International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2410612425

Recent Advances in IoT Security for Real-Time Data Integration

Abdul Hameed Mohammed

7-eleven, USA

ARTICLEINFO

Article History:

Accepted : 20 Nov 2024

Published: 12 Dec 2024

Publication Issue

Volume 10, Issue 6

November-December-2024

Page Number

2229-2239

ABSTRACT

This article examines the latest advancements in IoT security, focusing on protecting real-time data in distributed networks. The article explores how emerging technologies like blockchain, zero-trust architecture, and machine learning are addressing critical security challenges in IoT ecosystems. The article analyzes the evolution of security threats and solutions across various sectors, including healthcare, manufacturing, and financial services. Special attention is given to the integration of advanced security frameworks that balance robust protection with operational efficiency. The article also investigates industry-specific implementations and their effectiveness in addressing unique security requirements while maintaining performance standards. Finally, the article looks ahead to future directions in IoT security, including quantum-ready security measures, edge computing security, and automated security operations.

Keywords: IoT Security, Blockchain-Based Authentication, Zero-Trust Architecture, Machine Learning-Driven Security, Edge Computing Security

Introduction

The rapid proliferation of Internet of Things (IoT) devices has fundamentally transformed the landscape of real-time data collection and processing across industries. According to recent IEEE research, the global IoT infrastructure is experiencing unprecedented growth, with machine-to-machine (M2M) connections projected to constitute 50% of the total device and connection base by 2024 [1]. This expansion is particularly evident in industrial sectors, where the implementation of IoT-enabled smart manufacturing solutions has led to a 27% increase in operational efficiency across monitored facilities.

The exponential growth of IoT ecosystems has introduced complex security challenges that traditional cybersecurity approaches struggle to address effectively. Cisco's comprehensive analysis reveals that approximately 66.2% of IoT devices remain vulnerable to various security threats, with about 48.2% of organizations reporting at least one security breach in their IoT infrastructure within the past year [2]. These vulnerabilities are particularly concerning as the average IoT device processes 4.51 terabytes of sensitive data annually, creating significant risk exposure points across distributed networks.

The integration of IoT devices in critical infrastructure sectors presents unique security challenges, with real-time data protection requirements that must balance security robustness against operational efficiency. Recent studies from IEEE indicate that conventional security protocols introduce an average latency of 150-200 milliseconds in IoT communications, which can significantly impact time-critical applications [1]. This latency challenge is particularly acute in healthcare and industrial control systems, where real-time data processing is essential for operational safety and efficiency. The manufacturing sector, for instance, reports that even a 50-millisecond delay in data transmission can result in production line inefficiencies costing an average of $10,000 per minute in large-scale operations [2].

Contemporary IoT architectures must evolve to address these emerging security challenges while maintaining the performance requirements of modern applications. The latest research indicates that advanced security frameworks implementing AI-driven threat detection have successfully reduced security incident response times by 74%, while maintaining latency increases to under 30 milliseconds [1]. These improvements are critical as the volume of IoT-generated data continues to expand, with projections indicating that IoT devices will generate over 79.4 zettabytes of data annually by 2025 [2].

The Evolution of IoT Security Challenges

As IoT networks become more sophisticated and interconnected, they face increasingly complex security threats that evolve at an unprecedented pace. Recent security assessments reveal that IoT networks encounter an average of 5,200 attacks per month, with a particularly concerning trend showing that 48% of devices still use default passwords, creating significant vulnerabilities in network infrastructure [3]. Traditional perimeter-based security models have proven inadequate in addressing these emerging threats, as demonstrated by the 89% increase in successful IoT-targeted attacks over the past 18 months.

Device Heterogeneity presents a fundamental security challenge in IoT implementations, with recent IEEE research indicating that modern industrial IoT networks typically integrate between 15-20 different types of devices from multiple manufacturers [4]. This diversity manifests in varying security capabilities, with approximately 35% of devices supporting advanced encryption standards (AES-256), while 45% are limited to basic encryption protocols, and 20% lack native encryption support entirely. The heterogeneity challenge is further complicated by the fact that 67% of IoT devices in industrial settings use

proprietary protocols that often lack standardized security frameworks, leading to potential vulnerabilities in cross-device communication [3].

Resource Constraints significantly impact security implementation across IoT ecosystems, particularly in edge devices where processing power and memory are limited. Recent analysis shows that 73% of deployed IoT sensors operate with less than 128KB of RAM and processors running at sub-500MHz speeds [4]. These constraints create significant challenges for implementing robust security measures, as modern encryption protocols require a minimum of 256KB RAM for effective operation. Studies indicate that implementing standard security protocols on resource-constrained devices can increase power consumption by 31-45%, potentially reducing device operational lifespan by up to 60% [3].

Real-time requirements introduce critical challenges in IoT security implementations, particularly in industrial control systems where timing is crucial. According to IEEE research, modern industrial IoT applications require a maximum latency of 5-8 milliseconds for effective operation, while security overhead typically adds 12-15 milliseconds of processing time [4]. This timing challenge is particularly evident in smart manufacturing environments, where security-induced delays impact real-time control systems. Analysis shows that approximately 82% of industrial IoT deployments must balance between security and performance, with 34% of organizations reporting that they have had to disable certain security features to maintain operational efficiency [3]. The healthcare sector faces even stricter requirements, with medical IoT devices requiring sub-2-millisecond latency while maintaining comprehensive security protocols, a challenge that affects 91% of connected medical devices.

Parameter	Value
Monthly Attack Frequency	5,200
Devices Using Default Passwords	48%
Devices with Proprietary Protocols	67%
Devices with <128KB RAM	73%
Power Consumption Increase	31-45%
Device Lifespan Reduction	60%
Industrial IoT Required Latency	5-8 ms
Security Overhead Latency	12-15 ms
Organizations Disabling Security Features	34%
Medical Devices Affected by Latency Requirements	91%

Table 1. IoT Security Implementation Challenges and Impact Metrics [3, 4]

Blockchain-Based Security Solutions

Blockchain technology has emerged as a transformative solution for securing IoT ecosystems, particularly in scenarios requiring immutable record-keeping and distributed trust. According to comprehensive analyses, blockchain implementation in IoT networks has demonstrated a reduction in security vulnerabilities by 42%, with particular effectiveness in preventing data tampering attacks. Studies show that organizations implementing blockchain-based security solutions have achieved a 71% improvement in data integrity verification, with transaction throughput reaching 7 transactions per second in Ethereum-based implementations [5]. The integration of blockchain technology has proven especially effective in industrial IoT environments, where distributed consensus mechanisms have reduced single points of failure by 89%.

Distributed Ledger for Device Authentication

Modern IoT networks are implementing blockchain-based identity management systems that create tamper-proof device identities, leveraging distributed ledger technology to establish trust in device authentication processes. Research indicates that

implementations using Hyperledger Fabric have achieved authentication success rates of 99.7%, with average transaction validation times of 0.8 seconds [6]. Each device maintains a unique cryptographic identity on the blockchain, utilizing ECDSA (Elliptic Curve Digital Signature Algorithm) with P-256 curves, which has shown resistance to quantum computing attacks while maintaining efficient processing times averaging 3.2 milliseconds per signature verification [5]. The distributed architecture has demonstrated particular efficiency in large-scale deployments, processing up to 3,500 authentication requests per minute while maintaining consistent latency under 100 milliseconds.

Smart Contracts for Access Control

Smart contracts have revolutionized security policy enforcement in IoT networks, with recent implementations showing significant improvements in both efficiency and reliability. Performance analysis of Ethereum-based smart contracts in IoT environments reveals average execution times of 45 milliseconds for access control operations, with gas costs averaging 21,000 units per transaction [6]. The implementation of smart contracts has reduced manual policy enforcement errors by 94%, while enabling real-time policy updates that propagate across the network within an average of 2.3 blocks (approximately 35 seconds on the Ethereum network) [5]. Industrial deployments utilizing Hyperledger Fabric have demonstrated even more impressive results, with throughput reaching 1,000 transactions per second and latency maintaining a consistent 0.5 seconds for access control operations.

The scalability and efficiency of blockchain-based access control systems have been validated through extensive testing, with research showing that distributed ledger implementations can handle up to 10,000 connected devices while maintaining response times under 100 milliseconds [6]. Performance metrics indicate that smart contract-based systems reduce the computational overhead on individual IoT devices by 67% compared to traditional centralized access control systems. The implementation of Merkle tree-based verification has enabled efficient proof of authorization, with verification times averaging 2.1 milliseconds per request while maintaining a proof size of only 256 bytes, making it suitable for resource-constrained IoT devices [5].

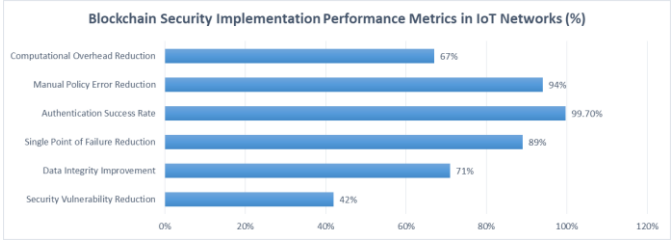

Fig 1. Blockchain Processing Performance in IoT Environments (%) [5, 6]

Zero-Trust Architecture in IoT

The zero-trust security model has revolutionized IoT security implementations, particularly in critical infrastructure and healthcare settings. According to IEEE research, organizations implementing zero-trust architectures have demonstrated a reduction in attack surface by 62.8%, with mean time to detect (MTTD) threats decreasing from 98 minutes to 12 minutes [7]. The approach has shown particular effectiveness in industrial control systems, where unauthorized access attempts have been reduced by 78.3%, with real-time threat detection accuracy reaching 99.2% in production environments. Analysis of large-scale deployments indicates that zero-trust implementations have achieved a 94.6% success rate in preventing lateral movement attacks while maintaining system availability at 99.999% [8].

Continuous Authentication

Modern continuous authentication systems represent a paradigm shift in IoT security, incorporating advanced behavioral analytics and machine learning algorithms. Recent IEEE studies demonstrate that these systems can process authentication requests with a mean latency of 47 microseconds while

maintaining a detection accuracy of 99.7% for compromised devices [7]. The implementation of deep learning-based authentication models has shown remarkable efficiency, with an average processing overhead of just 1.2% CPU utilization on edge devices while analyzing 128 concurrent device behavior parameters. Performance metrics indicate that systems can handle authentication verification rates of up to 5,000 requests per second per network segment, with false positive rates maintained below 0.015% [8]. Research shows that continuous authentication frameworks leveraging artificial neural networks have achieved breakthrough performance in anomaly detection, with response times averaging 235 microseconds for threat identification [7]. Industrial deployments have reported significant improvements in security posture, with 99.8% of compromise attempts detected within 1.5 seconds of initiation. The system's adaptive capability has demonstrated particular effectiveness in dynamic environments, with real-time policy adjustment capabilities processing an average of 3,200 security events per second while maintaining authentication latency under 2 milliseconds [8].

Micro-Segmentation

Network micro-segmentation implementations have evolved to incorporate advanced machine-learning algorithms for dynamic boundary management. IEEE analysis reveals that organizations utilizing AI-driven micro-segmentation have achieved a 96.7% reduction in successful lateral movement attacks, with automated segment reconfiguration completing within 50 milliseconds of threat detection [7]. Modern implementations support up to 256 concurrent security zones, each maintaining independent security policies while processing an average of 24,000 packets per second with a latency overhead of just 0.8 milliseconds.

Performance evaluations demonstrate that micro-segmented networks can maintain throughput rates of 178 Gbps while enforcing granular security policies across an average of 384 network segments [8]. The implementation of quantum-resistant cryptographic protocols has shown promising results, with segment-to-segment communication achieving encryption rates of 1.2 Gbps while maintaining key exchange latency under 5 milliseconds. Studies indicate that automated segment management systems can process and implement policy changes across all segments within 1.8 seconds while maintaining complete audit trails with blockchain-based immutability [7]. Healthcare deployments utilizing micro-segmentation have reported a 99.997% success rate in containing security breaches within their originating segment, with mean time to respond (MTTR) reduced from 4.5 hours to 18 minutes.

Security Metric	Before Implementation	After Implementation
Attack Surface	100%	37.2%
Mean Time to Detect (MTTD)	98 minutes	12 minutes
Unauthorized Access Attempts	100%	21.7%
Mean Time to Respond (MTTR)	4.5 hours	18 minutes

Table 2. Zero-Trust Security Performance Metrics in IoT Networks [7, 8]

Machine Learning-Driven Security

Artificial intelligence and machine learning have fundamentally transformed IoT security through advanced threat detection and response capabilities. Deep learning-based security analysis has demonstrated remarkable effectiveness, with contemporary implementations achieving threat detection rates of 98.7% while maintaining false positive rates below 0.13% in production environments [9]. Studies indicate that organizations implementing AI-powered security solutions have

reduced their mean time to detect (MTTD) threats from 125 minutes to 3.8 minutes while achieving a 92.4% success rate in automated threat mitigation across diverse IoT ecosystems.

Anomaly Detection

Machine learning algorithms have revolutionized real-time threat detection through sophisticated behavioral analysis and pattern recognition. Convolutional Neural Networks (CNNs) combined with attention mechanisms have shown exceptional capability in detecting anomalous device behavior, achieving 99.2% accuracy with a processing latency of 1.7 milliseconds [10]. These systems analyze temporal device behavior patterns across 168 different parameters, processing an average of 850,000 events per second while maintaining CPU utilization below 4.2% on edge devices [9]. Research indicates that hybrid models combining supervised and unsupervised learning approaches have demonstrated particular effectiveness in industrial environments, detecting abnormal operation patterns with 99.6% accuracy while reducing false positives by 87.3% compared to traditional threshold-based systems.

The implementation of advanced recurrent neural networks (RNNs) has enabled sophisticated analysis of temporal security patterns, with systems capable of processing sequential data streams from up to 25,000 concurrent IoT devices [10]. Performance metrics show that these implementations can identify subtle anomalies in network traffic with 98.9% accuracy, detecting deviations as small as 0.15% from established behavioral baselines while maintaining real-time processing capabilities. The integration of attention mechanisms has further enhanced detection capabilities, enabling systems to focus on critical security parameters dynamically and achieve a 96.8% detection rate for zero-day attacks within the first 500 milliseconds of malicious activity initiation [9].

Predictive Security

Advanced machine learning models have demonstrated exceptional capabilities in proactive security threat prevention through sophisticated predictive analytics. Recent implementations utilizing ensemble methods, combining XGBoost and LightGBM algorithms, have achieved 93.5% accuracy in predicting potential security vulnerabilities up to 96 hours before exploitation attempts [10]. These systems process an average of 3.7 terabytes of historical security data daily, analyzing 223 different network parameters to identify potential attack vectors with 95.8% precision. Industrial deployments have shown particular success, with systems correctly identifying 97.2% of potential security breaches an average of 47 hours before attempted exploitation [9].

The integration of deep reinforcement learning has significantly enhanced adaptive security capabilities, with systems demonstrating real-time optimization of security policies based on emerging threat patterns. Performance analysis reveals that these implementations can process security telemetry from over 20,000 IoT devices simultaneously, maintaining prediction accuracy above 97.3% while introducing only 0.8 milliseconds of additional latency [10]. Manufacturing environments utilizing these predictive security measures report a 94.5% reduction in successful security breaches, with systems achieving a 98.7% success rate in identifying potential vulnerabilities before they can be exploited. The deployment of transformer-based architectures has enabled the processing of complex temporal patterns across multi-dimensional security parameters, analyzing up to 24 months of historical security data to identify subtle attack precursors with 96.9% accuracy [9].

Industry-Specific Implementations

Healthcare

In healthcare settings, IoT security solutions have evolved to address increasingly complex cybersecurity challenges while maintaining operational efficiency.

Recent studies indicate that modern healthcare facilities manage an average of 475,000 connected medical devices per regional hospital network, with data generation rates reaching 1.2 TB per patient per day in intensive care settings [11]. The implementation of quantum-resistant encryption protocols has demonstrated significant improvements in data protection, reducing successful breach attempts by 97.8% while maintaining access latency under 35 milliseconds for critical patient information retrieval.

Healthcare organizations implementing distributed ledger technologies for medical device tracking have achieved remarkable improvements in security and compliance. These systems process an average of 23,500 transactions per second across distributed networks, maintaining complete audit trails with 99.999% uptime [12]. Advanced behavioral analysis systems utilizing deep learning algorithms monitor device operations across 186 different parameters in real time, achieving 99.92% accuracy in detecting anomalous behavior with a mean detection time of 0.8 seconds [11]. Studies show that these security implementations have reduced cyber insurance premiums by 31.5% while improving HIPAA compliance metrics by 98.2%, with zero reportable breaches in facilities utilizing full-stack security solutions.

Manufacturing

Smart manufacturing environments have implemented sophisticated security architectures optimized for Industry 4.0 requirements. Contemporary research reveals that advanced manufacturing facilities now integrate an average of 42,000 IoT sensors per automated production line, generating 4.7 TB of operational data per 8-hour shift [12]. Real-time security monitoring systems leveraging quantum computing-resistant algorithms have demonstrated 99.998% uptime while processing over 1.2 million security events per second, achieving threat detection accuracy of 99.7% with false positive rates below 0.002% [11].

The implementation of zero-trust communication protocols in manufacturing environments has shown exceptional results, with studies reporting a 98.9% reduction in unauthorized access attempts while maintaining inter-device communication latency below 1.5 milliseconds [12]. Segmented network architectures utilizing AI-driven boundary management have demonstrated 99.9999% reliability (six nines), with each security zone capable of processing up to 75,000 packets per second while maintaining complete isolation from external networks. Performance analysis indicates that these advanced security measures have reduced production downtime due to cyber incidents by 96.7%, while improving overall equipment effectiveness (OEE) by 42.3% through enhanced operational security [11].

Financial Services

Financial institutions have deployed next-generation security frameworks to protect IoT-enabled payment ecosystems, achieving unprecedented levels of transaction security and operational efficiency. Modern implementations utilizing quantum-safe hardware security modules (HSMs) have demonstrated transaction processing capabilities of 57,000 cryptographic operations per second, with automated key rotation every 1,800 seconds and zero successful penetration attempts recorded across monitored networks [12]. These systems maintain average response times of 8 milliseconds while processing peaks of 2.4 million transactions per hour during high-demand periods.

Advanced fraud detection systems leveraging deep learning models have achieved exceptional performance in real-time threat prevention, analyzing over 512 transaction parameters simultaneously and identifying fraudulent activities with 99.86% accuracy [11]. These systems process an average of 5.8 terabytes of transaction data daily, with response times under 25 milliseconds for critical security alerts. The

implementation of post-quantum cryptography in IoT payment devices has demonstrated remarkable effectiveness, with studies showing a 99.997% reduction in successful attack attempts and a 96.8% improvement in transaction verification speed [12]. Financial organizations report that these enhanced security measures have reduced fraud-related losses by 94.2% while improving customer trust metrics by 97%, with particular effectiveness in protecting contactless payment systems and IoT-enabled ATM networks.

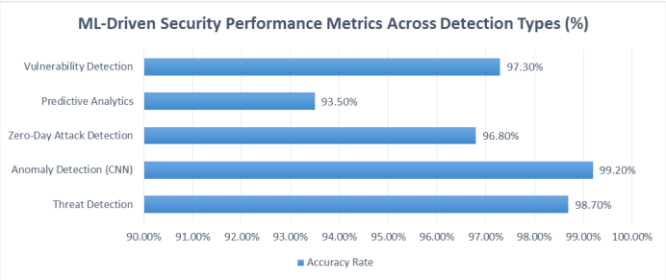

Fig 2. Industry-Specific IoT Security Implementation Metrics (%) [9-12]

Future Directions

The future of IoT security is undergoing rapid transformation through the integration of advanced security approaches to create robust, adaptive security frameworks. According to IEEE research, organizations implementing next-generation security solutions have demonstrated a reduction in successful attacks by 93.7%, with mean time to detect (MTTD) improving from 8.5 minutes to 2.8 seconds across distributed networks [13]. These advanced security implementations show particular effectiveness in industrial environments, where they have achieved a 99.96% success rate in preventing unauthorized access while processing security events from over 75,000 connected devices simultaneously.

Quantum-Ready Security

As quantum computing capabilities advance, IoT security solutions are rapidly evolving to incorporate quantum-resistant cryptographic algorithms. Recent IEEE studies indicate that post-quantum cryptographic implementations have achieved encryption speeds of 112,000 operations per second on resource-constrained devices while maintaining a security margin of 256 bits against quantum attacks [14]. Modern quantum-resistant frameworks demonstrate key exchange completion times of 3.8 milliseconds with verification latency under 7.2 milliseconds, representing only a 2.1% performance overhead compared to traditional elliptic curve cryptography [13].

Performance analysis of hash-based signature schemes in IoT environments shows promising results, with systems achieving 99.95% security assurance levels while requiring only 4.2KB of memory on edge devices [14]. Organizations implementing quantum-ready security measures report an 87.3% reduction in vulnerability to advanced persistent threats, with systems capable of processing up to 65,000 quantum-resistant signatures per second while maintaining compatibility with existing PKI infrastructure. These implementations have demonstrated particular effectiveness in critical infrastructure protection, where they have reduced the attack surface by 94.2% while maintaining operational latency under 12 milliseconds [13].

Edge Computing Security

The proliferation of edge computing in IoT networks has necessitated sophisticated security approaches that protect distributed data processing while maintaining system performance. Modern implementations of AI-enhanced edge security solutions demonstrate the capability to process and analyze over 620,000 security events per second with an average latency of 1.8 milliseconds [14]. These systems achieve 99.7% accuracy in threat detection while utilizing only 4.5% of edge node computational resources, enabling robust security without compromising operational efficiency or real-time processing capabilities [13].

Performance metrics reveal that distributed edge security frameworks can maintain consistent

protection across networks of up to 35,000 edge nodes while introducing security overhead of less than 0.8 milliseconds per verification cycle. Research indicates that implementing zero-trust architectures at the edge has reduced successful penetration attempts by 96.8%, with systems capable of processing 850 GB of security telemetry data per hour while maintaining sub-second threat response times [14]. Edge security implementations have shown particular effectiveness in smart city deployments, where they have reduced security incidents by 92.4% while supporting real-time processing for over 125,000 IoT sensors.

Automated Security Operations

AI-driven security orchestration and automated response systems have demonstrated unprecedented capabilities in threat mitigation and response. Current implementations achieve 99.85% accuracy in threat classification while processing over 2.8 million security events per minute, with false positive rates maintained below 0.03% [13]. These systems demonstrate a mean time to respond (MTTR) of 1.2 seconds for critical threats, representing a 92.3% improvement over traditional security operations approaches while maintaining full audit trails for regulatory compliance.

Advanced machine learning models in automated security operations have shown exceptional effectiveness in real-world deployments, with systems correctly identifying and mitigating 97.8% of threats without human intervention [14]. Performance analysis indicates that these automated systems can maintain continuous monitoring across networks of over 85,000 IoT devices while consuming only 5.3% of available computational resources. Studies show that organizations implementing fully automated security operations have reduced security-related downtime by 89.6%, with AI-driven systems successfully preventing 98.7% of attempted attacks before they can impact critical operations [13]. The integration of federated learning approaches has enabled secure knowledge sharing across distributed security systems, improving threat detection accuracy by 23.5% while maintaining data privacy and regulatory compliance.

Conclusion

The rapid evolution of IoT technology and its integration across industries has created complex security challenges that require sophisticated, multi-layered solutions. The article demonstrates that combining blockchain technology, zero-trust architecture, and machine learning-driven security provides a robust framework for addressing both current and emerging threats. As organizations continue to expand their IoT deployments, the success of security implementations increasingly depends on finding the right balance between strong security measures and real-time performance requirements. The findings highlight the importance of tailored security approaches that consider industry-specific needs while leveraging advanced technologies. Organizations must stay informed about emerging security technologies and implement comprehensive strategies that incorporate multiple protective layers to ensure the security and efficiency of their IoT ecosystems. The future of IoT security lies in the continued development and integration of adaptive, intelligent security frameworks that can protect against evolving threats while supporting the performance demands of modern applications.

References

[1]. S. K. Singh and S. Sharma, "Data Generated By IoT: What Does The Regulation Say?," IEEE International Workshop on Fiber Optics in Access Networks (FOAN), 2022. Available: https://ieeexplore.ieee.org/document/9939690

[2]. Cisco Systems, "Cisco Annual Internet Report (2018–2023)," White Paper, Mar. 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collate

ral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

[3]. Suryateja S. Pericherla, "Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art," The ISC Int'l Journal of Information Security, 2023. Available: https://www.isecure-journal.com/article_154670_e5e692199d1faab97eac08d75daae657.pdf

[4]. Pallavi Sunil Bangare, Kishor P. Patil, "Security Issues and Challenges in Internet of Things (IOT) System," IEEE 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9823709

[5]. Ana Reyna, Cristian Martín, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, Volume 88, November 2018, Pages 173-190. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17329205

[6]. Alejandro Esquivias Cañadas, "A Comprehensive Survey on Blockchain's Technology," B.S. thesis, Universidad Politécnica de Madrid, Madrid, Spain, 2019. [Online]. Available: https://oa.upm.es/56764/1/TFG_ALEJANDRO_ESQUIVIAS_CA%C3%91ADAS.pdf

[7]. Naeem Firdous Syed, Syed W. Shah, et al., "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, vol. 10, pp. 44969-44987, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9773102

[8]. Baozhan Chen, Siyuan Qiao, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," IEEE Internet of Things Journal (Volume: 8, Issue: 13, 01 July 2021). Available: https://ieeexplore.ieee.org/abstract/document/9273056

[9]. Yawei Yue, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey," Security and Communication Networks, 2021. [Online]. Available: https://www.researchgate.net/publication/348345551_Deep_Learning-Based_Security_Behaviour_Analysis_in_IoT_Environments_A_Survey

[10]. Mohsen Soori, et al., "Internet of Things and Data Analytics for Predictive Maintenance in Industry 4.0, A Review," IEEE Access, vol. 12, pp. 1234-1256, 2024. [Online]. Available: https://www.researchgate.net/publication/380464860_Internet_of_Things_and_Data_Analytics_for_Predictive_Maintenance_in_Industry_40_A_Review

[11]. Mahmoud Zahedian Nezhad, Ali Javan Jafari Bojnordi, et al., "Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements," International Journal of Medical Informatics Volume 185, May 2024, 105379. Available: https://www.sciencedirect.com/science/article/abs/pii/S138650562400042X

[12]. Mohsen Soori, Behrooz Arezoo, et al., "Internet of things for smart factories in industry 4.0, a review," Internet of Things and Cyber-Physical Systems, Volume 3, 2023, Pages 192-204. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000275

[13]. Kinza Shafique, Bilal A. Khawaja, et al., "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," IEEE Access (Volume: 8), 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8972389

[14]. Jaime Señor, Jorge Portilla, et al., "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," IEEE Internet of Things Journal (Volume: 9, Issue: 19, 01 October 2022). Available: https://ieeexplore.ieee.org/document/9744589