregularity recognition, user to root intrusion detection, and remote to local risk strike discovery. Nevertheless, it is important to note that exceeding a certain number of trees can adversely impact RF's performance, rendering it slower and less suitable for real-time classification operations. The K-Nearest Neighbor (KNN) algorithm calculates the Euclidean distance between nodes, allowing the prediction of unknown nodes based on the average value of their k-nearest neighbors. In IoT applications, KNN has found utility in tasks such as malware detection, anomaly detection, and intrusion detection. Although KNN offers advantages in terms of ease, cost-efficacy, and compliant execution, its performance may be compromised with larger datasets, and it proves to be overly vulnerable to outliers and overlooked values.

Regression algorithms, including Decision Trees (DTs) [19], Linear Regression (LR) [20], and Neural Networks (NNs) [21], play a vital role in investigating relationships between independent features

Table 3. IoT security objectives and anomaly detection techniques.

Security Objectives [5]	Layer [7]	Anomaly and Attacks	Attack Type	Anomaly Detection	ML Method to Detect Anomaly [8]	Detection Accuracy	Dataset
Integrity	Application	Data modification	Active	Statistical analysis	Support Vector Machines	95%	IoT-23 [9]
Authentication	Network	Unauthorized access	Active	Rule-based analysis	Decision Trees	90%	–
Confidentiality	Perception	Eavesdropping	Passive	Encryption analysis	Neural Networks	92%	CIC IoT Dataset 2022 [10]
Privacy	Sensing	Data leakage	Passive	Behavior-based analysis	Random Forest	88%	
Availability	Application	Denial of Service	Active	Traffic analysis	K-nearest neighbors	96%	–
Authorization	Network	Unauthorized resource access	Active	Role-based analysis	Naive Bayes	87%	–
Non-repudiation	Application	Transaction dispute	Passive	Signature analysis	Hidden Markov Models	93%	IoT-23 [9]
Identification	Perception	Device spoofing	Active	Pattern recognition	Convolutional Neural Networks	91%	–
Reliability	Sensing	Data corruption	Active	Outlier analysis	Isolation Forest	94%	–
Freshness	Network	Replay attack	Passive	Time-stamp analysis	Long Short-Term Memory	89%	–
Access Control Methods	Application	Unauthorized privilege escalation	Active	Rule-based analysis	Decision Trees	90%	–
Soundness	Perception	Impersonation attack	Active	Behavioral profiling	Support Vector Machines	93%	IoT-23 [9]

Table 4. IoT cyber attack detection and mitigation with machine learning models.

IoT Cyber Attack Type [5]	ML Model Name [11−13]	Category	Brief Description	Detection Mechanism	Advantages	Disadvantages and Limitations
Denial of Service (DoS)	LSTM-based Classifier	Anomaly Detection	Long Short-Term Memory (LSTM) model to detect DoS attacks	Analyzes network traffic patterns and behavior anomalies	Ability to capture sequential dependencies in data, high detection accuracy	May require large amounts of training data, potential false positives/ negatives
Man-in-the-Middle (MitM)	Random Forest (RF)	Supervised Learning	RF classifier to identify and prevent MitM attacks	Analyzes network traffic and identifies suspicious activities	High accuracy, can handle large feature spaces, interpretability	Limited in handling dynamic or evolving attack patterns, may require frequent retraining
Device Spoofing	Support Vector Machine (SVM)	Supervised Learning	SVM model for detecting device spoofing based on behavioral analysis	Analyzes device behavior and compares with known patterns	Can handle complex feature spaces, good generalization capability	Vulnerable to noise in training data, may struggle with detecting sophisticated spoofing techniques
Data Tampering	Deep Belief Networks (DBN)	Unsupervised Learning	DBN model for detecting anomalies and identifying data tampering	Compares data patterns and identifies deviations	Good at detecting unknown attacks, can handle complex data structures	Requires significant computational resources, may have high training time and complexity
Eavesdropping	Convolutional Neural Network (CNN)	Deep Learning	CNN-based model to detect eavesdropping by analyzing network traffic	Extracts features from network data and detects anomalies	Effective in capturing spatial patterns, high detection accuracy	Requires large, labeled datasets, may struggle with detecting advanced eavesdropping techniques
Replay Attacks	Recurrent Neural Network (RNN)	Deep Learning	RNN-based model to detect and prevent replay attacks	Analyzes message timestamps and detects replayed messages	Can capture temporal dependencies, effective in detecting repeated message patterns	Reliance on accurate timestamp synchronization, may require continuous monitoring and synchronization of devices
Malware Injection	Decision Tree	Supervised Learning	Decision tree model for identifying and blocking malware injection	Analyzes network traffic and identifies malicious patterns	Interpretable model, can handle both numeric and categorical data, relatively low computational requirements	May struggle with complex data relationships, may have limitations in handling unknown or evolving malware variants
Insider Threats	Recurrent Neural Network (RNN)	Deep Learning	RNN model to detect anomalous behavior and identify insider threats	Analyzes user activity patterns and identifies anomalies	Ability to capture sequential dependencies, effective in detecting subtle insider behavior	Dependence on accurate and representative training data, may require continuous monitoring and profiling of user behavior

Table 4. (continued)

IoT Cyber Attack Type [5]	ML Model Name [11–13]	Category	Brief Description	Detection Mechanism	Advantages	Disadvantages and Limitations
Physical Attacks	Support Vector Machine (SVM)	Supervised Learning	SVM model for detecting physical attacks on IoT devices	Analyzes sensor data and identifies abnormal physical events	Ability to handle complex feature spaces, good generalization capability	Limited by the availability of labeled physical attack data, may require fine-tuning for specific physical attack scenarios
Traffic Manipulation	Deep Reinforcement Learning (DRL)	Reinforcement Learning	DRL-based model for detecting and mitigating traffic manipulation	Analyzes network traffic and learns optimal defensive strategies	Adaptive and self-learning model, can respond to changing attack patterns	High computational requirements, complex training process, potential for suboptimal policy convergence

and dependent variables for predictive modeling. DTs utilize simple decision rules derived from extracted features to predict target variable values but are prone to instability and struggle with continuous variables. LR models estimate accurate constraints by minimizing the error between predicted and actual values, yet they are sensitive to outliers and assume linear relationships. NNs, inspired by human intelligence, control complex and nonlinear information efficiently, but their computational complexity poses challenges for implementation in resource-constrained IoT systems. To overcome limitations, Ensemble Learning (EL) [22] combines multiple algorithms to improve performance, making it a valuable tool for complex IoT problems such as network monitoring, attack detection, and anomaly detection. Careful consideration of model selection, optimization techniques, and ensemble strategies is necessary to harness the potential of these algorithms in IoT applications.

3.1.2. Unsupervised ML algorithms

Unsupervised ML algorithms can realize hidden models and examine unlabeled datasets without relying on training data. By evaluating relationships between dataset models and input variables, these algorithms group samples into clusters, thus enhancing the discretion and protection of IoT devices. Among the extensively sourced unsupervised ML procedures, K-means [23] effectively clusters objects into distinct groups based on their nearest mean, making it suitable for IoT systems. Principal Component Analysis (PCA) [24] serves as a dimensionality reduction technique, improving computational speed and feature selection for attack detection in IoT, although it assumes linearity and is sensitive to outliers. Hierarchical clustering [25] creates a hierarchy of clustered data samples, eliminating the need for a predefined number of clusters, but it struggles with mixed data types and large-scale datasets. Fuzzy K-means Clustering (FCM) [26] utilizes fuzzy logic to assign data points probabilities for cluster membership, offering a more flexible approach than traditional clustering techniques. Gaussian Mixture Models (GMMs) [27] assume that data models are spawned from a mixture of Gaussian distributions, employing a probabilistic methodology for soft clustering, where each cluster corresponds to a probability distribution in a multidimensional space.

3.1.3. Reinforcement learning (RL)

RL algorithms enable autonomous learning and decision-making in systems through interaction with the environment. The incorporation of Quality-learning mechanisms [28] (i.e., Distributed Q-

learning, Double Q Network, Dueling Q Network (DQN), etc.) in RL models allows for automatic decision-making without prior knowledge. RL operates dynamically, employing a trial-and-error approach to identify optimal actions for maximizing rewards. RL algorithms, such as Quality-learning and Deep Quality Network (DQN) [29], are utilized for security attack detection in IoT systems. These RL algorithms address limitations in conventional ML techniques, including high computational time, large parameter requirements, lower accuracy, and the inability to oversee complex problems. Conversely, RL encounters challenges associated with computational overload due to the significant amount of data required for computation.

3.1.4. Future directions for utilizing ML in anomaly detection

This section addresses the existing research gap by presenting potential areas of further investigation, focusing on enhancing the intelligence and dynamism of protocols by utilizing ML techniques.

(a) In the context of anomaly detection in IoT, future research should focus on developing ML models that are explainable and interpretable. This will enable stakeholders to understand the underlying reasons for anomaly detections and build trust in the system. Techniques such as rule extraction, feature importance analysis, and model visualization can be explored to provide meaningful explanations for anomaly predictions.

(b) As IoT systems become more vulnerable to adversarial attacks, potential research should investigate the application of adversarial ML techniques for robust anomaly detection. Adversarial training, defensive distillation, and anomaly detection in adversarial settings are potential research directions to enhance the resilience of ML-based anomaly detection models against sophisticated attacks.

(c) With the continuous stream of data produced by IoT devices, there is a need for real-time anomaly detection techniques. Imminent research should explore ML algorithms and frameworks that can handle high-velocity data streams and detect anomalies in real-time. Incremental learning, adaptive models, and online feature selection methods are potential approaches to address the challenges of online and streaming anomaly detection.

(d) Preserving data privacy is critical in IoT environments. Forthcoming research should focus on developing privacy-preserving ML techniques for anomaly detection in IoT. Reliable multi-party data processing, homomorphic encoding, and federated learning approaches can enable anomaly detection while ensuring data privacy and compliance with privacy regulations.

(e) IoT devices repeatedly have inadequate computational resources and energy constraints. Future research should focus on developing ML models and algorithms that are lightweight and energy-efficient, enabling anomaly detection directly on resource-constrained devices. Model compression, quantization, and knowledge distillation techniques can be explored to reduce the computational and memory requirements of ML models deployed on IoT devices.

Table 5 supports a structured and broad assessment of projected research and previously conducted surveys on cyber-attack detection using ML in the IoT network. Applied and considered terminologies are explained as follow.

i. 'Structured' indicates that the assessments and comparisons are presented in a well-organized and coherent format, making it easier to understand and analyze the information.

ii. 'Pros/Cons' highlight the advantages and weaknesses of the research and surveys that furnish a balanced view by discussing both the positive aspects and potential limitations of the approaches taken.

iii. 'Disparaging' suggests that certain assessments or comparisons in the survey might be critical or unfavorable in nature. It implies that there may be findings that are less favorable or that highlight shortcomings in the research or survey methodologies.

iv. 'Assessment' examines the procedure of evaluating or analyzing the research and survey that involves forming judgments, identifying patterns, and drawing conclusions based on the collected information.

v. 'Coverage of Other Technique' assesses the extent to which the research and surveys have explored and considered various techniques other than ML for detecting cyber-attacks in IoT networks.

vi. 'Technical Difficulty' indicates the degree of expertise and resources required to successfully apply evaluated techniques in real-world scenarios.

vii. 'Performance Comparison' involves comparing and evaluating the effectiveness and efficiency of different ML procedures in distinguishing cyber-attacks in IoT networks.

It focuses on measuring and analyzing factors such as accuracy, speed, false positives, and false negatives to determine the performance levels of various approaches.

3.2. Confidentiality in IoT

The purpose of cryptography in IoT security is to protect sensitive information from unauthorized access, interception, and tampering. By employing encryption algorithms, data can be transformed into ciphertext, making it unreadable to adversaries without the corresponding decryption key. This ensures confidentiality, preventing unauthorized entities from extracting meaningful information from intercepted data. In this context, the performance assessment of lightweight cryptographic algorithms is of utmost importance to determine their suitability for secure communication in IoT environments. Factors such as encryption type, signature schemes, communication latency, gate density, power consumption, and microcontroller platform significantly impact the overall performance and resource utilization. Additional look after features for adopting a suitable encoding algorithm are as follows [38−45].

a) The frequency of operation directly affects the processing speed, with higher frequencies enabling faster encryption and decryption operations.
b) The available RAM and ROM in kilobytes (kB) play a vital role in determining the memory requirements of cryptographic algorithms.
c) Power consumption, measured in milliamperes (mA), is a crucial consideration due to the limited power resources in IoT devices.
d) The choice of encryption algorithm, along with the key size, block size, and number of rounds, determines the cryptographic strength and efficiency.
e) The selection of an appropriate cipher and network type ensures secure communication and compatibility with IoT protocols.
f) Cyphering throughput, measured in megabits per second (Mbps), indicates the data processing speed, while latency in cycles reflects the responsiveness and real-time capabilities of IoT systems.

The evaluation of encryption features (i.e., illustrated in Table 6) provides insights into the practical applicability of lightweight cryptographic algorithms for securing IoT networks.

Table 5. Comparative representation of assessment between projected research and previously conducted surveys on cyber-attack detection in the IoT network utilizing ML techniques.

Survey	Year	Structured	Pros./Cons.	Disparaging Assessment	Coverage of Other Techniques	Technical Difficulty	Performance Comparison	Similar Research[a]
Projected Survey	2023	✓	✓	✓	✓	✓	✓	Not Available
[30]	2022	✓	×	✓	✓	×	×	11 papers (From 1989 to 2022)
[31]	2021	✓	✓	×	✓	×	×	1335 Papers (From 2000 to 2021)
[32]	2022	✓	✓	✓	×	×	✓	776 Papers (From 1983 to 2022)
[33]	2022	✓	×	✓	✓	×	×	291 Papers (From 1998 to 2022)
[34]	2021	✓	×	✓	×	✓	×	1057 Papers (From 2009 to 2021)
[35]	2021	×	×	✓	✓	×	×	971 Papers (From 2000 to 2021)
[36]	2023	✓	×	✓	✓	×	×	228 Papers (From 2000 to 2007)
[37]	2023	✓	×	×	×	×	×	Not Available

3.2.1. Quantum Crypto Physical Unclonable Functions (QC-PUF)

QC-PUF combines the principles of quantum cryptography and physical unclonable functions to enhance the security of cryptographic systems. PUFs exploit the inherent variations in hardware devices to generate unique cryptographic keys. In the context of quantum cryptography, PUFs can be used to generate and store quantum keys, providing a higher level of security against attacks.

In a Quantum Crypto PUF system, the bit pattern for plain text and ciphered data can be determined by the encryption algorithm used. The encryption algorithm operates on the plain text data using the cryptographic key, resulting in ciphered data. The key bits, generated by the PUFs, serve as the input for the encryption algorithm, ensuring the uniqueness and security of the key.

Key exchange criteria in Quantum Crypto PUFs involve securely exchanging the cryptographic keys between communicating parties. This can be achieved through protocols like Quantum Key Distribution (QKD) that utilize quantum properties to establish secure key exchange. The number of cryptographic rounds depends on the specific implementation and security requirements, ensuring the desired level of encryption strength.

In terms of infrastructure limitations for IoT, the use of Quantum Crypto PUFs faces challenges such as limited distance for transmitting photons, the need for specialized quantum devices that may be bulky and expensive, and scalability concerns when dealing with large-scale IoT networks. Yet, advancements in technology and research aim to address these limitations and enable the practical implementation of Quantum Crypto PUFs in IoT environments.

Nevertheless, by leveraging the inherent variations in hardware devices and incorporating quantum cryptographic principles, QC-PUFs enhance the resilience of cryptographic systems in Industrial IoT and IoMT, mitigating the risks associated with unauthorized access, data breaches, and tampering. This advanced security measure contributes to safeguarding critical industrial processes, sensitive medical data, and the integrity of interconnected devices in these evolving and interconnected ecosystems.

3.2.1.1. Novel technical considerations for QC-PUFs implementation.
We have encountered the following considerations while investigating the QC-PUF.

a) QC-PUF solutions need to be designed to seamlessly integrate with diverse IoT, IIoT, and IoMT hardware platforms. Factors such as

Table 6. Comparative analysis of cryptographic algorithms for IoT devices.

Lightweight Encryption Algorithm	Gate Density (kGEs/mm)	Power Consumption (nW/MHz/GE)	Microcontroller Platform	Frequency (MHz)	RAM (kB)	ROM (kB)	Power (mA)	Key Size, Block Size	Rounds	Throughput (Mbps)	Latency (Cycle)
GRAIN-128-AEADv2 [38]	5.2	40	Raspberry Pi 4	1500	4096	4096	650	128 bits	12	200	1000
PHOTON-beetle [39]	7.8	30	Arduino Uno	16	2	32	20	128 bits	12	10	100
FPGA Romulus [40]	4.6	35	ESP32	240	520	4096	80	128 bits	10	80	200
Sparkle [41]	8.3	45	BeagleBone Black	1	512	4096	200	128 bits	16	500	500
TinyJambu [42]	3.9	25	Particle Photon	120	128	128	70	128 bits	12	50	500
Ascon [43]	5.1	35	NVIDIA Jetson Nano	1600	8192	8192	1200	128 bits	12	600	800
GIFT-COFB [44]	4.8	40	Intel Edison	500	1024	4096	150	128 bits	12	400	300
Grain-128AEADv2 [45]	5.2	40	Particle Argon	120	256	4096	100	128 bits	12	300	400
SPARKLE-PIC32 [41]	8.3	45	Microchip PIC32	80	128	512	50	128 bits	16	100	1000

limited resources, low power consumption, and compatibility with various microcontroller architectures must be considered to ensure efficient and practical deployment.

b) To establish secure communication channels, post-quantum key exchange protocols should be implemented. These protocols address the vulnerability of classical cryptographic protocols to quantum attacks and guarantee the confidentiality and authenticity of data transmitted between devices.

c) The physical limitations of IoT, IIoT, and IoMT devices must be considered, including processing capabilities, memory constraints, and energy resources. Lightweight and efficient QC-PUF implementations are necessary to minimize computational overhead and power consumption while maintaining adequate security measures.

d) Environmental factors, such as temperature variations, electromagnetic interference, and physical vibrations, can affect the performance and reliability of QC-PUF enabled devices. Robust designs that account for these factors is essential to ensure consistent operation in real-world deployment scenarios.

e) Comprehensive lifecycle management strategies for QC-PUF qualified devices are vital for secure key generation, distribution, storage, rotation, and revocation processes. These strategies ensure the efficient management of cryptographic keys throughout the device lifecycle, minimizing the risk of key compromise.

3.2.2. Correlation of ML with lightweight cryptography

Machine learning modeling is crucial in fortifying the IoT against crippling cyber-attacks by collaborating with cryptographic implementation. ML algorithms provide powerful capabilities for data analysis, pattern recognition, and anomaly detection, which are vital in identifying and mitigating security threats. By integrating ML algorithms with lightweight cryptographic techniques, IoT systems can benefit from enhanced threat detection, robust authentication mechanisms, and secure communication protocols. ML algorithms contribute to the overall defense of IoT against cyber-attacks by strengthening key management, facilitating real-time threat monitoring, and enabling proactive security measures. The correlation between ML and cryptographic algorithms forms a comprehensive approach to strengthen IoT devices and networks, ensuring resilience and safeguarding against evolving threats.

Here it is worth highlighting that the centralized nature of IoT systems poses vulnerabilities such as data tampering, unauthorized access, and single points of failure. These challenges can be effectively addressed by leveraging Blockchain (BC) technology, which provides decentralized consensus, immutability, and transparency, ensuring a robust and secure IoT ecosystem. Likewise, by leveraging ML algorithms, the blockchain can analyze massive amounts of IoT data, detect anomalies, and identify potential security threats in real-time. Lightweight cryptography ensures efficient and secure communication between IoT devices, while the blockchain acts as a trusted distributed ledger, facilitating secure data sharing and authentication. The need for blockchain in IoT lies in its ability to establish a decentralized and tamper-resistant infrastructure, ensuring data integrity, privacy, and resilience against sophisticated cyber-attacks, ultimately fortifying IoT ecosystems.

3.3. Blockchain solution for IoT security

Literature review assessment [46−51] revealed that the Blockchain, whether it is implemented as a private, public, or federated network, plays a crucial role in strengthening IoT against anomalous cyber-attacks (i.e., illustrated in Table 7). By granting a dispersed and absolute ledger, blockchain ensures the integrity and transparency of IoT transactions and data. Cryptological algorithms and consensus procedures establish trust and enhance security, making it exceptionally complicated for malicious actors to fiddle with or compromise IoT devices and their associated data.

The blockchain paradigm utilizes cryptographic hash functions to calculate the data hash, providing a unique digital fingerprint. This hash, along with other transaction details, is stored in blocks, forming a chain. The blockchain's decentralized nature and consensus mechanisms make it particularly tough for adversary to alter or manipulate data stored on the BC, ensuring data authentication and integrity. A block in the BC comprises of a list of transactions that record data exchanges between IoT devices. The impact of blockchain on secure communication protocols like Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), or Extensible Messaging and Presence Protocol (XMPP) lies in providing an additional layer of security and trust through the decentralized nature of the blockchain, ensuring secure and reliable data transmission. Similarly, blockchain can impact IoT-specific routing protocols by enhancing the security, privacy, and reliability of data routing within IoT networks.

Considering IoT device resource constraints, blockchain functionality can be tailored to accommodate heterogeneous devices by employing lightweight consensus algorithms, optimizing data storage & processing, and leveraging off-chain solutions to minimize resource consumption while maintaining the core benefits of blockchain technology.

3.3.1. Challenges of blockchain

Integrating Blockchain technology into IoT presents domain-specific challenges. Table 8 outlines technical challenges and corresponding solutions.

3.3.1.1. Scalability limitations of blockchain.

The scalability limitations of blockchain technology in large-scale IoT networks present considerable challenges in ensuring efficient and reliable transaction processing. As the number of IoT devices and transactions increases, network congestion becomes a significant concern, leading to delays and increased transaction fees. The transaction throughput of traditional blockchain networks, such as Bitcoin and Ethereum, is limited, making it difficult to handle the vast number of transactions generated by IoT devices in real-time. Moreover, the consensus mechanisms employed in blockchain, such as Proof of Work (PoW) and Proof of Stake (PoS), can exacerbate scalability issues. PoW requires extensive computational resources, leading to slower transaction confirmation times, while PoS has its limitations in handling high transaction volumes. To address these challenges, various approaches are being explored, including sharding, sidechains, and off-chain processing. Sharding divides the blockchain network into smaller partitions, allowing parallel processing of transactions, while sidechains enable the execution of specific smart contracts off the main blockchain, reducing congestion. Off-chain processing moves non-critical transactions outside the main blockchain, alleviating the burden on the network. Achieving scalability in large-scale IoT blockchain networks requires a careful balance between transaction volume, consensus mechanisms, and innovative scaling solutions to ensure efficient and seamless data processing for IoT applications.

4. Ethical and legal considerations

Ethical considerations, privacy concerns, and legal frameworks play a pivotal role in shaping the

Table 7. Comprehensive Comparison of Public, Private, and Federated Blockchains for IoT Devices.

	Public [47]	Private [48]	Federated [49,50]
Access	Publicly accessible to any IoT entity	Restricted access to authorized entities	Restricted access to a group of trusted entities
Speed	Moderate to Slow	Fast	Fast
Efficiency	Moderate to Low	High	High
Security	High	High	High
Immutability	Immutable once confirmed	Immutable once confirmed	Immutable once confirmed
Consensus Process	Decentralized consensus	Permissioned consensus	Permissioned consensus
Consensus Mechanism	Proof of Work, Proof of Stake (Ethereum)	Various (e.g., Practical Byzantine Fault Tolerance, Raft)	Various (e.g., Federated Byzantine Agreement)
Network Type	Publicly shared network	Private or consortium network	Private or consortium network
Open Source	Yes	Yes	Yes
Smart Contracts Type	Turing Complete (Ethereum)	Turing Complete (Hyperledger Fabric)	Turing Complete (Multichain)
Particular Hardware Requisite	High computational power required	No specific requirements	No specific requirements
Avg. Transactions per Second	Varies (e.g., Ethereum: 15 TPS)	Varies (depends on network infrastructure)	Varies (depends on network infrastructure)
Hashing Algorithm	Various (e.g., SHA-256, Ethash)	Various (e.g., SHA-256, SHA-3)	Various (e.g., SHA-256, SHA-3)
Key Administration	Yes (through public-private key pairs)	Yes (through access controls)	Yes (through access controls)
Data Confidentiality	No (Transparent)	Yes	Yes
Scalability	Limited	Flexible	Flexible
Governance	Decentralized	Centralized	Consortium-based
Customization	Limited	High	High
Network Overhead	Higher	Lower	Lower
Interoperability	Limited	Limited	Limited
Cost Competence	Lower	Higher	Higher

landscape of IoT security. As IoT devices become more pervasive in our daily lives and critical infrastructure, safeguarding user privacy and adhering to ethical principles becomes paramount. The collection, storage, and processing of vast amounts of personal data by IoT devices raise significant ethical concerns regarding consent, data ownership, and potential misuse. Addressing these issues requires robust technical solutions that prioritize data protection and user control over their information. Implementing privacy by design principles, encryption, and secure data transmission protocols can help mitigate privacy risks and ensure data confidentiality.

In addition to technical measures, adhering to legal frameworks is essential to establish clear guidelines and responsibilities for all stakeholders involved in the IoT ecosystem. Compliance with existing data protection regulations, such as the General Data Protection Regulation (GDPR) and HIPPA, ensures that user data is handled lawfully and transparently. Legislative bodies worldwide must work collaboratively to create comprehensive and adaptive IoT-specific regulations to address emerging challenges. These legal frameworks must encompass device security standards, data breach notification requirements, and liability allocation to promote accountability among IoT manufacturers, service providers, and users. Moreover, ethical considerations extend beyond data privacy to encompass the potential societal impact of IoT technologies. Striking a balance between innovation and ethical use is crucial to prevent unintended consequences and potential harm. Robust risk assessment and ethical impact assessments should be integrated into the development and deployment of IoT systems. Responsible innovation in IoT security involves not only technical expertise but also a deep understanding of ethical principles, user perspectives, and social implications. By addressing ethical considerations, privacy concerns, and legal frameworks, the IoT security community can pave the way for a safer, more secure, and ethically conscious IoT ecosystem.

5. Key applicable recommendations

A rigorous review of survey analysis triggered the following recommendations to nominate lightweight, scalable, and effective cyber-shield in IoT cyber-defense.

a) Robust device authentication mechanisms, such as X.509 certificates and mutual authentication protocols like EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), help prevent unauthorized access to IoT devices. Implementing strong authentication mitigates the risk of impersonation attacks.

b) Deploying protocols like MQTT with TLS for end-to-end encrypted communication ensures the confidentiality and integrity of data exchanged between IoT devices and the server. Proper protocol selection and configuration are crucial for secure IoT communication.

c) Establishing a well-defined process for timely security updates and patches, following standards like ISO/IEC 27001, and leveraging vulnerability management frameworks like CVSS (Common Vulnerability Scoring System), ensures that known vulnerabilities are promptly addressed and reduces the likelihood of successful attacks.

d) Employing network segmentation using VLANs (Virtual Local Area Networks) or SDN (Software-Defined Networking) techniques helps isolate IoT devices into separate security zones, limiting the lateral movement of threats and minimizing the potential impact of attacks.

e) Employing security information and event management (SIEM) algorithms integrated with threat intelligence feeds, such as STIX/TAXII (Structured Threat Information Expression/ Trusted Automated Exchange of Indicator Information), facilitates proactive monitoring, timely incident detection, and response to emerging threats.

f) Employing techniques such as data-at-rest encryption, using algorithms like XTS-AES (XEX-based Tweaked CodeBook Mode with Cipher-Text Stealing and Advanced Encryption Standard), and secure protocols like HTTPS (Hypertext Transfer Protocol Secure) or SFTP (Secure File Transfer Protocol), ensures data confidentiality and integrity throughout its lifecycle.

g) Exploring the integration of blockchain technology, such as Ethereum or Hyperledger Fabric, in IoT infrastructure enhances security, transparency, and trust among participants. Employing smart contracts and distributed ledger technology ensures tamper-resistant data integrity, decentralized consensus, and auditable transactions.

h) Considering the future threat of quantum computers, exploring post-quantum cryptographic algorithms like lattice-based or code-based cryptography, along with physical unclonable functions (PUFs) for device authentication, enhances the resistance of IoT infrastructure against potential quantum-based attacks.

Table 8. The Integration of Blockchain Technology in IoT: Addressing Multi-Domain Challenges and Solutions.

BC Challenges	Description	Solution	Hindrance Issues	Applied Technologies and Protocols	Ref.
Interoperability	Ensuring seamless integration and compatibility between heterogeneous IoT devices and Blockchain networks	Standardized data formats and protocols	Diverse device architectures and protocols	IoT protocols: MQTT, CoAP, HTTP	[52]
Scalability	Addressing the scalability limitations of Blockchain to accommodate the growing number of IoT devices	Sharding, sidechains, off-chain processing	Performance impact, network congestion	Sharding: Ethereum 2.0, Hyperledger Fabric	[53]
Privacy and Security	Protecting sensitive IoT data from unauthorized access, tampering, and privacy breaches	Cryptographic algorithms, access control	Privacy breaches, data leakage, key management	Encryption: AES, RSA; Access control: ACL, RBAC	[54]
Smart Contracts	Developing secure and efficient execution environments for automated transactions and agreements	Secure contract coding, auditing	Vulnerabilities, smart contract bugs	Ethereum Virtual Machine (EVM), Solidity	[55]
Power Consumption	Optimizing energy efficiency in IoT Blockchain networks to minimize power consumption	Energy-efficient consensus mechanisms	Limited device resources, battery life	Proof of Stake (PoS), Proof of Authority (PoA)	[56]
Protocol Standardization	Establishing standardized communication protocols, data formats, and interfaces for IoT-Blockchain integration	IoT protocol harmonization	Lack of consensus, compatibility challenges	IETF standards, ISO/IEC standards	[57]
Infrastructure Compatibility	Ensuring compatibility between Blockchain infrastructure and diverse IoT device architectures	Middleware solutions, IoT gateway integration	Resource constraints, connectivity limitations	MQTT brokers, IoT gateways, Blockchain APIs	[58]
Legal and Compliance	Addressing legal and regulatory frameworks for data protection, privacy, and cybersecurity in IoT-Blockchain	Compliance frameworks, regulatory guidelines	Jurisdictional issues, cross-border data transfers	GDPR, HIPAA, ISO/IEC standards	[59]
Security Attacks	Mitigating security threats such as Sybil attacks, 51% attacks, and double-spending attacks	Consensus mechanisms, Byzantine fault tolerance	Attack complexity, network vulnerability	Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT)	[60]
Trust Establishment	Establishing trust among IoT stakeholders through identity management and reputation systems	PKI, decentralized identity systems	Trustworthiness verification, identity theft	Blockchain-based identity solutions, DIDs	[61]

Table 8. (continued)

BC Challenges	Description	Solution	Hindrance Issues	Applied Technologies and Protocols	Ref.
Skyline Query Processing	Designing efficient techniques for processing complex queries on Blockchain data in real-time	Distributed query processing algorithms	Query complexity, real-time response requirements	Distributed databases, MapReduce algorithms	[62]
Decentralized Cooperation	Enabling collective decision-making, consensus, and governance in IoT-Blockchain ecosystems	Decentralized governance models	Governance conflicts, scalability challenges	DAO (Decentralized Autonomous Organization), Voting mechanisms	[63]
Consensus Protocol	Evaluating and selecting consensus protocols that meet IoT application requirements	Lightweight consensus algorithms	Scalability, latency, consensus fault tolerance	Proof of Stake (PoS), Delegated Proof of Stake (DPoS)	[64]
Big Data and Machine Learning	Integrating secure and privacy-preserving big data analytics and ML algorithms in IoT-Blockchain	Homomorphic encryption, federated learning	Data privacy, model accuracy, computational overhead	Secure Multiparty Computation (MPC), Differential Privacy	[65]
SDN and Cellular Network	Integrating Blockchain with SDN and cellular networks for enhanced security, scalability, and device management	Blockchain-based network management	Network interoperability, latency, network overhead	Software-Defined Networking (SDN), 5G, Cellular IoT protocols	[66]
Energy Management	Designing energy-efficient mechanisms and protocols for IoT devices in Blockchain networks	Low-power consensus algorithms	Limited device resources, energy consumption	Proof of Stake (PoS), Proof of Authority (PoA)	[60]

i) The emergence of quantum-based attacks poses significant implications for the security of IoT-driven blockchain systems. Traditional cryptographic algorithms, such as RSA and ECC, are vulnerable to being broken by powerful quantum computers, jeopardizing the confidentiality and integrity of data exchanged in blockchain networks. To address this threat, post-quantum cryptographic algorithms have been proposed and evaluated for their applicability in the context of IoT-driven blockchain. These algorithms, based on lattice-based cryptography, code-based cryptography, multivariate polynomials, and other mathematical structures, offer resistance against quantum attacks due to their underlying mathematical complexity. However, the adoption of post-quantum cryptographic algorithms in IoT-driven blockchain introduces challenges related to performance and resource constraints. The higher computational overhead and memory requirements of these algorithms must be carefully balanced with the limited processing capabilities and energy constraints of IoT devices. In addition, ensuring interoperability and compatibility with existing blockchain frameworks and smart contract execution environments becomes crucial to achieve seamless integration. Further research and empirical validation are required to determine the most suitable post-quantum cryptographic algorithms for IoT-driven blockchain, striking a balance between security, performance, and resource efficiency in the face of quantum-based threats.

j) Human behavior and user interactions with IoT devices play a significant role in introducing potential vulnerabilities (e.g., misconfiguration, insecure network connections, lack of device firmware updates, etc.) to IoT security.

Understanding the impact of human factors, usability considerations, and user-centric security design principles is crucial in addressing these risks effectively. User-centered approaches that prioritize intuitive interfaces, clear instructions, and simplified security measures can enhance the overall security posture of IoT devices. Moreover, incorporating user education and awareness programs can empower users to make informed security decisions and adopt safe practices while interacting with IoT technology. By emphasizing user-centric security measures, the IoT ecosystem can mitigate potential security risks and create a more resilient and secure environment for users and their interconnected devices.

6. Enhancements from existing reviews/surveys

This review paper distinguishes itself from related surveys/reviews [31,32],[34−37],[47],[59],[67,68] through its adoption of a comprehensive research method, which rigorously explores procedural approach 'Systematic Review'. Unlike conventional surveys, this review delves deeper into the literature on IoT security, offering a comprehensive understanding of the subject matter. It not only identifies the vulnerabilities, threats, and challenges posed by interconnected devices but also proposes a robust framework for vulnerability assessment and mitigation. Moreover, the paper critically evaluates the efficacy of existing security features and protocols, providing a thorough analysis of their strengths and limitations. It goes beyond mere summarization of findings and recommends the integration of innovative technologies like blockchain and machine learning algorithms to fortify IoT security. This comprehensive and well-rounded analysis ensures a reliable and authoritative approach to evidence synthesis in the ever-evolving domain of IoT security.

7. Conclusion and future work

The 21st century has witnessed the widespread adoption of IoT in various domains, including smart homes, industries, and healthcare facilities, bringing numerous benefits and advancements in efficiency, automation, and convenience. Nonetheless, the growing reliance on IoT infrastructure necessitates a robust security framework due to the inherent vulnerabilities and threats associated with interconnected devices. These include potential unauthorized access, data breaches, device manipulation, and network disruptions, emphasizing the criticality of implementing effective security measures. This research paper on IoT security review makes significant contributions by providing a comprehensive understanding of the existing literature, conducting a systematic survey to identify anomalies and risks, proposing a framework for vulnerability assessment and mitigation, and evaluating the effectiveness of current security features and protocols. While the paper offers valuable insights and recommendations, it is important to acknowledge some limitations. The presented systematic review may not encompass all possible security aspects, and the proposed enhancements to security mechanisms require further empirical validation to ensure their efficacy in real-world IoT environments.

Future work. To pave the way for future research, it is imperative to explore various avenues that can enhance IoT security beyond the existing capabilities. Firstly, investigating the integration of quantum systems, 6G, Federated Learning (FL), and artificial intelligence (AI) into IoT infrastructure holds promise in significantly enhancing data processing, privacy preservation, and overall security measures. Moreover, evaluating the potential benefits and feasibility of implementing Named Data Network (NDN) as an alternative to IP-based systems is crucial. NDN's inherent data-centric approach can potentially improve data integrity, confidentiality, and resilience in IoT environments, warranting further exploration and experimentation.

Likewise, to address the ever-evolving threat landscape, continuous monitoring, and adaptation to emerging security regulations and standards are essential. This involves actively staying abreast of evolving policies, industry guidelines, and best practices to ensure that IoT security measures remain effective and up to date. Ultimately, the exploration of novel cryptographic algorithms, lightweight authentication protocols, and secure firmware update mechanisms specifically designed for IoT devices should be researched and investigated to significantly enhance the IoT ecosystem's security posture.

Institutional review board statement

The study was conducted according to the guidelines of the Declaration of Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Saudi Arabia.

Informed consent statement

Not applicable.

Data availability statement

Not applicable.

Conflicts of interest

The authors declare no conflict of interest.

Acknowledgments

References

[1] S. Ashraf, A proactive role of IoT devices in building smart cities, Int. Things and Cyber-Physical Systems 1 (2021) 8—13, https://doi.org/10.1016/j.iotcps.2021.08.001.

[2] A.G. Silva-Trujillo, M.J. González González, L.P. Rocha Pérez, L.J. García Villalba, Cybersecurity analysis of wearable devices: smartwatches passive attack, Sensors 23 (2023) 1—18, https://doi.org/10.3390/s23125438.

[3] C. Bayõlmõş, M.A. Ebleme, Ü. Çavuşoğlu, K. Küçük, A. Sevin, A survey on communication protocols and performance evaluations for Internet of Things, Digital Communications and Networks 8 (2022) 1094—1104, https://doi.org/10.1016/j.dcan.2022.03.013.

[4] L.J.S. Kumar, P. Krishnan, B. Shreya, S. MS, Performance enhancement of FSO communication system using machine learning for 5G/6G and IoT applications, Optik 252 (2022) 1—9, https://doi.org/10.1016/j.ijleo.2021.168430.

[5] U. Tariq, I. Ahmed, A.K. Bashir, K. Shaukat, A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review, Sensors 23 (2023) 1—46, https://doi.org/10.3390/s23084117.

[6] N. Priya, Cybersecurity considerations for industrial IoT in critical infrastructure sector, Int. J. Comput. Organ. Trends 12 (2022) 27—36, https://doi.org/10.14445/22492593/ijcot-v12i1p306.

[7] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, B. Stiller, Landscape of IoT security, Computer Science Review 44 (2022) 1—18, https://doi.org/10.1016/j.cosrev.2022.100467.

[8] S. Fraihat, S. Makhadmeh, M. Awad, M.A. Al-Betar, A. Al-Redhaei, Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm, Internet of Things 22 (2023) 1—22, https://doi.org/10.1016/j.iot.2023.100819.

[9] S. Garcia, A. Parmisano, M.J. Erquiaga, IoT-23: a labeled dataset with malicious and benign IoT network traffic, Zenodo (2020), https://doi.org/10.5281/zenodo.4743746.

[10] S. Dadkhah, H. Mahdikhani, P.K. Danso, A. Zohourian, K.A. Truong, A.A. Ghorbani, Towards the development of a realistic multidimensional IoT profiling dataset, 19th annual international conference on privacy, Security & Trust (PST) (2022) 1—11, https://doi.org/10.1109/PST55820.2022.9851966.

[11] A. Pinto, L.-C. Herrera, Y. Donoso, J.A. Gutierrez, Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure, Sensors 23 (2023) 1—18, https://doi.org/10.3390/s23052415.

[12] M. Hasan, Md.M. Islam, M.I.I. Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things 7 (2019) 1—14, https://doi.org/10.1016/j.iot.2019.100059.

[13] K. He, D.D. Kim, M.R. Asghar, Adversarial machine learning for network intrusion detection systems: a comprehensive survey, IEEE Communications Surveys & Tutorials. 25 (2023) 538—566, https://doi.org/10.1109/comst.2022.3233793.

[14] V. Gugueoth, S. Safavat, S. Shetty, Security of Internet of Things (IoT) using federated learning and deep learning — recent advancements, issues and prospects, ICT Express 9 (2023) 1—20, https://doi.org/10.1016/j.icte.2023.03.006.

[15] M. Arunkumar, K.A. Kumar, GOSVM: gannet optimization-based support vector machine for malicious attack detection in cloud environment, Int. J. Inf. Technol. 15 (2023) 1653—1660, https://doi.org/10.1007/s41870-023-01192-z.

[16] R. Yadav, I. Sreedevi, D. Gupta, Augmentation in performance and security of WSNs for IoT applications using feature selection and classification techniques, Alex. Eng. J. 65 (2023) 461—473, https://doi.org/10.1016/j.aej.2022.10.033.

[17] M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour, An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection, Multimed. Tool. Appl. 82 (2023) 23615—23633, https://doi.org/10.1007/s11042-023-14795-2.

[18] J.B. Awotunde, F.E. Ayo, R. Panigrahi, A. Garg, A.K. Bhoi, P. Barsocchi, A multi-level random forest model-based intrusion detection using fuzzy inference system for internet of things networks, Int. J. Comput. Intell. Syst. 16 (2023) 1—22, https://doi.org/10.1007/s44196-023-00205-w.

[19] M. Douiba, S. Benkirane, A. Guezzaz, M. Azrour, An improved anomaly detection model for IoT security using decision tree and gradient boosting, J. Supercomput. 79 (2022) 3392—3411, https://doi.org/10.1007/s11227-022-04783-y.

[20] Y. Zhou, L. Song, Y. Liu, P. Vijayakumar, B.B. Gupta, W. Alhalabi, H. Alsharif, A privacy-preserving logistic regression-based diagnosis scheme for digital healthcare, Future Generat. Comput. Syst. 144 (2023) 63—73, https://doi.org/10.1016/j.future.2023.02.022.

[21] N.A. Bajao, J. Sarucam, Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units, Mesopotamian J. Cyber Security 2023 (2023) 22—29, https://doi.org/10.58496/mjcs/2023/005.

[22] O. Abu Alghanam, W. Almobaideen, M. Saadeh, O. Adwan, An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning, Expert Syst. Appl. 213 (2023) 1—16, https://doi.org/10.1016/j.eswa.2022.118745.

[23] L. Prathibha, K. Fatima, A novel high-speed data encryption scheme for internet of medical things using modified elliptic curve diffie—hellman and advance encryption standard, Int. J. Image Graph. 22 (2022) 1—15, https://doi.org/10.1142/s0219467823400041.

[24] M. Alhanaya, K. Hamdi Ateyeh Al-Shqeerat, Performance analysis of intrusion detection system in the IoT environment using feature selection technique, Intelligent Automation & Soft Computing 36 (2023) 3709—3724, https://doi.org/10.32604/iasc.2023.036856.

[25] M. Asad, M. Aslam, S.F. Jilani, S. Shaukat, M. Tsukada, SHFL: K-Anonymity-Based secure hierarchical federated learning framework for smart healthcare systems, Future Internet 14 (2022) 1—16, https://doi.org/10.3390/fi14110338.

[26] S.V.N. Santhosh Kumar, Y. Palanichamy, M. Selvi, S. Ganapathy, A. Kannan, S.P. Perumal, Energy efficient secured K means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks, Wireless Network 27 (2021) 3873—3894, https://doi.org/10.1007/s11276-021-02660-9.

[27] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, D. Miu, Detection of unknown DDoS attacks with deep learning and Gaussian mixture model, Appl. Sci. 11 (2021) 1—13, https://doi.org/10.3390/app11115213.

[28] G. Sharma, J. Grover, A. Verma, QSec-RPL: detection of version number attacks in RPL based mobile IoT using Q-Learning, Ad Hoc Netw. 142 (2023) 1—16, https://doi.org/10.1016/j.adhoc.2023.103118.

[29] X. Chen, X. Liu, Y. Chen, L. Jiao, G. Min, Deep Q-Network based resource allocation for UAV-assisted Ultra-Dense Networks, Comput. Network. 196 (2021) 1−10, https://doi.org/10.1016/j.comnet.2021.108249.

[30] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H.T. Mouftah, P. Djukic, Machine learning-enabled IoT security: open issues and challenges under advanced persistent threats, ACM Comput. Surv. 55 (2022) 1−37, https://doi.org/10.1145/3530812.

[31] R. Ahmad, I. Alsmadi, Machine learning approaches to IoT security: a systematic literature review, Internet of Things 14 (2021) 1−42, https://doi.org/10.1016/j.iot.2021.100365.

[32] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L.F. Capretz, S.J. Abdulkadir, Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review, Electronics 11 (2022) 1−27, https://doi.org/10.3390/electronics11020198.

[33] U. Inayat, M.F. Zia, S. Mahmood, H.M. Khalid, M. Benbouzid, Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects, Electronics 11 (2022) 1−20, https://doi.org/10.3390/electronics11091502.

[34] L. Aversano, M.L. Bernardi, M. Cimitile, R. Pecori, A systematic review on Deep Learning approaches for IoT security, Comput. Sci. Review 40 (2021) 1−18, https://doi.org/10.1016/j.cosrev.2021.100389.

[35] S.H. Haji, S.Y. Ameen, Attack and anomaly detection in IoT networks using machine learning techniques: a review, Asian J. Res. Comput. Sci. 9 (2021) 30−46, https://doi.org/10.9734/ajrcos/2021/v9i230218.

[36] A. Ahmed Jamal, A.-A. Mustafa Majid, A. Konev, T. Kosachenko, A. Shelupanov, A review on security analysis of cyber physical systems using Machine learning, Mater. Today: Proc. 80 (2023) 2302−2306, https://doi.org/10.1016/j.matpr.2021.06.320.

[37] L.G.F. da Silva, D.F.H. Sadok, P.T. Endo, Resource optimizing federated learning for use with IoT: a systematic review, J. Parallel Distr. Comput. 175 (2023) 92−108, https://doi.org/10.1016/j.jpdc.2023.01.006.

[38] B. Li, H. Zhang, D. Lin, Efficient (masked) hardware implementation of grain-128AEADv2, Secur. Commun. Network. 2023 (2023) 1−16, https://doi.org/10.1155/2023/8044164.

[39] A.T. Mozipo, J.M. Acken, Residual vulnerabilities to power side channel attacks of lightweight ciphers cryptography competition finalists, IET Comput. Digital Tech. 17 (2023) 1−14, https://doi.org/10.1049/cdt2.12057.

[40] S. Jin, W. Yuanzhi, S. Yining, Design and implementation of wireless multimedia sensor network node based on FPGA and binocular vision, EURASIP J. Wirel. Commun. Netw. 2018 (2018) 1−8, https://doi.org/10.1186/s13638-018-1172-8.

[41] C. Beierle, A. Biryukov, L. Cardoso dos Santos, J. Großschädl, L. Perrin, A. Udovenko, V. Velichkov, Q. Wang, Lightweight AEAD and hashing using the sparkle permutation family, IACR Transactions on Symmetric Cryptology 2020 (2020) 208−261, https://doi.org/10.46586/tosc.v2020.is1.208-261.

[42] H.W. Sun, B.-B. Cai, S.-J. Qin, Q.-Y. Wen, F. Gao, Quantum attacks on beyond-birthday-bound macs, Phys. Stat. Mech. Appl. 625 (2023) 1−17, https://doi.org/10.1016/j.physa.2023.129047.

[43] P. Joshi, B. Mazumdar, SSFA: subset fault analysis of ASCON-128 authenticated cipher, Microelectron. Reliab. 123 (2021) 114155, https://doi.org/10.1016/j.microrel.2021.114155.

[44] S. Banik, A. Chakraborti, A. Inoue, T. Iwata, K. Minematsu, M. Nandi, T. Peyrin, Y. Sasaki, S.M. Sim, Y. Todo, GIFT-COFB, Cryptology ePrint Archive, 2022, pp. 1−30. https://eprint.iacr.org/2020/738.

[45] T. Oder, T. Schneider, T. Pöppelmann, T. Güneysu, Practical CCA2-secure and masked ring-LWE implementation, IACR Transactions on Cryptographic Hardware and Embedded Systems 2018 (2018) 142−174, https://doi.org/10.46586/tches.v2018.i1.142-174.

[46] U. Tariq, Rampant Smoothing (RTS) Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies, EURASIP J. Wirel. Commun. Netw. 2022 (2022) 1−22, https://doi.org/10.1186/s13638-022-02123-5.

[47] A. Attkan, V. Ranga, Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security, Complex & Intelligent Systems 8 (2022) 3559−3591, https://doi.org/10.1007/s40747-022-00667-z.

[48] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A.K. Bashir, U. Tariq, D. Yu, A.V. Vasilakos, Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: a survey, IEEE Trans. Intell. Transport. Syst. 23 (2022) 683−700, https://doi.org/10.1109/tits.2020.3019101.

[49] S. Liao, J. Wu, A.K. Bashir, W. Yang, J. Li, U. Tariq, Digital twin consensus for blockchain-enabled intelligent transportation systems in smart cities, IEEE Trans. Intell. Transport. Syst. 23 (2022) 22619−22629, https://doi.org/10.1109/tits.2021.3134002.

[50] R. Arul, Y.D. Al-Otaibi, W.S. Alnumay, U. Tariq, U. Shoaib, M.D.J. Piran, Multi-modal secure healthcare data dissemination framework using blockchain in IoMT, Personal Ubiquitous Comput. 2021 (2021) 1−13, https://doi.org/10.1007/s00779-021-01527-2.

[51] G.P. Joshi, E. Perumal, K. Shankar, U. Tariq, T. Ahmad, A. Ibrahim, Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks, Electronics 9 (2020) 1−15, https://doi.org/10.3390/electronics9091358.

[52] M.S. Rahman, M.A.P. Chamikara, I. Khalil, A. Bouras, Blockchain-of-blockchains: an interoperable blockchain platform for ensuring IoT data integrity in smart city, Journal of Industrial Information Integration 30 (2022) 1−11, https://doi.org/10.1016/j.jii.2022.100408.

[53] P. Pabitha, J.C. Priya, R. Praveen, S. Jagatheswari, ModChain: a hybridized secure and scaling blockchain framework for IoT environment, Int. J. Inf. Technol. 15 (2023) 1741−1754, https://doi.org/10.1007/s41870-023-01218-6.

[54] E.H. Abualsauod, A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network, Comput. Electr. Eng. 99 (2022) 1−13, https://doi.org/10.1016/j.compeleceng.2022.107847.

[55] Q. Zhou, K. Zheng, K. Zhang, L. Hou, X. Wang, Vulnerability analysis of smart contract for blockchain-based IoT applications: a machine learning approach, IEEE Internet Things J. 9 (2022) 24695−24707, https://doi.org/10.1109/jiot.2022.3196269.

[56] O.A. Khashan, N.M. Khafajah, Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems, Journal of King Saud University - Computer and Information Sciences 35 (2023) 726−739, https://doi.org/10.1016/j.jksuci.2023.01.011.

[57] A. Dixit, A. Trivedi, W.W. Godfrey, A survey of cyber attacks on blockchain based IoT systems for industry 4.0, IET Blockchain 3 (2022) 1−15, https://doi.org/10.1049/blc2.12017.

[58] E.E.-D. Hemdan, W. El-Shafai, A. Sayed, Integrating digital twins with IoT-based blockchain: concept, architecture, challenges, and future scope, Wireless Pers. Commun. 131 (2023) 1−24, https://doi.org/10.1007/s11277-023-10538-6.

[59] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, J. Platts, Cybersecurity, Data privacy and blockchain: a review, SN Computer Science 3 (2022) 1−12, https://doi.org/10.1007/s42979-022-01020-4.

[60] A. Alsirhani, M.A. Khan*, A. Alomari, S. Maryam, A. Younas, M. Iqbal, M.H. Siqqidi, A. Ali, Securing low-power blockchain-enabled IoT devices against energy depletion attack, ACM Trans. Internet Technol. 23 (2022) 1−17, https://doi.org/10.1145/3511903.

[61] T. Hewa, A. Braeken, M. Liyanage, M. Ylianttila, Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing, IEEE Trans. Ind. Inf. 18 (2022) 7174−7185, https://doi.org/10.1109/tii.2022.3140792.

[62] Z. Wang, L. Zhang, X. Ding, K.-K.R. Choo, H. Jin, A dynamic-efficient structure for secure and verifiable location-based

skyline queries, IEEE Trans. Inf. Forensics Secur. 18 (2023) 920—935, https://doi.org/10.1109/tifs.2022.3224666.

[63] H. Xue, D. Chen, N. Zhang, H.-N. Dai, K. Yu, Integration of blockchain and edge computing in internet of things: a survey, Future Generat. Comput. Syst. 144 (2023) 307—326, https://doi.org/10.1016/j.future.2022.10.029.

[64] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, R. Thomas, A survey and taxonomy of consensus protocols for blockchains, J. Syst. Architect. 127 (2022) 1—27, https://doi.org/10.1016/j.sysarc.2022.102503.

[65] A. Mitra, B. Bera, A.K. Das, S.S. Jamal, I. You, Impact on blockchain-based AI/ML-enabled big data analytics for Cognitive Internet of Things environment, Comput. Commun. 197 (2023) 173—185, https://doi.org/10.1016/j.comcom.2022.10.010.

[66] B. Sellami, A. Hakiri, S. Ben Yahia, Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network, Future Generat. Comput. Syst. 137 (2022) 363—379, https://doi.org/10.1016/j.future.2022.07.024.

[67] A.O. Bang, U.P. Rao, A. Visconti, A. Brighente, M. Conti, An IOT inventory before deployment: a survey on IOT protocols, communication technologies, vulnerabilities, attacks, and future research directions, Comput. Secur. 123 (2022) 1—14.

[68] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, Survey on IOT security: challenges and solution using machine learning, artificial intelligence and Blockchain technology, Internet of Things 11 (2020) 1—27, https://doi.org/10.1016/j.iot.2020.100227.