Proceedings of the International Conference on Modern Sustainable Systems (CMSS-2025)
DVD Part Number: CFP250Q9-DVD; ISBN: 979-8-3315-6509-1

Enhancing Industrial IoT Security with AI and Cloud Computing: A Review of Threats and Solutions

S.Saravana kumar,
Research Scholar,
Department of Computer Science & IT,
School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS),
Chennai, Tamil Nadu, India,
saravana.subbaraj@gmail.com

Dr.Balaji Kannan
Assistant Professor,
Department of Computer Science & IT,
School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS),
Chennai, Tamil Nadu, India,
balajikannan.scs@vistas.ac.in

Abstract: **Installing and using the Industrial Internet of Things (IIoT) technology at a higher rate has led to enormous changes in the industrial activities and a paradigm shift in the way industries operate, as well as in the manner in which management of assets and supply chain management is done. The digitalisation process allows us to collect data in real-time, have a predictive maintenance, and implement smart automation, which significantly increases operational efficiency and productivity. But this fast transformation has opened the door to a major issue of cybersecurity that poses a risk to integrity, confidentiality, and availability of important industrial infrastructure. An enlargement of networked things and technologies raises the attack surface such that IIoT ecosystems experience a more significant risk of being attacked by OT, like data breaches, ransomware, industrial espionage. The present paper is a detailed account of the key security threats affecting IIoT settings, which is then followed by a detailed analysis of how the features of artificial intelligence (AI) solutions and cloud-based platforms could be used to improve threat detection, incident response, and system resiliency. The combination of an analysis of recent threat vectors, new vulnerabilities, and new defense capabilities allows proposing a framework of best practices in securing IIoT infrastructure, within the study. Although AI-based threat detection and cloud-based security orchestration have become prime technological solutions, the results of further research and optimization are required to establish a workable and scalable implementation of security.**

Keywords: Industrial IoT, Cybersecurity, Artificial Intelligence, Cloud Computing, Threat Intelligence, Security Orchestration

1. Introduction

Operation Technology (OT) establishes connections with InformationTechnology (IT) through Industrial Internet of Things (IIoT) to generate data-centric networks combining industrial components with control systems and sensors and mechanical units that deliver automated decision systems and systems management capabilities. Analysts project that the global IIoT market will reach $1.1 trillion by 2028 through 22.8% yearly growth across 2023 to 2028 [1]. The IIoT market expands rapidly because industrial operators expect operational efficiency improvements as well as predictive maintenance capabilities that increase productivity throughout all industrial areas. When industrial control systems (ICS) split off from isolated networks by connecting to internet technologies the vulnerability to cyber threats significantly increased. IIoT environments deal with security issues beyond common IT systems because they need to prioritize operational speed alongside basic safety components in outdated equipment alongside severe threats that create safety dangers for personnel and disrupt manufacturing processes [2]. The security solutions designed for IT networks do not address the unique problems found in IIoT system deployment environments. Security approaches need to integrate operational industrial availability needs with business system confidentiality and integrity requirements when IT systems connect to OT networks [3]. IIoT deployments become harder to protect because different vendors supply parts with various security features to these heterogeneous systems. AI technology with cloud computing solutions enables developers to build adaptable enhanced security strategies that protect existing IIoT challenges. Artificial intelligence technology offers security protection by detecting irregular patterns while forecasting threats and implementing automated defenses so data analysis through security orchestration and central management can be achieved by integrating cloud infrastructure systems [4]. The paper evaluates modern security challenges affecting Industrial Internet of Things deployments by studying AI-based and cloud computing security solutions available for defense. Research reveals that this paper studies IIoT threat environments through an assessment of vulnerabilities and attack vectors while exploring AI-enhanced cloud solutions for secure IIoT deployments.

2. The IIoT Threat Landscape

2.1 Evolution of IIoT Security Threats

The security environment surrounding Industrial IoT infrastructure experienced substantial development from single incidents toward complex Attack focusing on critical infrastructure facilities during the last decade. Stuxnet became the first recorded industrial attack in 2010 when it manipulated industrial systems by infected their programmable logic controllers (PLCs). Modern threats in industrial environments have advanced significantly since their first appearance because attackers now create unique tools and techniques made to disrupt industrial facilities. During the last few years nation-state actors alongside advanced persistent threat (APT) groups have elevated their focus towards IIoT[5] systems to achieve espionage and sabotage as well as gain strategic benefits. Several notable industrial targeted cyber-attacks happened in 2015 where Ukrainian power grids were Attack followed by the TRITON malware Attack on safety instrumented systems in 2017 and the 2021 Florida water treatment facility strike [6,] [7], [8]. The recent attacks confirm that threat actors continue to develop their skills and show expanding interest in industrial systems. The availability of affordable attack tools together with ransomware-as-a-service platforms now allows cybercriminals to easily attack industrial sites. The

colonial pipeline ransomware attack from 2021 revealed that industrial operations disruptions cause extensive damage by disrupting fuel distribution through various parts of the United States [9].

2.2 Key Vulnerabilities in IIoT Environments

An industrial Internet of Things environment contains specific systematic weaknesses which set it apart from standard IT system infrastructure.

2.2.1 Legacy Systems and Technology Gaps

Industrial facilities maintain outdated systems which were built originally without security factors which leads to their inability to perform encryption protocols or authentication tasks and their inability to receive system updates. Since industrial systems operate with outdated firmware and operating systems containing known security flaws they cannot receive critical updates because operational limitations from vendors prevent easy software deployment [10]. Industrial equipment operates for extended periods of time reaching multiple decades in service rather than annual stimuli posing significant difficulties for protection.

2.2.2 Expanded Attack Surface

The connection between industrial systems previously maintained in air-gapped isolation and internet-accessible technologies increased the number of targeted entry points. Attackers can exploit the various connection points found in each sensor, controller, gateway or edge device. The CyberX research shows industries using outdated operating systems in 71% of their sites coupled with 64% of industrial sites sending unencrypted passwords through their networks [11].

2.2.3 Supply Chain Vulnerabilities

Overlapping security practices tend to appear across multiple vendors who contribute components for IIoT deployments that generate lengthy supply chains. Security breaches in any network component will impact the entire system protection level. In 2020 the SolarWinds supply chain attack exposed extensive damage that software supply chain weaknesses created for many different organizations worldwide [12].

2.2.4 Protocol Vulnerabilities

Industrial protocols mostly focus on performance rather than security during their creation because they contain no method for encryption or authentication systems as well as no mechanism for integrity checking. The development of protocols including Modbus DNP3 and BACnet occurred when cybersecurity issues were not yet essential so implementing security measures on these protocols remains highly complicated [13].

2.2.5 Comparative Analysis

The table 1 summarises the results of recent works related to the security of IoT, MEC, Fog and Cloud and identifies the areas of interest, core technologies, security issues, and primary contributions such as analyzing AI-based frameworks, blockchains and blockchain and federated DDoS detection, and layered threat modelling.

Table 1: Comparative analysis

Authors (Year)	Focus Area	Key Technologies	Security Focus	Main Contribution
C. Wang et al. (2023)	Mobile Edge Computing (MEC) with AI	AI, Edge Computing, Privacy-Preserving Models	Threat detection, intrusion response, trust management in MEC	Explores how AI enhances MEC security and privacy; proposes intelligent frameworks for anomaly detection and data protection.
L. Albshaier et al. (2024)	IoT, Cloud, Blockchain Integration	IoT, Cloud Computing, Blockchain	Confidentiality, trust, interoperability	Reviews hybrid architecture security challenges and outlines blockchain's role in ensuring secure data handling.
F. Rezaeibagha et al. (2023)	Secure Outsourced Computation	Cloud Computing, Homomorphic Encryption	Data confidentiality, secure computation for multi-user environments	Proposes a privacy-preserving computation model supporting multiple users on cloud-based IoT platforms.
V. Hassija et al. (2019)	IoT Security Landscape	IoT, Cybersecurity Frameworks	Threat taxonomy, authentication, data security	Comprehensive survey on IoT security threats and proposed solutions across various domains like healthcare, smart cities.

J. Singh et al. (2021)	Security in MEC-enabled IoT	MEC, Access Control, Trust Hierarchy	Layered trust models, secure data access	Introduces a hierarchical trust-based security paradigm tailored for MEC-IoT integration.
T. -A. N. Abdali et al. (2021)	Fog Computing Overview	Fog Architecture, Distributed Systems	Data integrity, availability, open security issues	Detailed review of fog computing components and security limitations; highlights research gaps and practical benefits.
M. A. Belay, A. Rasheed, P. S. Rossi (2025)	Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection	Digital Twin, Federated Learning, Semi-Supervised Learning, Industrial IoT	DDoS detection, threat mitigation in IIoT	Proposes a federated semi-supervised learning approach using knowledge distillation to detect DDoS attacks in industrial IoT environments.
A. K. Dwivedi, N. B. Kar, A. Shivhare (2025)	Cybersecurity Threat Modeling of IoT Security Design Patterns	IoT Security Patterns, Cyber Threat Modeling	Threat modeling, secure design principles	Develops a threat modeling approach to evaluate and strengthen IoT security design patterns for improved resilience.
D. Aggarwal, A. B. Saxena, D. Sharma (2025)	Mitigating Cybersecurity Risks in IoT	Layered Security Architecture, Threat Detection	Multi-layer threat detection, risk prevention	Introduces a layered approach for detecting and preventing cybersecurity threats in IoT systems, enhancing overall security posture.

3. AI-Driven Security Solutions for IIoT

The special security needs of IIoT environments can be addressed effectively through promising AI technologies. This section analyzes the major AI applications which protect IIoT systems.

3.1 Anomaly Detection and Behavioral Analysis

New threats present in IIoT environments challenge the effectiveness of signature-based detection solutions which are now insufficient for protecting these environments. A more efficient anomaly detection method involves AI technology by creating operational baseline patterns which allow detection of security incidents through deviations. The ability of machine learning techniques to detect industrial anomalies is well demonstrated through their unsupervised learning and deep learning and reinforcement learning algorithms. Through these methods organizations can discover minor indicators of system breakdown or security breaches manifested via technological systems and network data and system status information: Machine algorithms that operate without supervision can detect normal operational clusters and spot unusual behaviors autonomously since they need no labeled training data which provides benefits to sparse attack datasets. Analogous to autoencoders and recurrent neural networks (RNNs) demonstrate effective modeling of complex temporal industrial process patterns while detecting anomalies in time-series data derived from sensors and control systems according to research. Continuous reinforcement learning modifies detection models through feedback processing so the systems evolve better accuracy while decreasing false positive notifications. The research conducted by Ghaeini et al. proved that machine learning models succeed in detecting industrial control system attacks with 99.9% precision when scanning for certain threat types while surpassing standard rule-based detection screening standards.

3.2 Threat Intelligence and Predictive Analytics

AI threat intelligence systems analyze numerous data points from different sources to find new security risks that affect particular IIoT implementation environments. Natural language processing technology allows platforms to identify security-related insights from security publications and forums and security alerts before security threats can be addressed.

Public security incidents can undergo forecasting using historical datasets combined with system state records and information gathered from threat intelligence sources. These systems find security breach precursor patterns to warn security teams before attacks occur so preventive measures can be taken.

4. Cloud Computing for IIoT Security

The IIoT environment benefits from security solutions implemented through cloud computing infrastructure. This

part details the essential components of cloud-based security solutions for industrial environments.

4.1 Centralized Security Monitoring and Management

Cloud-based platforms grant organizations complete monitoring capabilities together with management functions across multipoint IIoT systems. The deployment of Security Information and Event Management (SIEM) systems in cloud environments allows organizations to merge multiple security data streams from different sources thereby enabling they can monitor industrial operations thoroughly. Research by [13] supports this claim. Scalable resources in cloud infrastructure allow users to analyze massive IIoT security telemetry data better than on-site infrastructure could handle. This functionality becomes crucial for implementing security approaches using AI as discussed in Section 3.

4.2 Secure Device Management and Updates

The distribution of IIoT deployments brings difficulties to administrators when they need to maintain their current firmware state and security patches. Organizations can deploy cloud-based platform services to distribute secure system updates across large device networks therefore maintaining security identity across all devices without interrupting daily operations . Security platforms deploy staged updates along with validation protocols that automatically trigger rollback procedures in order to handle critical system update risks. Update management under one central point allows organizations to deliver security patches quickly throughout their full IIoT system thus shortening the time of exposure to newly emerging threats [14].

4.3 Secure Communication and Data Processing

Cloud service providers deliver strong security protection for information while it is transferred along with its storage status. IIoT devices can maintain secure communications with cloud platforms through TLS with mutual authentication protocols that protect data from the start until the end of its lifecycle.

The current cloud platforms use complex encryption key management technologies and Hardware Security Modules (HSMs) as well as secure enclaves to defend both sensitive information and cryptographical operations. The capabilities provide critical protection for IIoT applications dealing with intellectual property together with operational parameters and personally identifiable information.

4.4 Scalable Security Analytics

The elastic cloud computing infrastructure makes possible large-scale security analysis operations which would cost impractically high to run on local premises. Organizations gain the ability to distribute computing power for security analytics depending on existing threat levels through dynamically allocated resources and this allows for enhanced surveillance during threat-prone times. Security analytics systems deployed in cloud environments utilize "security data lakes" which keep security telemetry data stored for lengthy durations to conduct retrospective analysis during threat discovery. Security teams have the ability to find indicators of compromise which traditional detection methods overlooked through this system [15].

4.5 Security-as-a-Service Models

Cloud platforms continually develop customized security solutions which target IoT alongside industrial systems requirements. Such services deliver managed security expertise directly to organizations without obligating them to develop their internal security expertise.

Security-as-a-Service models provide four main services for IIoT environments which are described.

Managed detection and response (MDR) stands as a security service to benefit industrial businesses.

- Vulnerability scanning and management
- The protection services include Distributed denial of service (DDoS) protection.
- Specialized threat intelligence for industrial environments
- Compliance monitoring and reporting

The security services provide organizations with essential support through expanded capabilities especially for companies having restricted security departments or focusing on enhancing their security expertise in particular areas.

5. Proposed methodology

Integrated Framework for IIoT Security

Our analysis of threats along with vulnerabilities in addition to emerging solutions leads to an integrated framework which utilizes AI and cloud capabilities to upgrade IIoT security. This structure evaluates industrial characteristics with methods which utilize the best aspects of each technology.

5.1 Framework Overview

The proposed framework has five connected layers which combine to offer total security to IIoT deployment systems.

Let the total security of the IIoT framework be represented by Stotal. The framework consists of five distinct, interconnected layers. We can define the set of layers,

$$L = \{L_{\text{dev}}, L_{\text{net}}, L_{\text{data}}, L_{\text{app}}, L_{\text{gov}}\}$$

Where:

$$L_{\text{dev}} = \text{Device Security Layer}$$
$$L_{\text{net}} = \text{Network Security Layer}$$
$$L_{\text{data}} = \text{Data Security Layer}$$
$$L_{\text{app}} = \text{Application Security Layer}$$
$$L_{\text{gov}} = \text{Governance and Compliance Layer}$$

The security of each layer, S(Li), is a function of its specific security measures, normalized to a value between 0 (no security) and 1 (perfect security) The Device Security Layer requires individual IIoT devices to establish proper security measures which remain securely configured from product inception to complete termination.The security of this layer depends on device integrity (c), secure lifecycle management (m), and patch status (p).

$$S(L_{\text{dev}}) = w_{cc} + w_{mm} + w_{pp}$$
$$w_{cc} + w_{mm} + w_{pp} = 1$$

The Network Security Layer protects all device-to-cloud communications as well as carrying out network monitoring and segmentation initiatives. this layer's security is determined by the protection of data in transit (t), at rest (r), and through access controls (a).

$$S(L_{\text{data}}) = w_{tt} + w_{rr} + w_{aa},$$
$$w_t + w_r + w_a = 1$$

- The Data Security Layer guarantees protection of information from its origin at devices and throughout its flow from transmissions to processing and storage right through archiving or destruction stage.
- The Application Security Layer requires developers to follow secure practices during the entire development cycle of operating applications and services in IIoT platforms.
- The Governance and Compliance Layer creates policies and procedures and implements oversight systems which drive uniform security control execution and standard and regulation compliance. In the figure 1 to illustrates the relationships between these layers and the integration of AI and cloud capabilities throughout the framework.

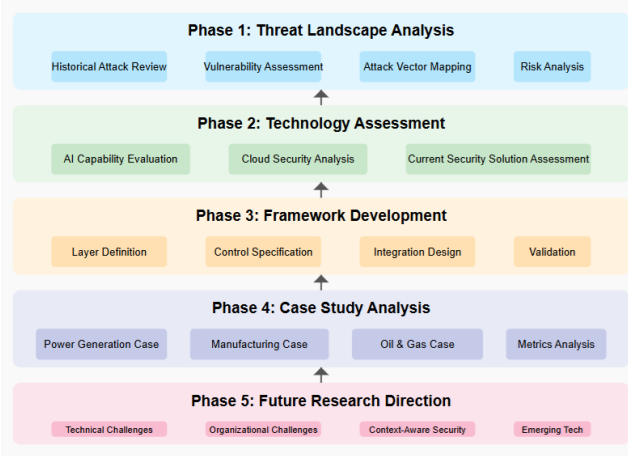

Figure 1: illustrates the relationships between these layers and the integration of AI and cloud capabilities throughout the framework.

In a layered security model, security does not add up. The robustness of the architecture is set by the robustness of all the layers and a failing of one of those will jeopardise the whole system. Hence the overall security, Stotal, can be represented as a product of individual increased securities of layers.

$$S_{\text{total}} = \prod_{i \in \{\text{dev, net, data, app, gov}\}} S'(L_i)$$

Substituting the enhanced security function, the comprehensive model is:

$$S_{\text{total}} = S'(L_{\text{dev}}) \cdot S'(L_{\text{net}}) \cdot S'(L_{\text{data}}) \cdot S'(L_{\text{app}}) \cdot S'(L_{\text{gov}})$$

$$S_{\text{total}} = \prod_{i=1}^{5} [\, S(L_i) \cdot \Psi(A_i, C_i)\,]$$

This is a multiplicative model that makes sure that when the security of any one layer nears zero the overall security of the framework would nears zero as well, which best describes the weakest link concept in cybersecurity.

5.2 Implementation Considerations

The framework implementation needs organizations to consider multiple essential factors.

5.2.1 Risk-Based Approach

Organizations should deploy security controls with a risk-based method to allocate resources for protecting their essential assets while overcoming major threats. The method understands that not every IIoT element needs equal protective measures thus guiding organizations to use their security funds in the most effective manner [16].

Operational risk assessments must evaluate attack probabilities and calculate associated risks that endanger industrial functions and safety while affecting business targets. Organizations should schedule regular updates for their assessments which need to show accurate information reflecting enemy advances and operational changes.

5.2.2 Defense-in-Depth Strategy

Every IIoT system requires multiple security controls and technologies to establish sufficient operational protection. Organizations need to deploy defense-in-depth solutions combining various security measures across multiple layers in order to defend their essential assets from complete compromise even if one control fails[17]. Security professionals must follow this method specifically in industrial facilities because safety combined with reliability requirements take precedence. Security controls must have built-in degradation capabilities[18] which preserve critical[20] operational functions when attack compromises[21] some system components[22][23][24][25][26][27].in the table 2 Comparative Table with Research Gaps

Table 2: Comparative Table with Research Gaps

Ref. No.	Main Contribution	Research Gaps Identified
[9] J. Zhang et al., 2023	Proposes a dynamic trust-based framework enabling secure collaboration between cloud and fog layers	Lacks evaluation in large-scale, real-time IoT deployments; trust dynamics for unknown or transient nodes not deeply addressed
[10] S. Drissi et al., 2025	Summarizes recent advancements in risk evaluation methods across cloud environments	Need for unified risk taxonomy; insufficient automation in real-time risk detection and response; missing risk metrics in hybrid cloud scenarios
[11] A. Rahdari et al., 2025	Reviews secure computation and federated learning approaches in distributed settings	Model poisoning attacks still unresolved; lack of lightweight privacy-preserving protocols for low-power devices; need for benchmark datasets
[12] F. Kandah et al., 2025	Discusses architectural models and countermeasure strategies for emerging IoT threats	Inadequate defense mechanisms against zero-day attacks; limited cross-layer adaptability; performance overhead of adaptive methods
[13] A. Ahmed et al., 2022	Proposes an energy-efficient mechanism combining data aggregation and blockchain	Blockchain latency and energy cost trade-offs still high; scalability issues in high-density networks; lacks real-time blockchain offloading techniques

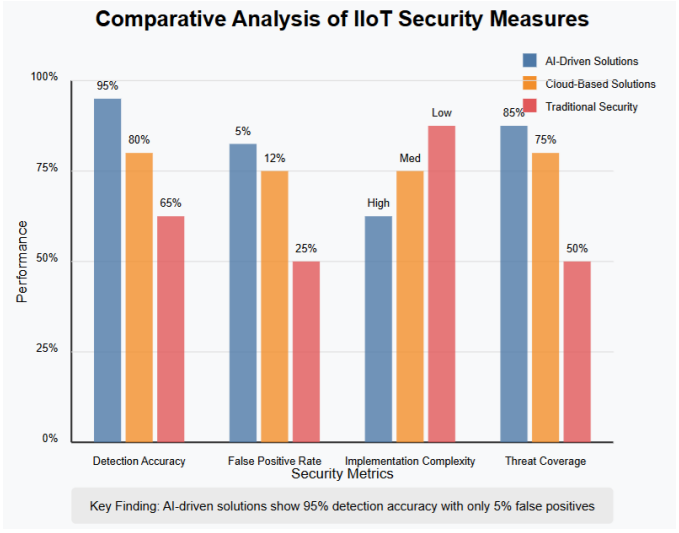

Figure 2: comparative analysis of different IIoT security approaches

In the figure 2 The analytical aspect of the comparative studies of the IIoT security metrics reveals the advanced outcomes of the AI-powered solutions in comparison with the traditional ones in terms of the main security indicators. The detection rate of these solutions stands at 95%, which is very high as compared to cloud-based (80%) and the traditional security (65%). Moreover, AI-based solutions possess a very small false positive rate of only 5%, as opposed to 12 and 25 percent of cloud-based and conventional systems accordingly. The solutions based on AI are rated highly on their implementation complexity, those based on the cloud are in the medium range, and traditional security is low, thus signifying the trade-off between the degree of eligibility and ease of difficulties. In threat coverage, AI-driven services are again on top with 85 percent, followed by cloud-based with 75 percent and with the traditional measures with 50 percent. The major conclusion is that the AI-based methods offer outstanding detection rates and the low rate of false alerts, which make them the strongest IIoT security option among the considered ones.

Figure 3: System Integration, Security Focus, Data Privacy, Edge/Fog Computing, Cloud Integration, and Application Domain.

Figure 3 show the comparative graph of both IoT and cloud security research papers gives one a graphical overview of the comparative strengths and weaknesses of each of the

research papers in the areas of major evaluation, which include system integration, security focus, data privacy, edge/fog, cloud integration, and application domain. These different studies are color coded in bar graphs so that one can directly compare the two different papers on particular categories. The highest results belong to the categories of Security Focus and Data Privacy, where some of the papers gain almost perfect results which means thorough coverage and developed solutions in these fields. On the other hand, poorer results in "Edge/Fog Computing" and "System Integration" indicate the sections as less covered by the majority of papers in question. The subjects of "Cloud Integration" and "Application Domain" depict a wide range of findings displaying differences in depth of analysis and its practical usages in the scanned literature. The total trend proves that although studies show high grades in a few areas of IoT and cloud security, none of them get excellent grades in all categories, which proves the possibility of this research area as multidimensional.

7. Conclusion

The industry use of the IoT technology is transforming industry through its efficiency, and predictive posterity, and unlocking value creation in manufacturing, energy, logistics, and various markets. IoT enables real-time look, data-based management, and innovation. Nevertheless, widespread application of networked devices entails complex security threats, involving unauthorized access and concealment, manipulation of hardware, and interference that may result in an expensive downward time or loss of data that otherwise creates sensitive operational information. IIoT offers significant potential; however, to achieve it, the infra software requires solid cybersecurity, to secure its structure and compliance. The suggested security model is based on the threat detection supported by the AI and security management being performed in the cloud to provide the industry-specific protection suiting the particular demands of industrial systems. As industry 4.0 adoption intensifies, security should be emphasized in the design, supported during implementation, and even in the lifetime. Technical and organizational types of problems in cybersecurity will have to be regularly researched, innovated, and assessed. The sustainability of IIoT security is based on cooperative collaboration of industry practitioners, academia, and technology suppliers and the occurrence of resilient systems and sustainable and smart manufacturing.

References

[1]. S. Drissi, M. Chergui and Z. Khatar, "A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements," in IEEE Access, doi: 10.1109/ACCESS.2025.3561123

[2]. S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," IEEE Internet Computing, vol. 22, no. 2, pp. 42-51, 2023.

[3]. C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li and D. O. Wu, "The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22008-22032, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304318.

[4]. L. Albshaier, A. Budokhi and A. Aljughaiman, "A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain," in IEEE Access, vol. 12, pp. 109560-109595, 2024, doi: 10.1109/ACCESS.2024.3435845.

[5]. F. Rezaeibagha, Y. Mu, K. Huang, L. Chen and L. Zhang, "Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 217-228, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3087614.

[6]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[7]. J. Singh, Y. Bello, A. R. Hussein, A. Erbad and A. Mohamed, "Hierarchical Security Paradigm for IoT Multiaccess Edge Computing," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5794-5805, 1 April1, 2021, doi: 10.1109/JIOT.2020.3033265.

[8]. T. -A. N. Abdali, R. Hassan, A. H. M. Aman and Q. N. Nguyen, "Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues," in IEEE Access, vol. 9, pp. 75961-75980, 2021, doi: 10.1109/ACCESS.2021.3081770.

[9]. J. Zhang, T. Li, Z. Ying and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1546-1561, 1 April-June 2023, doi: 10.1109/TCC.2022.3147226.

[10]. S. Drissi, M. Chergui and Z. Khatar, "A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements," in IEEE Access, vol. 13, pp. 76289-76307, 2025, doi: 10.1109/ACCESS.2025.3561123.

[11]. A. Rahdari et al., "A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond," in IEEE Open Journal of the Communications Society, vol. 6, pp. 3710-3744, 2025, doi: 10.1109/OJCOMS.2025.3560034.

[12]. F. Kandah, T. Mendis, L. Medury, H. Sherawat and H. Wang, "Navigating IoT Security: Architectures, Emerging Threats, and Adaptive Countermeasures," in IEEE Access, vol. 13, pp. 98888-98908, 2025, doi: 10.1109/ACCESS.2025.3576355.

[13]. A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," in IEEE Access, vol. 10, pp. 11404-11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[14]. Y. Zhang, J. Ren, J. Liu, C. Xu, H. Guo and Y. Liu, "A Survey on Emerging Computing Paradigms for Big Data," in Chinese Journal of Electronics, vol. 26, no. 1, pp. 1-12, January 2017, doi: 10.1049/cje.2016.11.016.

[15]. R. R. Irshad et al., "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User

Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," in IEEE Access, vol. 11, pp. 105479-105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[16]. J. Cui, B. Li, H. Zhong, G. Min, Y. Xu and L. Liu, "A Practical and Efficient Bidirectional Access Control Scheme for Cloud-Edge Data Sharing," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 2, pp. 476-488, 1 Feb. 2022, doi: 10.1109/TPDS.2021.3094126.

[17]. S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," in IEEE Access, vol. 8, pp. 188082-188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[18]. W. -Z. Zhang et al., "Secure and Optimized Load Balancing for Multitier IoT and Edge-Cloud Computing Systems," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8119-8132, 15 May15, 2021, doi: 10.1109/JIOT.2020.3042433.

[19]. I. A. Elgendy, W. -Z. Zhang, Y. Zeng, H. He, Y. -C. Tian and Y. Yang, "Efficient and Secure Multi-User Multi-Task Computation Offloading for Mobile-Edge Computing in Mobile IoT Networks," in IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2410-2422, Dec. 2020, doi: 10.1109/TNSM.2020.3020249.

[20]. H. Zhang et al., "Secure Edge-Aided Computations for Social Internet-of-Things Systems," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 76-87, Feb. 2022, doi: 10.1109/TCSS.2020.3030904.

[21]. I. Gupta, A. K. Singh, C. -N. Lee and R. Buyya, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," in IEEE Access, vol. 10, pp. 71247-71277, 2022, doi: 10.1109/ACCESS.2022.3188110.

[22]. B. Yuan et al., "Leakage of Authorization-Data in IoT Device Sharing: New Attacks and Countermeasure," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 3196-3210, July-Aug. 2024, doi: 10.1109/TDSC.2023.3323713.

[23]. Z. Qu, S. Kumari, M. S. Obaidat, B. A. Alzahrani and H. Xiong, "Traceable Attribute-Based Encryption With Equality Test for Cloud Enabled E-Health System," in IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 9, pp. 5033-5042, Sept. 2024, doi: 10.1109/JBHI.2023.3321939.

[24]. M. A. Belay, A. Rasheed and P. S. Rossi, "Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection," 2025 IEEE Symposium on Computational Intelligence in Security, Defence and Biometrics Companion (CISDB Companion), Trondheim, Norway, 2025, pp. 1-5, doi: 10.1109/CISDBCompanion65092.2025.11010678.

[25]. A. K. Dwivedi, N. B. Kar and A. Shivhare, "Cyber Security Threat Modeling of IoT Security Design Patterns," 2025 International Conference on Intelligent and Cloud Computing (ICoICC), Bhubaneswar, India, 2025, pp. 1-6, doi: 10.1109/ICoICC64033.2025.11052094.

[26]. D. Aggarwal, A. B. Saxena and D. Sharma, "Mitigating Cybersecurity Risks in IoT: A Layered Approach to Threat Detection and Prevention," 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2025, pp. 501-505, doi: 10.1109/ICSADL65848.2025.10933329.

[27]. S. S. Makubhai, G. R. Pathak and P. R. Chandre, "Exploring the Trade-Offs Between Blackbox and Explainable AI: A Comparative Study," 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2023, pp. 1-8, doi: 10.1109/ICCUBEA58933.2023.10391996