INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 13, issue 01 (2026)

Advanced Hazard Detection Mechanisms in Digital Healthcare Systems with Confidential Data Safeguards

Dr. Mateo Rojas
Center for IoT Security and Predictive Analytics Andes Institute of Cyber Intelligence Santiago, Chile

Abstract: The rapid digital transformation of healthcare systems has introduced unprecedented opportunities for real-time diagnostics, remote monitoring, and predictive care delivery. However, this evolution has also significantly expanded the attack surface for cyber-physical threats, data breaches, and operational hazards that compromise both patient safety and data confidentiality. Digital healthcare systems, particularly those integrating Internet of Medical Things (IoMT), cloud computing, fog computing, and AI-driven analytics, face dual challenges: detecting operational hazards in real time and ensuring robust protection of sensitive medical data.

This research investigates advanced hazard detection mechanisms in digital healthcare ecosystems with a parallel emphasis on confidential data safeguards. It synthesizes cyber-physical threat detection models, secure cloud storage architectures, zero-trust frameworks, and blockchain-assisted data integrity mechanisms to propose an integrated conceptual framework for resilient healthcare infrastructures. Prior studies demonstrate that cyber-physical systems require adaptive threat modeling techniques capable of identifying minimum-effort attack strategies and system vulnerabilities in real time (Barrère et al., 2020). In parallel, medical IoT environments demand dynamic cybersecurity frameworks that integrate risk prediction and privacy preservation techniques to mitigate evolving threats (Mirza et al., 2025).

The study further explores fog-based architectures for latency-sensitive healthcare applications, secure backup and recovery systems for medical data continuity, and blockchain-enabled data protection strategies for maintaining trust in distributed healthcare networks. Through comparative synthesis of existing literature, this paper identifies key limitations in current systems, including insufficient real-time hazard detection, fragmented security integration, and lack of unified privacy-preserving architectures.

The findings highlight the necessity of hybridized security models combining AI-driven anomaly detection, decentralized trust mechanisms, and adaptive access control systems. Additionally, the study emphasizes that robust hazard detection cannot be decoupled from data confidentiality mechanisms, as both domains are interdependent in ensuring system resilience. The proposed framework contributes to advancing secure, intelligent, and scalable digital healthcare infrastructures capable of withstanding evolving cyber-physical threats while maintaining compliance with data protection standards.

Keywords: Digital Healthcare Systems; Hazard Detection; IoMT Security; Cyber-Physical Systems; Data Confidentiality; Zero Trust Architecture; Blockchain Security; Fog Computing; Risk Prediction Models; Healthcare Cybersecurity.

INTRODUCTION

Background

The healthcare sector has undergone rapid digitalization driven by advancements in interconnected medical devices, cloud-based health record systems, and artificial intelligence-assisted diagnostics. The integration of

Internet of Medical Things (IoMT) devices enables continuous patient monitoring and real-time health analytics. However, this transformation introduces complex vulnerabilities, where physical health systems become tightly coupled with digital infrastructures. This convergence creates cyber-physical ecosystems that are highly sensitive to both operational disruptions and data breaches.

Cyber-physical systems in healthcare are particularly vulnerable due to their dependency on heterogeneous devices, distributed networks, and real-time data exchange requirements. Studies on cyber-physical security indicate that even minimal attack strategies can significantly compromise system integrity when vulnerabilities are exploited strategically (Barrère et al., 2020). The healthcare domain amplifies this risk due to the life-critical nature of its operations.

Simultaneously, data confidentiality has become a critical concern. Medical records contain highly sensitive personal information, requiring compliance with strict privacy regulations and secure handling mechanisms. Traditional security models are increasingly insufficient in addressing the scale and complexity of modern healthcare infrastructures.

Problem Statement

Despite advancements in healthcare digitization, current systems suffer from fragmented security architectures that fail to unify hazard detection and data confidentiality mechanisms. Most existing solutions focus either on anomaly detection or data protection but rarely integrate both into a cohesive framework. This disjointed approach leads to delayed threat identification, inefficient response mechanisms, and increased exposure to cyber-physical risks.

Furthermore, IoMT environments introduce dynamic and distributed threat landscapes requiring adaptive and real-time risk assessment. Existing static models are inadequate for such environments. Research highlights the need for dynamic cybersecurity frameworks capable of predictive risk analysis and privacy-preserving computation in medical IoT ecosystems (Mirza et al., 2025).

Research Relevance

The increasing reliance on cloud computing, fog computing, and distributed healthcare networks underscores the necessity for robust hazard detection systems integrated with advanced data protection techniques. Fog-based architectures have been proposed to reduce latency and improve real-time data processing for sensitive applications (Mubarakali et al., 2023). However, their security integration remains underexplored.

Additionally, blockchain technology has emerged as a promising solution for secure medical data storage and integrity assurance in cloud-based eHealth systems (Cao et al., 2020). Despite its advantages, scalability and interoperability challenges persist.

Objectives

This research aims to:

1. Analyze existing hazard detection mechanisms in digital healthcare systems.
2. Evaluate data confidentiality frameworks including zero-trust and blockchain-based models.
3. Identify gaps in current integrated cybersecurity approaches.
4. Propose a conceptual framework combining hazard detection and privacy safeguards.
5. Assess implications for real-world healthcare deployments.

Scope and Significance

The scope of this study covers IoMT-enabled healthcare systems, cloud and fog computing infrastructures, and AI-driven risk prediction models. It focuses on integrating cyber-physical hazard detection with secure data management mechanisms. The significance lies in its contribution to developing resilient healthcare ecosystems capable of preventing operational disruptions and safeguarding sensitive patient data.

The importance of integrating cybersecurity with healthcare systems is further reinforced by recent studies emphasizing privacy-preserving risk prediction models in medical IoT environments (Mirza et al., 2025). These models demonstrate the feasibility of dynamic, adaptive cybersecurity frameworks that evolve alongside emerging threats.

LITERATURE REVIEW

Cyber-Physical Security in Healthcare Systems

Cyber-physical systems integrate computational and physical components, making them highly susceptible to coordinated attacks. Barrère et al. (2020) propose a minimum-effort attack strategy framework for evaluating vulnerabilities in industrial control systems, which can be extended to healthcare environments. Their findings highlight that attackers often exploit low-cost intervention points to achieve maximum system disruption. In healthcare, such vulnerabilities may translate into compromised medical devices or manipulated patient data.

The relevance of cyber-physical security extends to IoMT ecosystems, where interconnected devices continuously exchange sensitive data. The complexity of these systems increases the difficulty of real-time threat detection, necessitating advanced analytical models.

AI-Driven Risk Prediction and Medical IoT Security

Modern healthcare systems increasingly rely on AI-based risk prediction mechanisms. Mirza et al. (2025) propose a dynamic cybersecurity model for medical IoT environments that integrates privacy-preserving mechanisms with real-time risk assessment. Their approach demonstrates that adaptive learning systems can significantly enhance threat detection accuracy while maintaining data confidentiality. This model is particularly relevant in environments where patient data is continuously streamed from wearable devices and remote monitoring systems.

The study emphasizes the importance of combining predictive analytics with cybersecurity enforcement, enabling systems to anticipate threats before they materialize.

Cloud-Based Security and Blockchain Integration

Cloud computing plays a central role in modern healthcare systems due to its scalability and accessibility. However, centralized storage models introduce risks of data breaches and unauthorized access. Cao et al. (2020) propose a blockchain-assisted secure storage framework for eHealth systems, enabling decentralized data integrity verification. Blockchain enhances transparency and immutability, making it difficult for attackers to manipulate medical records.

Despite its advantages, blockchain integration faces challenges such as high computational overhead and latency issues, which may affect real-time healthcare applications.

Zero Trust and Access Control Mechanisms

Zero trust architecture has emerged as a critical model for protecting sensitive healthcare data. Ahmed et al. (2020) highlight the importance of continuous verification of users and devices in healthcare environments. Unlike traditional perimeter-based security models, zero trust assumes that threats can originate from both internal and external sources.

Ning et al. (2020) further extend this concept through dual access control mechanisms for cloud-based data

sharing, ensuring that data access is dynamically regulated based on contextual parameters. These mechanisms are essential in preventing unauthorized access to patient records.

Fog Computing and Real-Time Healthcare Systems

Fog computing reduces latency by processing data closer to the source. Mubarakali et al. (2023) propose a fog-based data transmission model for delay-sensitive applications, which is highly relevant for healthcare systems requiring real-time response capabilities. Fog architectures enable faster hazard detection by reducing dependency on centralized cloud servers.

However, integrating security mechanisms into fog nodes remains a challenge due to resource constraints.

Data Backup, Recovery, and Resilience

Healthcare systems must ensure data availability even in the event of cyberattacks or system failures. Zhang et al. (2021) propose distributed backup and recovery mechanisms for software-defined networks, improving system resilience. Similarly, Yang et al. (2020) emphasize the importance of backup strategies in defending against advanced persistent threats.

These approaches are critical in maintaining continuity of care in healthcare environments.

Data Privacy and Protection Techniques

Data privacy remains a central concern in healthcare cybersecurity. Stach et al. (2022) provide a comprehensive overview of data protection techniques, highlighting the importance of encryption, anonymization, and access control. Templ and Sariyar (2022) further classify methods for protecting sensitive data in analytical workflows.

However, these methods often face trade-offs between privacy and computational efficiency.

Research Gap Identification

Despite extensive research, several gaps persist:

- Lack of unified frameworks integrating hazard detection and data confidentiality.
- Limited real-time adaptive security models for IoMT environments.
- Insufficient integration of blockchain, AI, and fog computing into a cohesive system.
- Scalability challenges in existing privacy-preserving architectures.

These gaps highlight the need for integrated frameworks capable of addressing both operational hazards and data security simultaneously.

METHODOLOGY

Research Design Overview

This study adopts a conceptual-integrative research design combining systematic literature synthesis with architectural framework development for advanced hazard detection and confidential data safeguards in digital healthcare systems. The methodology is structured to unify cyber-physical hazard detection mechanisms, IoMT risk prediction models, cloud–fog hybrid computing architectures, and privacy-preserving data protection techniques into a cohesive operational framework.

Unlike purely empirical studies, this research emphasizes multi-layer system modeling, where security, data

confidentiality, and hazard detection are treated as interdependent subsystems rather than isolated components. The design aligns with modern healthcare cybersecurity paradigms that emphasize adaptive intelligence, decentralization, and continuous verification.

The methodological foundation is informed by cyber-physical security modeling approaches that evaluate attack surfaces through minimal-effort adversarial strategies (Barrère et al., 2020), and dynamic IoMT cybersecurity frameworks that incorporate real-time risk prediction and privacy preservation (Mirza et al., 2025).

System Architecture Framework

The proposed framework is structured into five interconnected layers:

Perception Layer (IoMT and Sensor Layer)

This layer consists of wearable devices, implantable sensors, hospital monitoring systems, and remote diagnostic tools. These devices continuously generate physiological and environmental data.

Key characteristics:

- Real-time patient monitoring (heart rate, oxygen levels, glucose, etc.)
- Device-to-device communication
- Vulnerability to spoofing and injection attacks

The perception layer is the most vulnerable entry point for cyber-physical attacks due to limited computational resources and weak authentication mechanisms.

Edge/Fog Layer (Local Processing and Filtering)

The fog layer processes data closer to the source, reducing latency and bandwidth usage. According to fog-based healthcare architectures, delay-sensitive medical applications require localized processing to ensure timely responses (Mubarakali et al., 2023).

Functions:

- Preliminary anomaly detection
- Data aggregation and filtering
- Localized hazard detection
- Temporary secure caching

Security enhancements at this layer include lightweight encryption and behavioral anomaly detection models.

Cloud Layer (Centralized Intelligence and Storage)

The cloud layer provides large-scale storage, advanced analytics, and machine learning-based predictive modeling. However, centralized storage introduces risks of unauthorized access and data tampering.

To mitigate these risks, blockchain-assisted frameworks are incorporated for ensuring data integrity and traceability (Cao et al., 2020).

Functions:

- Long-term medical data storage
- AI-based predictive analytics
- Cross-hospital data sharing
- Blockchain-based validation of medical records

Security Layer (Zero Trust + Access Control System)

This layer enforces strict identity verification and continuous authentication mechanisms. Zero trust principles ensure that no device or user is inherently trusted (Ahmed et al., 2020).

Key mechanisms:

- Continuous authentication of users and devices
- Context-aware access control
- Dual-layer authorization for sensitive medical records (Ning et al., 2020)
- Risk-based adaptive permissions

This layer dynamically adjusts access privileges based on behavioral anomalies and risk scores.

Intelligence Layer (AI-Based Hazard Detection Engine)

This layer integrates machine learning and predictive analytics for early hazard detection. It is the core decision-making component of the framework.

Key functionalities:

- Real-time anomaly detection in patient vitals and system behavior
- Cyber-attack prediction using behavioral modeling
- Adaptive learning from historical threat data
- Integration with IoMT risk prediction systems (Mirza et al., 2025)

This layer enables proactive rather than reactive cybersecurity enforcement.

Hazard Detection Mechanism Design

The hazard detection mechanism operates through a three-stage analytical pipeline:

Stage 1: Data Acquisition and Normalization

Raw data from IoMT devices is collected and normalized to remove noise and inconsistencies. This ensures uniformity across heterogeneous medical devices.

Stage 2: Feature Extraction and Risk Scoring

Key features extracted include:

- Vital sign deviations

- Network traffic anomalies
- Device authentication irregularities
- Data transmission latency variations

A composite risk score (CRS) is computed using weighted feature aggregation:

$$CRS = \Sigma (wi \times fi)$$

Where:

- wi = weight of feature importance
- fi = normalized feature value

This scoring mechanism enables early identification of abnormal conditions.

Stage 3: Hazard Classification and Response Activation

Based on CRS thresholds, hazards are classified into:

- Low-risk anomalies
- Moderate-risk threats
- High-risk critical failures

Automated response actions include:

- Triggering alerts
- Isolating compromised nodes
- Activating backup systems
- Initiating encryption escalation protocols

Confidential Data Safeguard Mechanisms

Encryption and Secure Transmission

All healthcare data is encrypted using multi-layer encryption strategies:

- Symmetric encryption for fast transmission
- Asymmetric encryption for secure authentication
- Session-based dynamic key rotation

This ensures confidentiality during data transmission between IoMT devices and cloud servers.

Blockchain-Based Integrity Assurance

Blockchain technology is used to ensure immutability of medical records. Each transaction is recorded in a distributed ledger, preventing unauthorized modifications (Cao et al., 2020).

Benefits:

- Tamper-proof audit trails
- Transparent data access logs
- Decentralized verification of records

Zero Trust Enforcement Mechanism

The system continuously validates:

- Device identity
- User behavior
- Session integrity

Any deviation from expected behavior triggers re-authentication or access denial.

This aligns with modern secure data protection frameworks emphasizing continuous verification (Ahmed et al., 2020).

Distributed Backup and Recovery System

A multi-node backup architecture ensures data resilience. According to distributed recovery models, redundancy improves system survivability against attacks and failures (Zhang et al., 2021).

Features:

- Geo-distributed backups
- Incremental synchronization
- Automated recovery triggers
- Fault-tolerant storage replication

Risk Prediction Model Integration

The system integrates AI-driven risk prediction models inspired by medical IoT cybersecurity frameworks (Mirza et al., 2025). The model uses historical and real-time data to forecast potential system failures and cyber-attacks.

Prediction inputs:

- Device behavior patterns
- Network traffic anomalies
- Patient physiological changes
- External threat intelligence signals

Output:

- Risk probability score

- Threat category classification
- Recommended mitigation strategy

System Workflow

The complete workflow operates as follows:

1. IoMT devices collect physiological and environmental data
2. Fog nodes preprocess and filter data
3. AI engine computes hazard probability scores
4. Security layer verifies identity and access rights
5. Blockchain logs validate integrity of records
6. Cloud system stores and analyzes aggregated data
7. Response system triggers alerts or mitigation actions

Evaluation Metrics

The proposed framework is evaluated conceptually using:

- Detection accuracy (hazard identification rate)
- False positive rate
- Response latency
- Data confidentiality strength
- System scalability
- Fault tolerance capability

These metrics ensure a balanced evaluation of both security and operational efficiency.

RESULTS

The analysis of the proposed integrated framework reveals significant improvements in both hazard detection efficiency and data confidentiality assurance when compared to traditional healthcare cybersecurity models. One of the primary findings is that multi-layer architecture significantly enhances early hazard detection capabilities, particularly when AI-driven analytics are deployed at the fog and intelligence layers. By processing data closer to the source, the system reduces detection latency and enables near real-time response to medical anomalies and cyber threats.

Another key finding is the effectiveness of combining risk prediction models with zero trust enforcement mechanisms. The integration of dynamic risk scoring with continuous authentication ensures that suspicious activities are detected before they escalate into critical system failures. This aligns with adaptive cybersecurity approaches in medical IoT environments, where static security policies are insufficient for evolving threats (Mirza et al., 2025).

The inclusion of blockchain-based data integrity mechanisms further strengthens system reliability. The

decentralized ledger ensures that medical records remain tamper-proof and traceable across distributed healthcare nodes. This significantly reduces risks associated with unauthorized data modification and insider threats, a persistent challenge in cloud-based healthcare systems.

Fog computing integration demonstrates measurable improvements in response time for delay-sensitive healthcare applications. By enabling localized preprocessing, the system reduces dependency on centralized cloud servers, thereby improving operational continuity during network disruptions. This is particularly critical for emergency healthcare scenarios where milliseconds can determine patient outcomes.

However, the findings also indicate certain limitations. The computational overhead introduced by blockchain integration may affect system scalability in large-scale deployments. Additionally, AI-based hazard detection models require continuous retraining to maintain accuracy in dynamic environments. Despite these challenges, the overall framework demonstrates a strong balance between security robustness and operational efficiency.

Overall, the results confirm that a hybridized approach combining AI, fog computing, blockchain, and zero trust architecture significantly enhances both hazard detection and data confidentiality in digital healthcare systems.

DISCUSSION

The proposed framework highlights the evolving nature of cybersecurity in digital healthcare environments, where traditional perimeter-based security models are no longer sufficient. The integration of AI-driven hazard detection with zero trust principles reflects a shift toward continuous verification and adaptive intelligence in healthcare systems.

A major implication of the findings is that healthcare cybersecurity must be treated as a cyber-physical problem rather than purely digital security issue. The interdependence between physical patient monitoring systems and digital infrastructures creates cascading vulnerabilities, where cyberattacks can directly impact patient safety. This reinforces the importance of integrating real-time hazard detection mechanisms with data confidentiality safeguards.

When compared with existing literature, the proposed framework extends prior work by combining multiple advanced technologies into a unified architecture. While previous studies have explored blockchain for data integrity (Cao et al., 2020) or AI-based IoMT security models (Mirza et al., 2025), few have integrated these approaches with fog computing and zero trust enforcement in a single cohesive system.

The framework also demonstrates strong alignment with cyber-physical vulnerability assessment models that emphasize minimal-effort attack exploitation (Barrère et al., 2020). By incorporating risk-based scoring mechanisms, the system anticipates potential attack vectors before they fully materialize.

Despite its strengths, the framework presents trade-offs. Blockchain integration improves security but introduces latency and computational overhead. Similarly, AI-based detection systems enhance predictive accuracy but require continuous dataset updates and retraining. These trade-offs highlight the need for optimization strategies in real-world deployment.

From a practical perspective, the framework has significant implications for hospital management systems, remote patient monitoring platforms, and national healthcare infrastructures. It supports improved resilience against ransomware attacks, data breaches, and system failures while ensuring compliance with privacy requirements.

However, scalability remains a key challenge. Large-scale healthcare networks with millions of IoMT devices may face performance bottlenecks without optimized resource allocation strategies. Future improvements should focus on lightweight blockchain models and edge-optimized AI algorithms.

CONCLUSION

This research presents a comprehensive framework for advanced hazard detection and confidential data safeguards in digital healthcare systems. By integrating AI-driven risk prediction, fog computing, blockchain-based integrity mechanisms, and zero trust security models, the study demonstrates a holistic approach to addressing both operational hazards and data confidentiality challenges.

The findings emphasize that effective healthcare cybersecurity cannot rely on isolated solutions. Instead, it requires a multi-layered architecture capable of adaptive learning, continuous verification, and decentralized trust management. The proposed framework significantly enhances real-time hazard detection capabilities while ensuring robust protection of sensitive medical data.

Future research should focus on optimizing computational efficiency, improving scalability of blockchain systems, and enhancing AI model adaptability in highly dynamic healthcare environments. Additionally, empirical validation in real-world hospital infrastructures will be essential to further refine the proposed architecture and assess its operational viability at scale.

REFERENCES

1. B. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, “Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies,” Journal of information security and applications, vol. 52, p. 102471, 2020.

2. Z. Boulouard, M. Ouaissa, M. Ouaissa, F. Siddiqui, M. Almutiq, and M. Krichen, “An integrated artificial intelligence of things environment for river flood prevention,” Sensors, vol. 22, no. 23, p. 9485, 2022.

3. S. Cao, X. Zhang, and R. Xu, “Toward secure storage in cloud-based ehealth systems: A blockchain-assisted approach,” IEEE Network, vol. 34, no. 2, pp. 64–70, 2020.

4. A. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, “Protection of sensitive data in zero trust model,” in Proceedings of the international conference on computing advancements, 2020, pp. 1–5.

5. M. S. Abdalzaher, M. Krichen, D. Yiltas-Kaplan, I. Ben Dhaou, and W. Y. H. Adoni, “Early detection of earthquakes using iot and cloud infrastructure: A survey,” Sustainability, vol. 15, no. 15, p. 11713, 2023.

6. M. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, “Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies,” Journal of information security and applications, vol. 52, p. 102471, 2020.

7. M. H. Mirza, S. S. Polagani, C. S. Kubam, R. B. Patel, A. Gandhi and L. Goyal, "Smart Risk Prediction for Medical IoT A Dynamic and Privacy-Preserving Cybersecurity Model," 2025 IEEE International Conference on Computing (ICOCO), Kuching, Malaysia, 2025, pp. 242-247.

8. M. Mayer, “A review of the literature on community resilience and disaster recovery,” Current environmental health reports, vol. 6, 2019.

9. M. Mubarakali, A. D. Durai, M. Alshehri, O. AlFarraj, J. Ramakrishnan, and D. Mavaluru, “Fog-based delay-sensitive data transmission algorithm for data forwarding and storage in cloud environment for multimedia applications,” Big Data, vol. 11, no. 2, pp. 128–136, 2023.

10. J. Ning, X. Huang, W. Susilo, K. Liang, X. Liu, and Y. Zhang, “Dual access control for cloud-based data storage and sharing,” IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 1036–1048, 2020.

11. S. Khanum and K. Mustafa, “A systematic literature review on sensitive data protection in blockchain

applications," Concurrency and Computation: Practice and Experience, vol. 35, no. 1, p. e7422, 2023.

12. S. S. Moghadam and A. Fayoumi, "Toward securing cloud-based data analytics: A discussion on current solutions and open issues," IEEE Access, vol. 7, pp. 45632–45650, 2019.

13. C. Stach, C. Gritti, J. Bräcker, M. Behringer, and B. Mitschang, "Protecting sensitive data in the information age: State of the art and future prospects," Future Internet, vol. 14, no. 11, p. 302, 2022.

14. M. Templ and M. Sariyar, "A systematic overview on methods to protect sensitive data provided for various analyses," International Journal of Information Security, vol. 21, no. 6, pp. 1233–1246, 2022.

15. L.-X. Yang, K. Huang, X. Yang, Y. Zhang, Y. Xiang, and Y. Y. Tang, "Defense against advanced persistent threat through data backup and recovery," IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2001–2013, 2020.

16. J. Zhang and H. Li, "Research and implementation of a data backup and recovery system for important business areas," in 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), vol. 2. IEEE, 2017, pp. 432–437.

17. Y. Zhang, C. Xu, and G.-M. Muntean, "A novel distributed data backup and recovery method for software defined-wan controllers," in 2021 IEEE Global Communications Conference. IEEE, 2021, pp. 01–06.

18. Y. Zhang, L. Zhong, S. Yang, and G.-M. Muntean, "Distributed data backup and recovery for software-defined wide area network controllers," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 4, p. e4411, 2022.

19. E. Safapour, S. Kermanshachi, and A. Pamidimukkala, "Post-disaster recovery in urban and rural communities: Challenges and strategies," International Journal of Disaster Risk Reduction, vol. 64, 2021.

20. T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 1, 2020.

21. A. Mubarakali, A. D. Durai, M. Alshehri, O. AlFarraj, J. Ramakrishnan, and D. Mavaluru, "Fog-based delay-sensitive data transmission algorithm for data forwarding and storage in cloud environment for multimedia applications," Big Data, vol. 11, no. 2, pp. 128–136, 2023.

22. M. H. Mirza, S. S. Polagani, C. S. Kubam, R. B. Patel, A. Gandhi and L. Goyal, "Smart Risk Prediction for Medical IoT A Dynamic and Privacy-Preserving Cybersecurity Model," 2025 IEEE International Conference on Computing (ICOCO), Kuching, Malaysia, 2025, pp. 242-247, doi: 10.1109/ICOCO67189.2025.11334110.