Review of Security-aware Software Engineering Frameworks for Internet of Things

Nada Mohammed Hassan Moter [1], Mustafa Moosa Qasim [2,*], Mohanad Ahmed Abdulrazzaq Diwan Alzamili [3], Mahmood A. Al-Shareeda [4, 5,*], Mohammed Amin [6], and Rami Shihab [7]

[1] Pharmacy Department, Medical Technical Institute-Basra, Southern Technical University, Basra, Iraq
[2] Department of Intelligent Medical Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[3] Department of Computer Networking and Software Techniques, Basra Technical Institute, Southern Technical University, Basra, Iraq
[4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq
[5] College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[6] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[7] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
Email: tsnada2016@stu.edu.iq (N.M.H.M.); mustafa_mq87@uobasrah.edu.iq (M.M.Q.); mohanad.a.abdulrazaq@stu.edu.iq (M.A.A.D.A.); mahmood.alshareedah@stu.edu.iq (M.A.A.-S.); m.almaiah@ju.edu.jo (M.A.); rtshehab@kfu.edu.sa (R.S.)
*Corresponding author

***Abstract*—Internet of Things (IoT) environments are rapidly growing, which in turn has accelerated security threats that are often mitigated by re-activistic deployment-stage controls rather than actively embedded throughout the software development process. Although many other works suggest technical security solutions, little is understood about the process by which security is managed throughout the Software Development Life Cycle (SDLC). This paper provides a systematic literature review of the security aware software engineering frameworks for IoT systems proposed from 2018 to 2025, along with the definition of six dimensions in order to help with its classification and comparison. This taxonomy is organized along six distinct dimensions: (i) phases of SDLC security integration, (ii) categorization of security frameworks, (iii) core security objectives, (iv) trust and adversarial threat premises, (v) contextual limitations imposed by IoT deployments, and (vi) standard of valibation procedures. Comparative analysis conducted via the proposed taxonomy reveals that most existing frameworks prioritize runtime security enforcement and authentication-focused protection targets, rely on implicit or centralized trust paradigms, and suffer from insufficient real-world verifiable validation. Derived from these analytical findings, we identify prominent research gaps spanning full-lifecycle embedded security integration, transparent, verifiable trust modeling, cross-domain framework portability, and repeatable experimental validation methodologies. Beyond its analytical utility, this taxonomy delivers a standardized structural foundation to guide subsequent investigations into security-by-design engineering workflows tailored for IoT software systems.**

***Keywords*—security-aware software engineering, Security and Operations (DevSecOps), Internet of Things (IoT) security frameworks, software development lifecycle, systematic survey**

I. Introduction

The Internet of Things (IoT) has become a fundamental technology paradigm that facilitates ubiquitous connectivity in many domains such as industrial automation, healthcare, transportation, smart cities and critical infrastructures [1–3]. Modern IoT ecosystems are in turn being more software defined as they tap into complex chains of software stacks, heterogeneous distributed services, cloud–edge architectures and Continuous Integration and Deployment (CI/CD) [4–6]. Whilst this evolution is good for functionality and scalability, the drift expands the attack surface introducing great-security threats into heterogeneous and constrained environments [7–9].

Prevailing traditional IoT security research has predominantly focused on cryptographic protocol, secure communication scheme, network layer defense [10–12]. While these methods are essential, they typically consider security as a reactive after-thought to be attached onto implementations well into the design or even deployment phase [13–15]. These reactive practices fail to solve vulnerabilities that stem from insecure requirements engineering, architectural design flaws and inadequate lifecycle governance, resulting in enduring and expensive security breaches [16–18].

Software engineering provides the systematic principles, methods, models and tools to control the

Manuscript received December 20, 2025; revised January 12, 2026; accepted February 28, 2026; published July 17, 2025.

complexity of software development in all stages of Software Development Life Cycle (SDLC) [19–22]. Security-aware (or secure-by-design) engineering, the process of incorporating security into software system development/architecting phases, has proven its effectiveness in traditional software systems [23–26]. Nevertheless, these considerations are difficult to apply in the IoT systems due to the presence of device heterogeneity issues, constrained environments in terms of processing capabilities, dynamic trust relationships between devices, real-time constraints and also for the scalability of a large mass deployment [27–30].

Recent techniques in security aware software engineering have been proposed for IoT environment, and these include Development, Security and Operations (DevSecOps) pipelines [31], model-driven engineering approaches [32], secure architectural frameworks and runtime security management solutions. These works notwithstanding, the existing studies still suffer from being scattered and domain-specific, evaluated using a diverse set of validation strategies which hampers cross comparison and renders conclusions not easy for generalization [33–37].

Although a number of survey papers regarding IoT security protection mechanisms have been published, most of them concentrate on protocol-level solutions or domain-specific threat models. Little effort has been made to study how security is being focused in a consistent manner throughout the SDLC and across architectural principles. Existing surveys also do not investigate trust assumption realization, context restriction and rigor of validation, all as well-organized relative dimensions. This absence of a single analytical framework restricts the possibility to measure research maturity and the identification of structural voids in security aware IoT software engineering.

To counter these constraints, this work presents a multilayered taxonomy that aims to broadly categorise and compare security aware software engineering frameworks for IoT systems. The introduced taxonomy supports structured cross dimensional analysis, and facilitates identification of research trends, limitations, and open challenges in the context of lifecycle-oriented IoT security engineering. The main contributions of this paper are as follows:

- A survey of secure-aware software engineering frameworks for IoT systems, in the period from 2018 up to 2025 with focus on lifecycle integration instead of single mechanisms.
- A new six-dimensional taxonomy that categorizes prior work according to SDLC integration stage, framework type, security objectives, trust and threat assumptions, IoT context constraints, and validation rigor.
- A taxonomy-based comparative synthesis of the prevailing research trends and structural deficiencies in state-of-the art methods.
- Identification of the key problems in research and future directions for promoting integrated security-by-design IoT software engineering practices.

The remainder of this paper is organized as follows: Section II presents the background and motivation for security-aware software engineering in IoT systems. Section III introduces the proposed novel taxonomy of research studies. Section IV provides a comparative analysis and discussion based on the taxonomy. Section V outlines open challenges and future research directions. Finally, Section VI concludes the paper.

II. Background

A. Software-Centric Security Challenges in IoT

The Internet of Things (IoT) has become increasingly a software-defined ecosystem, resulting in more extensive deployment of connected devices in areas such as industrial automation, healthcare and wellbeing systems, transports and smart cities [38–40]. Today's IoT systems are based on sophisticated software stacks, distributed services and continuous updates, greatly expanding the attack surface of the system [40–43]. Therefore, the security holes now more likely come from software weaknesses, poor configurations and mismanagement of lifecycle rather than just the hardware or communication layers. Fig. 1 depicts the IoT and software focused security challenges, highlighting how growing software complexity, diversity of IoT application domains and lifecycle mismanagement augment the attack surface and lead to long-term security vulnerabilities in contemporary IoT systems.

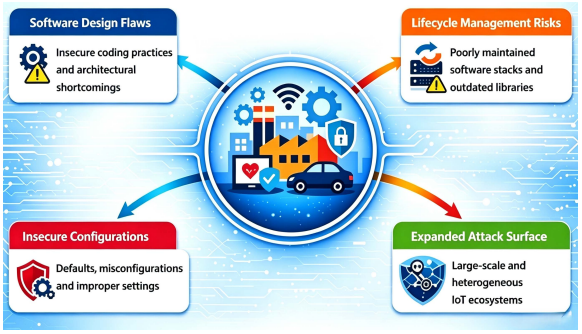

Fig. 1. Internet of things and software-centric security challenges, illustrating how software design flaws.

B. Shortcomings of Existing IoT Security Solutions

Traditional research in the field of security for IoT has traditionally covered cryptographic protocols, secure communication and network-level protections [44–46]. Although, these solutions have some security mechanisms in place, their use results in reactive way of securing systems and management at after deployment stage [47–49]. These approaches do not consider security vulnerabilities that are originated at early development stages and therefore leave such weaknesses as latent bugs causing persistent and more expensive solutions [50–52].

C. Role of Software Engineering in IoT Security

Software engineering provides structured approaches, idealizations, and products for the coping of complexity in SLDC. By baking security into the software engineering process, either by its formalization or security as a

development focus of application, termed secure-aware or secure-by-design Software Engineering (SE), vulnerabilities can be identified and mitigated at the early stages of software engineering [53–55]. But it is challenging to employ these concepts for IoT systems because of factors such as resource constraints (limited processing power and storage capabilities), heterogeneity among devices, establishing trust relationships dynamically and requirement to run in real-time. Fig. 2 depicts Role of Software engineering in IoT Security that demonstrates the composite effect of secure-by-design principles, systematic engineering methods, vulnerability handling and insights, IoT specific constraints that together empower proactive and security-aware integration (life-cycle sensitive).

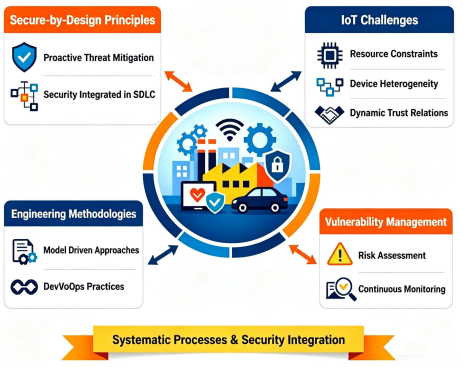

Fig. 2. Role of software engineering in IoT security, illustrating how secure-by-design principles.

D. *Security-Oriented Software Engineering Approaches for the IoT*

Recent works have addressed these challenges and proposed different security-aware software engineering frameworks for IoT, such as DevSecOps pipelines, model-driven engineering strategies, secure architectural patterns and runtime security management frameworks [56–58]. Such initiatives seek to integrate security into various phases of SDLC. Beyond this, current studies are fragmented and domain-specific and are tested using different validation approaches, which hampers systematic comparison/analysis. Fig. 3 presents an overview of state-of-the-art security-aware software engineering frameworks for IoT, focusing on the adoption of DevSecOps, model driven engineering, secure architectures and runtime security mechanisms along different stages of the software lifecycle.

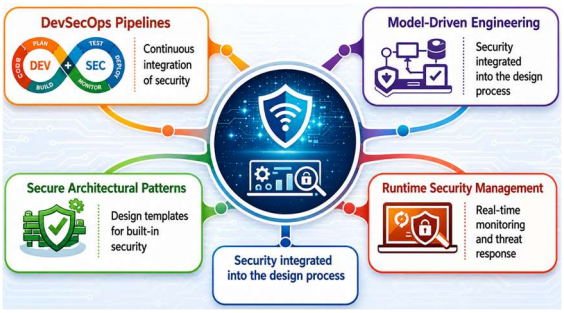

Fig. 3. Software engineering–centric view of IoT security integration across the software development life cycle.

E. *Survey Methodology*

To ensure transparency and reproducibility, this study follows a structured literature review protocol consisting of the following steps:

- Literature Source Selection: Papers were extracted from well-known digital libraries such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink and Google Scholar to consider diverse coverage of qualitative peerreviewed research.
- Search Strategy: Key-based systematic search was carried out in which variations of "security-aware software engineering", "IoT security frameworks", "DevSecOps for IoT", and "secure-by-design IoT", were used.
- Inclusion and Exclusion Criteria: Only peer-reviewed journal articles and conference papers from 2018 to 2025 were included. They were seriously considered if they specifically dealt with the integration of security in the development process of software for IoT systems. We did not consider works dealing exclusively with low level cryptographic protocols or hardware-only security solutions, where no software development point-of-view was considered.
- Screening and Filtering: A preliminary selection was done on the basis of titles and abstracts to exclude irrelevant studies. Full-text reviews were performed next to identify relevant, technically detailed papers that contributed to security-aware IoT software engineering.
- Data Extraction and Classification: Each of the selected studies was reviewed, and mapped into the proposed six-dimensions taxonomy consisting of integration with SDLC, framework type, security objectives addressed by it, trust & threat model assumed its definition, context specific requirements (specific to IoT) constraining it and rigor of validation resorts used.
- Comparative Analysis and Synthesis: The classified research was qualitatively analyzed and comparison of them was performed systematically in order to reveal the major trends, common bottlenecks and required investigation. The findings from this analysis serve as the baseline for the comparative tables, discussion and identification of open problems which we present in this survey.

F. *Motivation for a Taxonomy-Based Analysis*

Because of different and various approaches as well as a lack of a common paradigm in the viewpoint on analysis, it is highly required to own an organized taxonomy for classifying security aware IoT software engineering studies. Such a taxonomic approach facilitates the comparison of lifecycle integration, framework types, security objectives, trust assumptions and contextual constraints as well as of validation rigor. This intuition motivates the novel taxonomy presented in the next section that is used to structure the comparative analysis of urban heat and health risks throughout this paper.

III. Novel Taxonomy of Research Studies

In order to discuss and compare security-aware software engineering frameworks for the IoT in a systematic way, this study presents a new multi-dimensional taxonomy which categorizes relevant research from software engineering and cybersecurity domains, as shown in Fig. 4. In contrast to the previous works which are limited mainly to individual security mechanisms or application domains, our taxonomy provides a representation of where in the SDLC security is inserted, type of engineering frames used, targeted security objectives, baseline trust and threat assumptions context specific IoT constraints and validation rigor. Such a structured classification allows for an in-depth analysis of research maturity, reveals underexplored overlaps and provides guidance with respect to open issues and future directions.

Fig. 4. Proposed novel taxonomy of research studies for security-aware software engineering frameworks in the internet of things.

A. SDLC Security Integration Point

This dimension categorizes the researches in terms of where security is incorporated into the Software Development Life Cycle (SDLC) pertinent to IoT systems: requirements engineering, architectural design, implementation, testing and deployment and runtime maintenance. The significance of this is that it highlights how early and consistently security is approached. A large number of researches focus on penetration testing and intrusion detection, yet less work adopts secure-by-design philosophy at the stage of requirements or design, which results in fragmented and passive security strategies.

Zhukabayeva *et al.* [59] proposed an edge-assisted IIoT security model based on clustering and categorization strategy to analyze traffic patterns as well as to detect intrusion. Experimental results show efficient anomaly detection, good classification performance, and low latency, proving the feasibility of ML-based cybersecurity solutions in real-time IIoT. Li *et al.* [60] introduced a full-industrial-edge-of-things security framework with an in-depth analysis of threats, solutions, and architectures based on each layer. Ouyang *et al.* [61] present a smart cross-border logistics platform based on IoT, serverless, and microservices to realize high scalability and more security. The experimental results demonstrate a low operational cost and a flexible system for cross-border business, protecting logistics and data in complex transaction environments. Hasan *et al.* [62] present a Long Short-Term Memory (LSTM)-based intrusion detection mechanism utilizing Software-Defined Networking (SDN) to defend heterogeneous IoT systems. Based on a deep learning framework and SDN orchestration, the proposed method demonstrates superior detection accuracy over benchmark data sets, providing a scalable and efficacious way to defend against threats targeting essential IoT infrastructure components. Bhandari *et al.* [63] proposed Internet of Things Vulnerable Code Dataset (IoTvulCode)—a new framework that integrates a dataset-generation tool and machine learning principles to identify vulnerabilities in source code related to IoT frameworks. Zuraiqi and Greer [64] performed a large-scale static analysis of IoT device firmware and identified critical vulnerabilities as well as long-lived security issues. Yadav *et al.* [65] introduced Internet of Things Penetration Testing Framework (IoT-PEN), which is the first-of-its-kind and full-fledged end-to-end penetration testing approach for IoT networks that discovers multi-stage and multi-host attack paths. Hatmai *et al.* [66] proposed a secure and scalable onboarding solution for limited capability IoT nodes by combining SCHC Zero with Bootstrapping Remote Secure Key Infrastructure (BRSKI). Validated through a Long-Range Wide Area Network (LoRaWAN) deployment, our approach gives rise to an autonomous and low-overhead device onboarding and management mechanism that exhibits scalable support for a secure massive IP-based IoT landscape.

B. Framework Type

This dimension classifies studies according to the kind of software engineering artifact that they present, i.e. process-oriented frameworks (e.g. DevSecOps), model-driven frameworks, tool chain-based approaches, architectural frameworks, assurance/compliance models and hybrid solutions [67–69]. Each type of framework is an abstraction layer with a certain level of complexity when it comes to adoption. This categorization illustrates that security-aware IoT solutions are diverse in term of their maturity, the extent to which they can be reused, automation support and alignment with software engineering practices.

Spina *et al.* [70] proposed an Internet of Everything (IoE)-enabled architecture which can to not only provide all the aforementioned features at once but also provides energy and security management for IoT. It provides an IoE controller and Efficient Split Artificial Intelligence (ESAI) metric for optimizing security-energy trade-offs. The proposed approach improves efficiency and device lifetime while providing security guarantees, targeting limitations present in current Transport Layer Security/ Datagram Transport Layer Security (TLS/DTLS) design within dynamic, resource constrained environments to enable scalable 6G IoT deployments. Schicchi *et al.* [71] focused on efforts to include security as part of the early stages of Agile development by implementing a DevSecOps model. By focusing on automated, repeatable security controls within Continuous Integration/Continuous Delivery (CI/CD) pipelines and by validating recommendations through an industrial case study, the work demonstrates that, even in a culture of high-speed development priority, one can develop good software quality without sacrificing speed. Sharma *et al.* [72] presented a blockchain-based approach for improving supply chain traceability and data integrity. Through the introduction of trust-enabled hybrid consensus and authorization schemes, the work bears low latency and light resource consumption. Moin *et al.* [73]

presented ML-Quadrat, an integrated model driven software engineering and machine learning framework for Cyber-Physical Systems (CPS) in the IoT. Confirmed by implementation and user feedback, this work realizes enhanced efficiency in system development, optimization, and practitioners' brittle experience towards intelligent IoT systems.

C. Security Objectives

This dimension categorizes research based on their focus of the main security goals that need to be achieved, in terms of confidentiality, integrity, availability and authentication access control and privacy. This dimension allows comparison of frameworks by concentrating on specific security objectives, in contrary to generic "IoT security" claims. We find that most solutions focus on authentication and intrusion detection, while goals such as privacy-by design or availability assurances, and full Confidentiality, Integrity, and Availability (CIA) coverage are largely under investigated in security aware IoT software engineering.

Fang *et al.* [74] proposed a universal cross-platform secure communication scheme for an industrial IoT platform based on conditional proxy re-encryption. The proposed solution successfully addresses the data security problem with low computation and communication overhead by means of aggregating all possible industrial settings into a general model. Subramani *et al.* [75] introduced a light-weight privacy-preserving anonymous authentication scheme for Wireless Body Area Network (WBAN). Specifically, the novel scheme protects data and user confidentiality in practical healthcare systems with constraints on sensors, offers selective patient anonymity, and provides conditional anonymity to assure normal users for easy integration with applications without extra change. Tao *et al.* [76] introduced multi-tiered cloud-based architecture for IoT empowered smart home to overcome heterogeneous devices and services. Leveraging ontology-based interoperability and security services, the architecture supports universal communication, data representation and privacy preserving management among diverse vendors and protocols. Mudassar *et al.* [77] presented a fault-tolerant framework for edge computing in the IoT applications that uses smart checkpoint and replication. By replicating those checkpoints on adjacent edge nodes, the method enhances task reliability and availability, while still ensuring application deadlines in resource limited and failure-prone edge contexts. Alhosban *et al.* [78] described SFSS, a self-healing fault management system for service-oriented architectures. By predicting, identifying and recovering faults with Quality of Service (QoS)-aware schemes and user preference, Smart Fabric Storage Software (SFSS) can select the best recovery plan by estimating service's quality improvement level to support the selection quality of services as a whole system reliability/performance. Alzaidi *et al.* [79] presented a secure and privacy-aware blockchain-and fog-based multi-factor authentication for Vehicular Ad Hoc Networks (VANETs) with privacy preservation, integrity checking, light-weight overhead. By integrating biometrics and Quick Response (QR) codes with distributed ledgers, it achieves the balance between computation, communication costs and security protection under various attacks in the environment of dense vehicles.

D. Trust/Threat Assumptions

This talks about the trust model and threat assumptions for each research, e.g., centralized trust, distributed or blockchain based model of trust, zero trust architecture, or adaptive models of trust. It's important to spell-out these assumptions, because they have a huge impact on scaling, reliability and deploy ability. Most systems assume that the gateways or cloud is to be trusted, thus cannot satisfy general adversaries multi-party settings. This dimension reveals the concealed dependencies and facilitates a realistic evaluation of frameworks.

Cheng *et al.* [80] presented a lightweight authentication oriented trusted management framework for IoT collaboration. Through the combination of efficient authentication and key agreement, blockchain-based traceability, distributed storage and fine-grained access control, our framework can achieve secure and reliable task execution with low overhead under practical IoT settings. Giao *et al.* [81] presented a Service-Oriented Architecture–based system for an International Internet of Things Expo (IOTE)-manufacturing, to overcome the heterogeneity among various services. The proposed architecture enables dynamic discovery, reuse, and integration of composable IoT services to improve flexibility and efficiency while leveraging practical challenges and constraints inherent in industrial IoT settings. Kouicem *et al.* [82] introduced a hierarchical and scalable blockchain-based trust management protocol for the Internet of Everything. Through broadcasting the trust information on System Network Architecture (SNA), our approach is friendly both with heterogeneity and mobility, immune to malicious interference and comparative superiority in terms of scalability, communication efficiency and computation complexity. Anasuri [83] introduced Zero Trust Architecture to protect the multi-cloud environment. Through a combination of federated identity, micro-segmentation, and dynamic policy enforcement capabilities, the architecture mitigates risks related to fragmented identities and server-to-server movement as well or better than traditional perimeter-based models in terms of security efficiency and operational resiliency. Alserhani *et al.* [84] presented a machine learning-based cognitive hyperphysical system to protect Medical IoT infrastructures. The proposed framework harmonizes behavior analysis and Extreme Learning Machine (ELM) based classification to provide adaptive detection, high accuracy, scalability, and efficiency that efficiently safeguards the life-critical Medical Internet of Things (MIoT) systems.

E. IoT Context Constraints

This dimension is the type of studies, based on the domain of application and operational constraints of the desired IoT environment (e.g. industrial IoT, healthcare, smart cities; vehicular network, home automation). It also

takes into account the energy, real-time, mobility and instability etc. constraints of the network. As IoT security solutions strongly depend on the context, this dimension explains why protocols and frameworks that works in one area may not work in another, supporting context-aware design and assessment.

Ungurean *et al.* [85] presented a low-abstraction, four-tier software architecture for the Industrial Internet of Things (IIoT) that includes fog and edge computing. By using consistent addressing & System on Chip (SoC) based platforms with dedicated co-processors, it allows for real-time, efficient and scalable processing of industrial data and interaction. Hassan *et al.* [86] presented hyperphysical security challenges in IIoT systems and brings out the trans-formative role of AI. It presents a modular AI-driven cybersecurity model, that provides real-time threat detection capability while maintaining resilience and compatibility with legacy systems, and delivers direction for future research, policy development, application to industry practice. Hasan *et al.* [87] introduced a novel SDN-based multi-objective optimization scheme for IIoT premise energy systems that can dynamically make use of security countermeasures. Bayesh *et al.* [88] proposed a security-oriented framework for self-driving IoT systems that combines Explainable Artificial Intelligence (XAI) to the structured security profiling. Mapping the explainable ML results to feature-level importance factors, it improves the contextual understanding of threats, enabling users with actionable security insights in real-time which is validated on a smart irrigation testbed. Marchang *et al.* [89] presented the secure-by-design Internet of Medical Things (IoMT)-based real-time e-health population monitoring architecture. The framework achieves the desired confidentiality, integrity and availability of information by providing privacy-preserving key management, resilient authentication and secure live data exchange validated through real-world network experimentation under resource poor healthcare conditions. Thangam *et al.* [90] proposed a Directed Acyclic Graph (DAG)-based secure Vehicle-to-Everything (V2X) communication framework not only for immediate decision making but also for the efficient detection of malicious nodes.

F. Validation Rigor

This dimension measures the empirical validation strength of the evaluation channel applied toward the considered frameworks, from conceptual analysis/prototypes to controlled experiments real-world deployments and reproducible benchmarking. Validation is a vital part in identifying "pipedreams" from legitimate proposals. Our analysis indicates that a large number of studies consider only limited prototypes or simulations, and very few offer comparative, replicable to real-world validation—pinpointing a significant research gap in security aware IoT software engineering.

Longari *et al.* [91] suggested a semi-automatic, topology driven risk analysis model to secure automotive and on-board networks. The method provides a formal analysis to obtain topologies of networks with known Adaptive Learning Network (ALN) risk metrics and find vulnerabilities that are fed into the Secure Computing and Communication (SecC) system and determine security-hardened designs for preventing critical attacks, thereby improving safety in new connected cars. Paul *et al.* [92] investigated zero-trust security model for Industry 4.0 and smart manufacturing. It analyzes principles, architectural aspects and enabling technologies, and suggests a micrified zero trust design integrating micro-segmentation, device discovery & control, and policy driven compliance of IoT enabled industrial systems spanning infrastructure on-premises as well as in the cloud. Roman *et al.* [93] put forward a lightweight quantum resistant remote attestation protocol for low-cost IoT devices with a Robust Trust based on Physical Unclonable Functions (PUFs) and Attestation Read-Only Memory (ROM). By utilizing hash-based one-time signatures, the strategy can achieve secure firmware integrity verification with little computational, memory, and communication overhead. Coito *et al.* [94] introduced an intelligent automation platform for Industry 4.0 with Realtime ability, interoperability and deterministic communication capability. Using Open Platform Communications Unified Architecture (OPC UA) over Time-Sensitive Networking (TSN), fog computing and dynamic scheduling to the structure of standard and industrial practice, the framework presents a pharmaceutical industry use case for validation.

Hussain *et al.* [95] proposed a layered security model for the IoT based real time e-health monitoring system using Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) and HyperText Transfer Protocol Secure (HTTPS). The proposed framework guarantees confidentiality, integrity, and authenticity of the health data at perception, network, and application layers for sensor-based healthcare applications with low security risks in end-to-end communication.

IV. Comparative Analysis and Discussion

This text provides a detailed comparative analysis and discussion on security-aware software engineering for IoT with respect to existing frameworks based on the elicited compact taxonomy. Our desire with this section is to establish, through a systematic review of the reviewed articles along different analysis dimensions, dominant trends and recurrent limitations in the studies analyzed, but also to identify crucial research lines yet unexplored. The comparative study presents a systematic review on existing approaches, whereas the discussion consolidates the cross-dimensional lessons learned to point out opportunities and challenges in security-aware IoT software engineering.

A. Comparative Analysis

This subsection compares security-aware software engineering frameworks for the Internet of Things based on the novel taxonomy presented. Common characteristics, limitations and implications from all reviewed papers are summarized in Table I, to systematically analyze the quality of such contributions.

TABLE I. COMPARATIVE ANALYSIS OF SECURITY-AWARE IOT SOFTWARE ENGINEERING STUDIES BASED ON THE PROPOSED TAXONOMY

Comparison Dimension	Dominant Trend	Secondary Trend	Observed Gap	Implication
SDLC Security Integration	Runtime monitoring and deployment-level security dominate.	Testing and intrusion detection during post-development phases.	Limited focus on requirements engineering and secure design.	Security remains reactive, increasing long-term maintenance cost.
Framework Type	Architecture- and toolchain-based frameworks prevail.	Hybrid and DevSecOp oriented approaches are emerging.	Process-driven and assurance frameworks are underrepresented.	Lack of systematic, lifecycle wide security governance.
Security Objectives	Authentication and integrity protection are primary goals.	Intrusion detection and access control.	Availability, privacy-by design, and supply-chain security.	Partial security coverage in complex IoT deployments.
Trust / Threat Assumptions	Centralized and implicit trust models are common.	Distributedand zero-trust models are increasing.	Explicit threat modeling is often missing.	Limited scalability and reduced resilience in adversarial settings.
IoT Context Constraints	Domain-specific solutions (IIoT, IoMT, V2X).	Smart city and smart home applications.	Cross-domain adaptability and portability.	Frameworks are difficult to generalize across IoT domains.
Validation Rigor	Prototype implementations and simulations dominate.	Controlled experimental evaluations.	Real-world deployment and reproducible benchmarking.	Uncertain long-term effectiveness and limited technology transfer.

TABLE II. DISCUSSION OF STRENGTHS, LIMITATIONS, AND FUTURE RESEARCH DIRECTIONS BASED ON THE PROPOSED NOVEL TAXONOMY

Taxonomy Dimension	Observed Strengths	Observed Limitations	Future Research Directions
SDLC Security Integration Point	Strong focus on runtime monitoring, intrusion detection, and deployment-level security mechanisms.	Limited integration of security during requirements engineering and architectural design phases.	Develop security-by-design and requirement-driven IoT software engineering frameworks.
Framework Type	Well-established architectural and toolchain-based frameworks; growing adoption of DevSecOps practices.	Limited integration between process, modeling, tooling, and assurance layers.	Design unified frameworks combining process, model-driven, and tool-supported security.
Security Objectives	Effective coverage of authentication, integrity, and intrusion detection with lightweight solutions.	Fragmented coverage of confidentiality, availability, privacy-by-design, and supply-chain security.	Expand toward holistic CIA coverage, privacy-aware design, and software supply-chain protection.
Trust / Threat Assumptions	Emerging use of distributed trust and zerotrust architectures improves resilience.	Implicit or centralized trust assumptions reduce scalability and real-world applicability.	Formalize explicit threat models and adopt adaptive and zero-trust mechanisms.
IoT Context Constraints	Domain-specific solutions effectively address real-time, energy, and mobility constraints.	Limited cross-domain generalization and adaptability across heterogeneous IoT environments.	Develop context-baroreceptor table security-aware IoT SE frameworks.
Validation Rigor	Widespread use of prototypes and controlled experimental evaluations.	Scarcity of real-world deployments, benchmarking, and reproducible validation.	Promote open datasets, comparative benchmarks, and real-world testbeds.

B. Discussion

This subsection reviews the studies that have been analyzed in terms of the proposed novel taxonomy, synthesizing strengths, limitations and research gaps along several dimensions as summarized in Table II. Instead of assessing the individual papers, we identify cross-dimensional trends that are characteristic for security-aware software engineering approaches in the Internet of Things.

The longevity of the issues identified in security-aware IoT software engineering can be explained by several structural and practical reasons. From an industry viewpoint, security needs are frequently forced by time-to-market constraints and adding security reactively rather than systematically building in security from the start. From a tooling perspective, mature and widely accepted development tools (e.g., simulators, emulators, code analyzers) that can seamlessly incorporate formal security modeling and threat analysis are also not available beyond existing DevSecOps pipelines. In addition, the lack of standardized and agreed upon matrices for assessing IoT security frameworks restricts reproducibility, and discourages extensive validation in real life scenarios. The heterogeneity of IoT environment such as varied hardware platforms, communication protocols, application domains among other things make more difficult the adoption of holistic engineering strategies. These altogether cause disjointed solutions and a slowdown in translating security-aware software engineering research results into deployable IoT systems.

V. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite some achievements, there are still Some critical challenges (Fig. 5) which need to be addressed in the field of security-aware software engineering for Internet of Things systems. Leveraging the comparative discussion of Table I, Fig. 5 brings the identified gaps together as a series of open research challenges. Although the available frameworks are dedicated to different security details, we identify some common weaknesses regarding preliminary phase of security integration, explicit trust model

establishment, integrated engineering workflow and strong validation. Collectively, these challenges emphasize the requirement for end-to-end software engineering practices with security considerations embedded throughout the IoT development process and not just siloed phase-based solutions.

Security-by-Design across the SDLC: Security requirements, threat modeling and risk analysis must become part of the entire SDLC from its very beginning in future frameworks. Accentuating the need for requirements engineering and secure architectural patterns may reduce the number of vulnerabilities induced during later parts in development and maintenance of a system.

Unified and Integrated Engineering Frameworks: Existing techniques are still scattered through the process oriented, model-driven and tool-centric solutions. Unified frameworks are in high demand, which can integrate secure software engineering activities, formal modeling, automated reasoning and continuous security enforcement into DevSecOps pipelines well.

Comprehensive Security Objective Coverage: Most of the current studies emphasize on authentication and intrusion detection, but protect read "availability", privacy-by design and software supply-chain security are less concerned. In the future, research needs to target comprehensive coverage for confidentiality, integrity, availability and privacy both in safety-critical and in large-scale IoT scenarios.

Trust models Both Explicit and Adaptive: A lot of previous work adopts implicit or centralized trust assumptions, which are not scalable and resilient. It would be interesting to have more refined models for threat and evidence, as well as adaptive trust that has potential behind zero-trust with ability of responding situationally couple between an attack surface and between various stakeholders in which they are interacting.

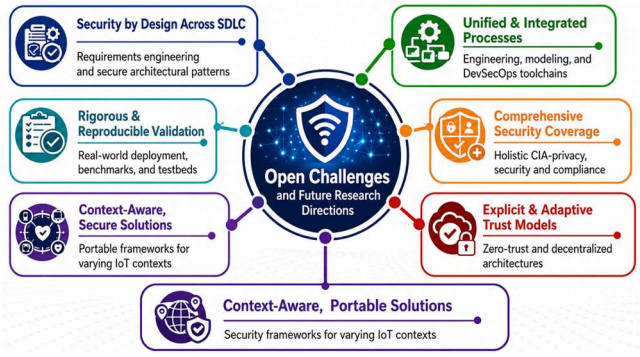

Fig. 5. Open challenges and future research directions in security-aware Internet of Things software engineering.

Context-Aware yet Portable Solutions: Security models are, in many cases, specializing on specific IoT n domains as industrial, healthcare and vehicular systems. The future work will concentrate on building context-aware solutions that are still portable, and configurable in different heterogeneous IoT applications with different constraints and requirements.

Rigorous and Reproducible Validation: There is a significant divide between theoretical designs and practical implementations. It should be highlighted that there is a space of research around real-world deployment measures, comparative benchmarking and reproducibility of experimentation through publicly available datasets and testbeds efforts in order to acquire credibility in what would render technology transfer.

To mitigate the fragmentation of security practices in IoT software development, future research should focus on unified and integrated engineering frameworks guided by well-defined design principles for specifying secure architectures. Early-Stage Security Integration (Security-by-Design): Software development from the requirements collection to architectural design Security should be build-in at every phase of the software development Process. It is also possible to use traditional threat modelling and risk analysis to define security objectives before the system is constructed.

Model-Driven Security Specification: Such models can be defined using model-driven engineering approaches, e.g. security policies, trust relationships, access control rules.

These models can act as a common model of the trust relationships, while being automatically transformed to enforced security configurations and code level artifacts.

DevSecOps Pipeline Integration: Consolidated platforms must bake security models directly into DevSecOps pipelines, allowing end-to-end, real-time security checks. For instance, security requirements could be converted into automated tests, static analysis rules and deployment policies checked during build-, test- and deployment-time.

Modular and Microservices-Based Architecture: Architectural styles, such as microservices and containers deployment enable modularity and isolation that are necessary to scale-out and secure IoT systems. These design patterns allow for increased portability across disparate IoT environments by abstracting the services from the underlying hardware.

Explicit Trust and Threat Modeling: Trust assumptions (adversarial capabilities) should not be implicit or centralized and they could implicitly-track trust relationships, but avoiding defining trust-management policies in it. This allows for uniform security reasoning across various deployment environments and provides better protection against both insider and infrastructure-level attacks.

Cross-Domain Adaptability: To cater to various IoT domains including health care, industrial automation and smart cities, security mechanisms must be developed as reusable and configurable components. Architectural abstraction layers can assist in accommodating DS specific constraints with no need for a re-design of the entire framework.

Continuous Validation and Feedback: Built in support for on-going validation, with regard to both testing and simulation and, where feasible, real-world tests. Lessons learned from the operation of such installations may be employed to better formal security model and bolster long term robustness of systems.

VI. Conclusion and Future Work

This paper presented a comprehensive survey of the progression of security-aware software engineering frameworks for IoT based systems using structured taxonomy-driven approaches. There is a pattern presenting an individual piece of study's findings, that reflects the continuing structural inequality within current research. Integration focus has been largely on security at deployment and runtime, with early-stage requirements engineering and architectural design receiving relatively little attention. Likewise, Authentication and Intrusion Detection are areas which are heavily represented in the landscape and for which comprehensive coverage can be found; while availability (in suitable form) is not yet quite as fragmented but has more representation occurring.

Another important observation is related to trust model. Many of the referred frameworks however often implicitly presuppose centralized or mostly trusted infrastructures, which limits scalability and robustness in adversarial and heterogeneous IoT scenarios. The systematic adoption of distributed and zero trust paradigms in the software development life-cycle is still limited. There is also incomplete empirical verification about the effectiveness of concrete systems, as well as limited real-world deployment experience on such field, and lack of benchmarking with reproducibility.

Overall, the findings demonstrate that if we wish to progress IoT security beyond a phase-based approach then we must move towards a lifecycle-centric integrated engineering framework. The future work should emphasize on security-by-design integration, explicit and adaptive trust modeling across the nodes in a community, cross-domain portability as well as rigorous validation strategies. By mapping the literature and delineating the structural gaps, this work offers a conceptual basis to inform further security aware IoT software engineering practice.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Nada Mohammed Hassan Moter contributed to the conceptualization of the study, conducted the literature review, and drafted the initial manuscript; Mustafa Moosa Qasim supervised the research process, contributed to the methodology design, and critically revised the manuscript; Mohanad Ahmed Abdulrazzaq Diwan Alzamili contributed to data analysis, taxonomy development, validation of the reviewed frameworks, data collection, classification of studies, and preparation of figures and tables; Mahmood A. Al-Shareeda contributed to the research design, technical validation, and manuscript revision, and provided overall guidance on security modeling and IoT frameworks; Mohammed Amin contributed to the interpretation of results and improvement of the discussion and future research directions; Rami Shihab provided supervision, critical review, and final approval of the manuscript; all authors have read and approved the final version of the manuscript.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU261324).

References

[1] R. Mishra and A. Mishra, "Current research on Internet of Things (IoT) security protocols: A survey," *Computers and Security*, vol. 151, 104310, 2025.

[2] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, pp. 45–56, 2024.

[3] V. Choudhary, P. Guha, G. Pau, and S. Mishra, "An overview of smart agriculture using Internet of Things (IoT) and web services," *Environmental and Sustainability Indicators*, vol. 26, 100607, 2025.

[4] S. Jamshidi, A. Nikanjam, K. W. Nafi, F. Khomh, and R. Rasta, "Application of deep reinforcement learning for intrusion detection in internet of things: A systematic review," *Internet of Things*, vol. 31, 101531, 2025.

[5] M. M. Qasim, A. N. Zulkifli, M. Ahmad, M. Omar, and J. A. A. Bakar, "Educating parents in dealing with childhood obesity through the use of the BMI monitor app," *Man in India*, vol. 96, no. 1–2, pp. 367–376, 2015.

[6] S. Padmanaban, M. A. Nasab, A. Sagar, M. Zand, M. A. Dashtaki, and M. A. Nasab, "Improving Energy Consumption in Smart Homes Based on the Internet of Things," in *Biomass and Solar-Powered Sustainable Digital Cities*, O. V. G. Swathika, K. Karthikeyan, M. S. Dangate, and N. Ravasio, Eds., Hoboken, NJ, USA: Wiley, 2024, ch. 9, pp. 147–161.

[7] S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula, "Study of security issues and solutions in Internet of Things (IoT)," *Materials Today: Proceedings*, vol. 80, pp. 3554–3559, 2023.

[8] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022.

[9] H. Taherdoost, "Security and internet of things: benefits, challenges, and future perspectives," *Electronics*, vol. 12, no. 8, 1901, 2023.

[10] A. N. Lone, S. Mustajab, and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the IoT world," *Security and Privacy*, vol. 6, no. 6, e318, 2023.

[11] M. M. Qasim and A. R. Abdulkareem, "Software engineering and the adoption of internet of things: A systematic literature review," in *Proc. 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, 2024, pp. 1–6.

[12] D. Alsalman, "A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats," *IEEE Access*, vol. 12, pp. 14719–14730, 2024.

[13] M. M. Qasim, M. Ahmad, M. Omar, A. N. Zulkifli, and J. A. A. Bakar, "A systematic process for persuasive mobile healthcare applications," in *Proc. AIP Conference Proceedings*, vol. 1891, no. 1, 020115, 2017.

[14] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. AlMekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 12, 5939, 2022.

[15] M. Moosa Qasim, M. Ahmad, M. Omar, A. N. Zulkifli, and J. A. A. Bakar, "Development and validation of an instrument to measure the persuasion effects on parents after using the persuasive mobile child obesity monitor app," *Journal of Computational and Theoretical Nanoscience*, vol. 16, pp. 2424–2432, 2019.

[16] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A survey on security, privacy, trust, and architectural challenges in IoT systems," *IEEE Access*, vol. 12, pp. 57128–57149, 2024.

[17] M. M. Qasim, J. M. Altmemi, A. H. Abd Ali, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Ca-hbca: A software engineering

framework for secure, scalable, and adaptive healthcare blockchain systems," *Journal of Robotics and Control (JRC)*, vol. 6, no. 4, pp. 2052–2063, 2025.

[18] E. B. Fernandez, H. Washizaki, N. Yoshioka, and T. Okubo, "The design of secure IoT applications using patterns: State of the art and directions for research," *Internet of Things*, vol. 15, 100408, 2021.

[19] X. Chen *et al.*, "Deep learning-based software engineering: progress, challenges, and opportunities," *Science China Information Sciences*, vol. 68, no. 1, 111102, 2025.

[20] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," in *Proc. 2018 International Arab Conference on Information Technology (ACIT)*. 2018, pp. 1–5.

[21] A. Fan, B. Gokkaya, M. Harman, M. Lyubarskiy, S. Sengupta, S. Yoo, and J. M. Zhang, "Large language models for software engineering: Survey and open problems," in *Proc. 2023 IEEE/ACM International Conference on Software Engineering: Future of Software Engineering (ICSE-FoSE)*, 2023, pp. 31–53.

[22] X. Hou, Y. Zhao, Y. Liu, Z. Yang, K. Wang, L. Li, X. Luo, D. Lo, J. Grundy, and H. Wang, "Large language models for software engineering: A systematic literature review," *ACM Transactions on Software Engineering and Methodology*, vol. 33, no. 8, pp. 1–79, 2024.

[23] L. Belzner, T. Gabor, and M. Wirsing, "Large language model assisted software engineering: prospects, challenges, and a case study," in *Proc. International Conference on Bridging the Gap Between AI and Reality*, 2023, pp. 355–374.

[24] G. De Vito, "Assessing healthcare software built using IoT and LLM technologies," in *Proc. 28th International Conference on Evaluation and Assessment in Software Engineering*, 2024, pp. 476–481.

[25] M. M. Qasim, M. Ahmad, and M. Omar, "Analyzing persuasive mobile healthcare architecture using systematic process design," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 2, pp. 77–84, 2017.

[26] R. C. Motta, K. M. Oliveira, and G. H. Travassos, "An evidence-based roadmap for IoT software systems engineering," *Journal of Systems and Software*, vol. 201, 111680, 2023.

[27] R. Vavekanand, "Advancements in software engineering for IoT applications: Addressing challenges and seizing opportunities," arXiv Preprint, arXiv: 1405.0312, 2014. doi: 10.48550/arXiv.1405.0312

[28] W. R. Martınez and A. A. G. Gomez, "An approach from´ software engineering to an IoT and machine learning technological solution that allows monitoring and controlling environmental variables in a coffee crop," *Information*, vol. 26, no. 3, pp. 465–478, 2021.

[29] S. Siddamsetti, M. M. Qasim, N. Sravanthi, K. Dinesh, V. Velmurugan, S. Sengan, and P. Dadheech, "Wireless sensor networks with modular metric spaces," *J. Interdiscip. Math*, vol. 28, no. 2, pp. 659–667, 2025.

[30] M. Jantti and M. Aho, "Engineering iot-based software systems for forestry: A case study," in *Proc. 18th International Conference on Software Engineering Advances (ICSEA'23)*, 2023, pp. 13–17.

[31] O. B. Abiola and O. G. Olufemi, "An enhanced cicd pipeline: A devsecops approach," *International Journal of Computer Applications*, vol. 184, no. 48, pp. 8–13, 2023.

[32] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, "Monitoring real time security attacks for iot systems using devsecops: A systematic literature review," *Information*, vol. 12, no. 4, 154, 2021.

[33] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, no. 1, pp. 27–36, 2025.

[34] S. A. Sari *et al.*, "Ea-uap: A software engineered adaptive and energy-aware authentication protocol for 5genabled UAV networks," *International Journal of Robotics and Control Systems*, vol. 6, no. 1, pp. 577–608, 2026.

[35] M. Norouzi *et al.*, "Security-aware resource management approaches in software defined networks: Comprehensive analysis, opportunities and challenges," *Journal of High-Speed Networks*, vol. 29, no. 3, pp. 169–181, 2023.

[36] J. M. H. Altmemi, F. K. A. Shammri, Z. M. Alzamili, M. A. A. Shareeda, M. A. Almaiah, R. Shehab, M. A. B. Ngadi, and A. Z. A. Aljarwan, "A software-centric evaluation of the veins framework in vehicular ad-hoc networks," *Journal of Robotics and Control (JRC)*, vol. 6, no. 2, pp. 822–845, 2025.

[37] D. Alalisalem and H. Rahman, "Securing healthcare digital twin with blockchain: A systematic review of architecture, threats and evaluation," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, pp. 46–66, 2026.

[38] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296–312, 2023.

[39] S. Alsahaim, M. A. Almaiah, and R. B. Sulaiman, "Security threats in mobile phones: Challenges, countermeasures, and the importance of user awareness," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2023, no. 1, pp. 1–10, 2023.

[40] N. Rane, "Enhancing customer loyalty through Artificial Intelligence (AI), Internet of Things (IoT), and big data technologies: improving customer satisfaction, engagement, relationship, and experience," *Internet of Things (IoT), and Big Data Technologies: Improving Customer Satisfaction, Engagement, Relationship, and Experience*, 2023.

[41] N. Radwan and M. Farouk, "The growth of Internet of Things (IoT) in the management of healthcare issues and healthcare policy development," *International Journal of Technology Innovation and Management (IJTIM)*, vol. 1, no. 1, pp. 69–84, 2021.

[42] M. S. Alghareeb, M. Almaiah, and Y. Badr, "Cyber security threats in wireless LAN: A literature review," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2024, no. 1, pp. 11–20, 2024.

[43] M. Ho, S. Ang, S. Huy, and M. Janarthanan, "Mumspi: A model for usability measurement of single-platform interface for multitasking in big data tools," *Jordanian Journal of Informatics and Computing*, vol. 2026, no. 1, p. 1–14, 2026.

[44] C. M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M. A. Kourtis, "On the design of IoT security: Analysis of software vulnerabilities for smart grids," *Energies*, vol. 14, no. 10, 2818, 2021.

[45] M. Alrajeh, M. Almaiah, and U. Mamodiya, "Cyber risk analysis and security practices in industrial manufacturing: Empirical evidence and literature insights," *International Journal of Cybersecurity Engineering and Innovation*, no. 1, 2025.

[46] S. Von Solms and L. A. Futcher, "Adaption of a secure software development methodology for secure engineering design," *IEEE Access*, vol. 8, pp. 125630–125637, 2020.

[47] G. Pulkkis, J. Karlsson, and M. Westerlund, "Blockchain-based security solutions for IoT systems," in *Internet of Things A to Z*, Wiley, 2025, ch. 21, pp. 523–537.

[48] M. A. Shareeda and H. Alrudainy, "Sustainable and secure energy optimization strategies in the internet of healthcare things (IoHT)," *International Journal of Cybersecurity Engineering and Innovation*, no. 1, 2026.

[49] M. Fahmideh, A. Ahmad, A. Behnaz, J. Grundy, and W. Susilo, "Software engineering for internet of things: The practitioners' perspective," *IEEE Transactions on Software Engineering*, vol. 48, no. 8, pp. 2857–2878, 2021.

[50] I. A. Barazanchi, A. Murthy, A. A. Q. A. Rababah, G. Khader, H. R. Abdulshaheed, E. Daghighi, and Y. Niu, "Blockchain-technology-based solutions for IoT security," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp 52–61, 2022.

[51] M. A. Shareeda, H. A. Musa, A. Jaafar, A. A. Salman, Z. J. Tami, H. M. Hameed, A. Muaid, H. A. H. Hasan, and N. S. Bashkh, "Design and implementation of a speech-to-sign robotic arm for deaf communication," *International Journal of Cybersecurity Engineering and Innovation*, no. 1, 2026.

[52] D. Swessi and H. Idoudi, "A survey on internet-of-things security: Threats and emerging countermeasures," *Wireless Personal Communications*, vol. 124, no. 2, pp. 1557–1592, 2022.

[53] A. N. Duc, R. Jabangwe, P. Paul, and P. Abrahamsson, "Security challenges in IoT development: A software engineering perspective," in *Proc. XP2017 Scientific Workshops*, 2017, pp. 1–5.

[54] Z. G. Al-Mekhlafi, S. A. Lashari, J. M. H. Altmemi, M. A. A. Shareeda, B. A. Mohammed, A. A. Sallam, B. A. A. Qatab, M. T. Alshammari, and A. M. Alayba, "Oblivious transfer-based authentication and privacy preserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, vol. 12, pp. 100152–100166, 2024.

[55] R. C. Motta, K. M. De Oliveira, and G. H. Travassos, "On challenges in engineering IoT software systems," in *Proc. the XXXII Brazilian Symposium on Software Engineering*, 2018, pp. 42–51.
[56] H. Ramesh, N. Ismail, N. A. A. Rahman, and A. Ali, "Phishguard: AI-driven graph-based analysis for smarter email security," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, pp. 31–45, 2026.
[57] B. A. Mohammed, M. A. Al-Shareeda, Z. G. A. Mekhlafi, J. S. Alshudukhi, and K. A. A. Dhlan, "Hafc: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251–6261, 2024.
[58] S. Ang, M. Ho, S. Huy, and M. Janarthanan, "A multi-layered adaptive cybersecurity framework for the banking sector integrating next-gen firewalls with ai-driven IDPS," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, pp. 67–76, 2026.
[59] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, and A. Abdildayeva, "An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial IoT," *Sensors*, vol. 25, no. 8, 2395, 2025.
[60] P. Li, J. Xia, Q. Wang, Y. Zhang, and M. Wu, "Secure architecture for Industrial Edge of Things (IEoT): A hierarchical perspective," *Computer Networks*, vol. 251, 110641, 2024.
[61] R. Ouyang, J. Wang, H. Xu, S. Chen, X. Xiong, A. Tolba, and X. Zhang, "A microservice and serverless architecture for secure IoT system," *Sensors*, vol. 23, no. 10, 4868, 2023.
[62] T. Hasan, A. Akhunzada, T. Giannetsos, and J. Malik, "Orchestrating SDN control plane towards enhanced IoT security," in *Proc. 2020 6th IEEE Conference on Network Soft Webization*, 2020, pp. 457– 464.
[63] G. P. Bhandari, G. Assres, N. Gavric, A. Shalaginov, and T.-M. Grønli, "Iotvulcode: AI-enabled vulnerability detection in software products designed for IoT applications," *International Journal of Information Security*, vol. 23, no. 4, pp. 2677–2690, 2024.
[64] A. A. Zuraiqi and D. Greer, "Static analysis of IoT firmware: Identifying systemic vulnerabilities with RMMIDL," in *Proc. 2025 IEEE/ACM 6th International Workshop on Engineering and Cybersecurity of Critical Systems*, 2025, pp. 7–14.
[65] G. Yadav, K. Paul, A. Allakany, and K. Okamura, "IoT-pen: An e2e penetration testing framework for IoT," *Journal of Information Processing*, vol. 28, pp. 633–642, 2020.
[66] M. Hatami, S. Cespedes, and J. W. Atwood, "A framework for secure autonomic IoT device management in constrained networks," in *Proc. 2025 Applied Networking Research Workshop*, 2025, pp. 150–156.
[67] A. Gampel and T. Eveleigh, "Model-based systems engineering cybersecurity risk assessment for industrial control systems leveraging NIST risk management framework methodology," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 204–221, 2025.
[68] A. Yassin and M. Almaiah, "Cyber security risk assessment for determining threats and countermeasures for banking systems," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, Jan. 2026.
[69] O. Aljumaiah, W. Jiang, S. Reddy Addula, and M. Amin Almaiah, "Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework," *Journal of Cyber Security and Risk Auditing*, vo. 2025, no. 2, pp. 12–26, Apr. 2025.
[70] M. G. Spina, A. Boukerche, and F. De Rango, "An IoE-powered framework for adaptive energy-security trade-off in IoT," *IEEE Network, Early Access*, vol. 40, no. 2, pp. 65–71, 2025.
[71] M. Schicchi, K. Vallittu, B. Crispo, P. Sainio, and S. Virtanen, "Security in DevOps: Understanding the most efficient way to integrate security in the agile software development process," M.S. thesis, Dept. Comput. Sci., Univ. of Turku, 2020.
[72] H. Sharma, "Blockchain-based supply chain framework in IoT with trust-driven hybrid consensus," in *Proc. 4th International Conference on the Leadership and Management of Projects in the Digital Age (ICLAMP),* 2025, pp. 269–278.
[73] A. Moin, M. Challenger, A. Badii, and S. Gunnemann, "A model driven approach to machine learning and software modeling for the Iot: Generating full source code for smart internet of things (iot) services and Cyber-Physical Systems (CPS)," *Software and Systems Modeling*, vol. 21, no. 3, pp. 987–1014, 2022.
[74] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, "A secure and finegrained scheme for data security in industrial IoT platforms for smart city," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7982–7990, 2020.
[75] J. Subramani *et al*., "Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANS," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3484–3491, 2021.
[76] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040–1051, 2018.
[77] M. Mudassar, Y. Zhai, and L. Lejian, "Adaptive fault-tolerant strategy for latency-aware IoT application executing in edge computing environment," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13250–13262, 2022.
[78] A. Alhosban, Z. Malik, K. Hashmi, B. Medjahed, and H. Al-Ababneh, "A two phases self-healing framework for service-oriented systems," *ACM Transactions on the Web (TWEB)*, vol. 15, no. 2, pp. 1–25, 2021.
[79] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A fog computing and blockchain-based anonymous authentication scheme to enhance security in VANET environments," *Engineering, Technology and Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, 2025.
[80] G. Cheng, Y. Wang, S. Deng, Z. Xiang, X. Yan, P. Zhao, and S. Dustdar, "A lightweight authentication-driven trusted management framework for IoT collaboration," *IEEE Transactions on Services Computing*, vol. 17, no. 3, pp. 747–760, 2024.
[81] J. Giao, A. A. Nazarenko, F. Luis-Ferreira, D. G. Alves, and J. Sarraipa, "A framework for Service-Oriented Architecture (SOA)-based IoT application development," *Processes*, vol. 10, no. 9, 1782, 2022.
[82] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, "Decentralized blockchain-based trust management protocol for the internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1292–1306, 2020.
[83] S. Anasuri, "Zero-trust architectures for multi-cloud environments," *International Journal of Emerging Trends in Computer Science and Information Technology*, vol. 3, no. 4, pp. 64–76, 2022.
[84] F. Alserhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design," *Sensors*, vol. 25, no. 15, 4720, 2025.
[85] I. Ungurean and N. C. Gaitan, "A software architecture for the industrial internet of things—A conceptual model," *Sensors*, vol. 20, no. 19, 5603, 2020.
[86] Y. G. Hassan, A. Collins, G. O. Babatunde, A. A. Alabi, and S. D. Mustapha, "AI-powered cyber-physical security framework for critical industrial IoT systems," *Machine learning*, vol. 27, pp. 1158–1164, 2023.
[87] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Software-defined networking for cyber resilience in Industrial Internet of Things (IIoT)," *Modeling and Design of Secure Internet of Things*, pp. 453–477, 2020.
[88] M. Bayesh and S. Jahan, "Embedding security awareness in IoT systems: A framework for providing change impact insights," Applied Sciences, vol. 15, no. 14, 7871, 2025.
[89] J. Marchang, J. McDonald, S. Keishing, K. Zoughalian, R. Mawanda, C. D. Bugard, and N. Bouillet, "Secure by design real-time IOMT architecture for e-health Population Monitoring (RTPM)," 2024.
[90] S. Thangam and S. S. Chakkaravarthy, "An edge enabled region-oriented DAG-based distributed ledger system for secure V2X communication," *KSII Transactions on Internet and Information Systems*, vol. 18, no. 8, pp. 2253–2277, 2024.
[91] S. Longari, A. Cannizzo, M. Carminati, and S. Zanero, "A secure by design framework for automotive on-board network risk analysis," in *Proc. 2019 IEEE Vehicular Networking Conference (VNC)*, 2019, pp. 1–8.
[92] B. Paul and M. Rao, "Zero-trust model for smart manufacturing industry," *Applied Sciences*, vol. 13, no. 1, 221, 2022.
[93] R. Roman, R. Arjona, and I. Baturone, "A lightweight remote attestation´ using PUFS and hash-based signatures for low-end IoT devices," *Future Generation Computer Systems*, vol. 148, pp. 425–435, 2023.
[94] T. Coito, M. S. Martins, J. L. Viegas, B. Firme, J. Figueiredo, S. M. Vieira, and J. M. Sousa, "A middleware platform for intelligent

automation: An industrial prototype implementation," *Computers in industry*, vol. 123, 103329, 2020.
[95] A. Hussain *et al*., "Security framework for IoT based real-time health applications," Electronics, vol. 10, no. 6, 719, 2021.