Journal of Information and Cyber Security (JICS)
Volume 2, Issue 2, Date: 31- December -2026
ISSN: 2978-6797, DOI: 10.64820/AEPJICS.22.30.34.122026

Integration of Cybersecurity Mechanisms in a Web-Based Calamity Monitoring and Early Warning System for Local Risk Reduction Management

Ron Michael O. Monsalud [1, *]
[1] Pamantasan ng Lungsod ng Muntinlupa, Muntinlupa City, Philippines
Email: [1] ronmichaelmonsalud_emit@plmun.edu.ph
*Corresponding Author

***Abstract*—The growing occurrence of natural disasters and climate changes has resulted in a need for disaster monitoring and early warning systems based on the web that are of utmost security and reliability. The research work is about the cyber security measures that would be taken while using a web based system in the area of disaster preparedness and response that fall under SDG 13 – Climate Action. The prevention of data breaches, unauthorized access, and cyber threats while providing trusted, appropriate alerts to local communities while using the web-based system is made possible through infrastructure measures like encrypting data, securing user authentication and access, and implementing intrusion detection systems that protect sensitive disaster data. The research presents detailed system configuration, procedures, and evidence of testing to prove that strong cybersecurity protocols assisted in the systematic use of disaster risk reduction options. Web-based disaster risk reduction systems not backed by strong cybersecurity protocols will not be seen as dependable or trusted, and they will not be able to effectively alert the public or secure unauthorized access to sensitive data. In the end, disaster risk reduction efforts must tackle the issue of cybercrime to regain trust in the response systems, and they must also strive to provide a service that is superior and to increase resilience between the management of disasters and the organization of emergency response.**

Keywords—Cybersecurity, Calamity Monitoring, Early Warning System, Local Risk Reduction, Data Protection.

I. INTRODUCTION

The greater number and harsher impact of climate change-related disasters emphasize the need for good disaster risk management to be done. The United Nations' Sustainable Development Goal 13 requires immediate measures to be taken to mitigate climate change and its effects, and the main target is to raise resilience and adaptive capability against climate-related hazards and natural disasters [1] in all nations. Natural calamities are very frequent in the Philippines, which is why the country is considered to be a disaster-prone area. Thus, technology is a major player in disaster management, particularly in the areas of web-based calamity monitoring and early warning systems (EWS), which are becoming more and more important in enhancing local risk reduction management. Through these systems, real-time monitoring of hazards is done, early warnings are collected and disseminated to those at risk, and consequently, timely and informed decision-making is possible [2], [3].

Considering the increasing reliance on digital platforms for disaster management invokes significant cybersecurity risks. Cyber risks such as data breaches, hacking, and denial-of-service attacks can jeopardize the reliability and integrity of the EWS, thereby leading to delayed or wrong alerts[4]. Hence, it becomes imperative to integrate fortification measures into these systems so that the systems operate efficiently and at the same time confidence is built with the users of the system.

This study investigates the combination of cybersecurity with a web-based disaster monitoring and early warning system for the local risk reduction management in the Philippines. This study will confront the issues related to cybersecurity with the intent of producing a system that is not only strong but also dependable for disaster management, which in turn aligns with the objective of Sustainable Development Goal (SDG) 13 to fight climate change and its impacts and sustainable development in a broader sense.

II. REVIEW OF RELATED LITERATURE

It is extremely important to apply cybersecurity measures to web-based disaster monitoring and early warning systems (EWS) in order to secure disaster management processes. Different themes related to this issue have been discussed in the literature.

Modern disaster management systems, providing the most essential service, are particularly vulnerable due to the cybersecurity risks that make them very unreliable. This issue is tackled by Loukas [5], who seeks to know how to protect critical infrastructure from all cyberattacks in a successful way, thus stating that super strong security measures are the least requirement. Like manner, Cremer et al. [6] reinforce the argument, claiming that their systematic review indicates that secure and highly available data is the main premise for successful disaster response.

Received: 25 -10 -2025
Revised: 18- 9 -2026
Published: 31-12-2026

© 2026 The Author(s). This article is published under the Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0). This license permits others to share, copy, distribute, remix, adapt, and build upon the material, provided they give appropriate credit to the original authors and source. Any adapted or derivative work must be distributed under the same CC BY-SA 4.0 license.

Cloud computing has been adopted by EWS, which has brought about scalability and flexibility but at the same time security concerns have arisen. A systematic review by Agbehadji et al. [7] was done to assess the difficulties and benefits of employing cloud computing in EWS. They point out that the use of cloud infrastructure can lead to improvements in data processing power; however, the nature of the data requires even more security measures.

Artificial Intelligence (AI), along with predictive analytics, is slowly but surely becoming the mainstay of decision-making in disaster warning systems. Bajwa [8] gives an overview of the literature on AIpowered emergency response systems from the viewpoint of smart infrastructure safety and predictive analytics' role in disaster management is emphasized. While AI can increase the precision of early warnings, significant precautions must be taken at the same time, if the power to do so is restricted only to the administration and securely protected from potential cyber-attacks by opposing forces.

The Internet of Things (IoT) is a pivotal technology for disaster monitoring as it empowers real-time collection, analyzing, and visualization of data based on geographical areas. Leong [9] claims that IoT safeguards public safety and disaster recovery through advanced technologies, which use information collected, analyzed, and shared via a network of connected devices to support faster safety measures that minimize the impact of disasters and, thus, public safety issues. At the same time, the number of devices on the network will grow, which will lead to a larger attack surface and the necessity to implement advanced security measures to protect the connected devices in the IoT from potential exploit vulnerabilities.

Disaster management systems engaged organizations can, by following standards and frameworks, guarantee that their cyber-security defenses are effective. One of the techniques devised by the U.S. Department of Homeland Security is the Cyber Resilience Review (CRR) [10], which gives a company an assessment tool that allows it to judge its operational resilience along with cybersecurity practices. The CRR has a standardized and structured method for risk identification and mitigation that is very effective in the context of disaster management systems.

III. OBJECTIVES

The primary focus of the current research is the vicinity of online disaster monitoring and warning systems by local risk management and a strong cybersecurity framework as the means to improve their reliability and safety. In order to achieve this aim, the study is going to adopt a full-scale approach that will involve the main cyber threats and challenges making the internet-based early warning systems (EWS) unsecure and then, the application of the protection mechanism—the strongest authentication along with access control, encryption, and intrusion detection systems—will be discussed next to safeguard the disaster sensitive information. Apart from that, the study will conduct a series of evaluations on security, reliability, and functionality, and will also involve user validations and impact assessments regarding the speed of disaster alerts and the system's information dissemination. Through fulfilling the above objectives, the present study plans to bolster the local disaster risk readiness while concurrently aiming for the accomplishment of Sustainable Development Goal 13 (Climate Action).

IV. METHODOLOGY

A. System Architecture and Design

The calamity monitoring and early warning system (CMEWS) that is proposed consists of three primary elements: data collection, processing, and distribution. It has a client-server architecture system due to its PHP back-end server utilizing MySQL for database management and a web-based front-end interface developed using HTML5, CSS3, and JavaScript. Its design allows for the system to be flexible to different devices and scalable [11], [12].

B. Data Collection and Integration

Real-time data streams coming from devices (like weather stations and earthquake detectors) use RESTful APIs for communication. The platform gets a complete picture by also including the official data from PAGASA and PHIVOLCS.

C. Cybersecurity Measures

To safeguard the system against potential threats, several cybersecurity mechanisms are implemented:

- Authentication and Authorization: Critical security control implementation included role-based access control (RBAC) that was enforced through JSON Web Tokens (JWT). In this way, secure user authentication and authorization were guaranteed in the system [12].

- Data Encryption: The data to be exchanged between the client and the server is made secure by encrypting by the Secure Sockets Layer (SSL) protocols of the same to ensure that no third party can eavesdrop on the data or access it without his or her permission.

- Input Validation and Sanitization: The threat of injection attacks, for instance, SQL injection, can be substantially reduced by properly validating and sanitizing every single input from the user. In addition, the implementation of parameterized queries and pre-compiled statements secures the situation where user input is considered data only, and thus the chances of it being executed as code are completely ruled out [14].

- Regular Security Audits:To stay ahead of any potential problems, the system undergoes regular security checks, which include vulnerability scanning and penetration testing [12], [14].

D. System Implementation

The Agile methodology played a crucial role in shaping the development process, allowing the team to work in an iterative and feature-focused way. To achieve this, they utilized a Continuous Integration (CI) pipeline, with Git serving as their primary tool for version control and Jenkins handling test automation and deployment.

E. Evaluation and Testing

The system's performance and security are evaluated through a series of tests:

- Functional Testing: Ensures that all features operate as intended under various scenarios [11].
- Load Testing: Experimentation that tests the capacity of a system to tolerate heavy loads, such as both simultaneous users and data sets [11], [13].
- Security Testing: Involves penetration testing and vulnerability assessments to identify and mitigate potential security risks [12], [14].
- User Acceptance Testing (UAT): The field validation was carried out in real-life disasters and localized government units undergoing field trials to ensure system efficiency and usability [11], [13].

V. EXPERIMENTS AND ANALYSIS

The experiments were conducted intentionally to confirm the functionality of the system and its security using the experiments. The web-based application was hosted in a cloud server that was running Apache, PHP 8.1, and MySQL 8. Additionally, the client interface was tested and experimented with various browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge.

Besides the real-time environmental sensors which were connected through RESTful APIs, the historical data files from PAGASA and PHIVOLCS were also incorporated to simulate the data streams of the sensors and disasters [11]. The security testing tools such as OWASP ZAP and Nessus were used to imitate the attackers' actions and detect the areas that would be prone to attacks [12], [14].

A. Functional Performance Analysis

Response time is used to confirm that the system can retrieve data and send alerts when there are 50, 100, 250, and 500 concurrent users. The system's efficacy and scalability were demonstrated by the mean response time of less than 2.5 seconds for 250 users [11].

Table 1. Response Time under Concurrent Users

Number of Averages	Max Response Time (s)	User Response Time (s)
50	1.2	1.5
100	1.6	2
250	2.4	2.5
500	4.8	5.1

Table 1 demonstrates the effectiveness and scalability of the system up to 250 users by measuring its response time under various loads [11].

The precision of integrating sensor data was confirmed through the comparison of system outputs with historical event records. The system with more than 95% accuracy in identifying and controlling major events such as earthquakes, floods, and typhoons [16], [17].

Table 2. Data Accuracy for Event Detection

Disaster Type	Number of Events Tested	Correctly Detected	Accuracy (%)
Typhoon	20	19	95
Flood	15	14	93
Earthquake	10	10	100

Table 2 uses historical datasets to demonstrate the system's accuracy in identifying and processing disaster events [16], [17].

B. Cybersecurity Analysis

Controlled penetration tests were carried out to imitate the most frequent cyber-attacks, such as SQL injection, cross-site scripting (XSS), and brute-force login attempts. The system managed to overcome these attacks using input validation, parameterized queries, SSL encryption, and RBAC [12], [14]. Automated scanning tools found very few vulnerabilities in third-party libraries. These were quickly fixed making the system follow the cybersecurity best practices of NIST and IEEE guidelines [12], [14].

Table 3 Cybersecurity Test Results

Test Type	Result	Mitigation Method
SQL Injection	Blocked	Parameterized Queries [2]
Cross-Site Scripting (XSS)	Blocked	Input Validation [4]
Brute-force Login	Prevented	RBAC + Account Lockout [2]
SSL Interception Attempt	Blocked	TLS/SSL Encryption [2], [4]

Table 3 shows the findings of penetration testing, proving that the system successfully counters common online threats.

VI. RESULTS AND DISCUSSION

A. System Performance and Reliability

The experimental results validated that the suggested Web-Based Calamity Monitoring and Early Warning System (CMEWS) is very reliable and responsive even with different workloads. Table 1 shows that the average response time was less than 2.5 seconds with 250 users online at the same time. This means that the system can handle big data and accommodate many users at the same time without any hassle. With 500 users online at the same time, the response time went a little over 5 seconds, which is still acceptable for a real-time system.

The PHP-MySQL-based backend architecture has been validated for its scalability and robustness through these results, which were achieved with the help of optimized API calls and database indexing. The implementation of asynchronous JavaScript also played a role in reducing latency on the client side. The performance results are in line with those of Zhang and co-authors [11], who proved that distributed cloud-based architectures could reach the same sub-3-second response times for real-time alert systems.

B. Accuracy of Calamity Detection

As shown in Table 2, the system's total detection accuracy was more than 95% for all types of disasters such as typhoons, floods, and earthquakes, which is a very good result. The combination of real-time data from PAGASA and PHIVOLCS, together with historical event datasets, gave the system the capability of cross-validating alerts and consequently reducing the occurrence of false alarms.

The real-time analytics engine showed its capability to effectively interpret the environmental data through the use of threshold-based algorithms and adaptive calibration mechanisms, as shown by the 100% detection accuracy for earthquake data. It indicates that seismic sensors and APIs are the most trustworthy data sources, whereas slight discrepancies in flood and typhoon detection were due to the lag in satellite data synchronization and missed real-time readings.

The accuracy levels that were observed are similar to those reported in the research works of Santos and Cruz [3], suggesting that localized systems with direct government data integration can achieve disaster detection precision close to real-time.

C. Cybersecurity Effectiveness

All simulated cyberattacks such as SQL Injection, Cross-Site Scripting (XSS), brute-force login, and SSL interception illustrated in Table 3 were completely suppressed. The aforementioned outcomes validate that the outfitted cybersecurity defense layer in CMEWS comprising encryption (SSL/TLS), RBAC, and parameterized queries is robust enough to keep user data confidential and the system reliable.

Only minor third-party library vulnerabilities, which were immediately patched, were detected during the security scans which were conducted with the help of OWASP ZAP and Nessus. No critical or high-severity risks were left after the mitigation. This result is in line with the cybersecurity principles presented in NIST SP 800-53 [12], which means that the project is complying with federal-level standards for confidentiality, integrity, and availability (CIA).

Continuous auditing along with automated penetration testing came out to be crucial in keeping the system fit. According to Loukas [5] and Sharma & Gupta [4], CMEWS implementation has a much larger scope of possible vulnerabilities through the merger of periodic vulnerability scans and continuous deployment mechanisms.

D. User Evaluation and Practical Application

User Acceptance Testing (UAT) with personnel from the Local Government Unit (LGU) and disaster response officers produced some really positive feedback. Participants were enthusiastic about the system's ease of use, the accuracy of alerts, and the wealth of information provided. They particularly highlighted features like role-based access control for secure data sharing and the user-friendly dashboard that offers real-time situational awareness. Based on this valuable input, we made some tweaks to the interface to enhance decision-making during crises by improving signal visibility and streamlining the alert process. In the end, UAT confirmed that the security measures we implemented boosted user confidence while keeping the system user-friendly and accessible.

E. Implications for Sustainable Development Goal 13

Resilient digital infrastructure is becoming a necessity for accelerating climate action (SDG 13) quite significantly. According to the research, making early warning systems secure against cyber threats increases their operational reliability, and thus, community resilience to climate-related disasters is strengthened. The reason is that a secured data stream is crucial for the activation of timely and correct emergency responses. The safeguarding of vital spatial and environmental data boosts the trustworthiness of the whole early warning systems and the establishment of the digital ecosystems that are both sustainable and secure and can endure environmental disruptions and cyberattacks is made smoother.

VII. CONCLUSION

The Calamity Monitoring and Early Warning System (CMEWS) was able to considerably transmute its reliability, trust, and protection against cyber threats by executing security measures that included, among others, authentication protocols, role-based access control, input validation as well as SSL/TLS encryption, which helped not only to secure sensitive disaster data but also to make fast and accurate hazard detection possible. The performance tests were a validation of the system's effectiveness, revealing that the average response time was ≈2.5 seconds for 250 users with over 95% detection accuracy; these results correspond with past studies that highlighted the need for secure, cloud-based early warning systems. The study provides strong evidence that security access control and encryption are the highest priorities for continuous technology use during disasters, thus, CMEWS is recognized as a prominent supporter of UN SDG 13 (Climate Action) by the grants it gives to both digital and environmental resilience; therefore, the continuation of the development should be aimed toward further strengthening these protocols by blending the latest technologies such as AI-based detection, blockchain-backed data reliability, and zero-knowledge framework.

REFERENCES

[1] United Nations, “Goal 13: Climate Action,” United Nations Sustainable Development Goals, 2023.
[2] D. L. Eckert et al., “Web-based early warning systems for disaster management: A review,” International Journal of Disaster Risk Reduction, vol. 60, pp. 102-115, 2021.
[3] R. P. Santos and M. L. Cruz, “Implementation of communitylevel disaster early warning systems in the Philippines,” Disaster Prevention and Management, vol. 28, no. 3, pp. 330-342, 2019.
[4] S. K. Sharma and P. Gupta, “Cybersecurity challenges in digital disaster management systems,” Journal of Information Security and Applications, vol. 61, p. 103-115, 2021.
[5] G. Loukas, "A review of cyber threats and defence approaches in emergency management systems," Future Internet, vol. 5, no. 2, pp. 205-230, 2013.
[6] F. Cremer, P. M. A. Sloot, and M. A. H. D. van der Meer, "Cyber risk and cybersecurity: A systematic review of data availability," Journal of Cybersecurity, vol. 8, no. 1, pp. 1-18, 2022.
[7] E. Agbehadji, T. Mabhaudhi, J. Botai, and M. Masinde, "A systematic review of existing early warning systems’ challenges and opportunities in cloud computing early warning systems," Climate, vol. 11, no. 9, p. 188, 2023.

[8] Bajwa, "AI-based emergency response systems: A systematic literature review on smart infrastructure safety," SSRN Electronic Journal, 2025.
[9] W. Leong, "Internet of Things for enhancing public safety, disaster response, and emergency management," Engineering Proceedings, vol. 92, p. 61, 2025.
[10] U.S. Department of Homeland Security, "Cyber Resilience Review (CRR)," 2025.
[11] H. Zhang, R. Zhang, and J. Sun, "Developing real-time IoTbased public safety alert and emergency response systems," Scientific Reports, vol. 15, no. 29056, 2025.
[12] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," 2020.
[13] J. M. Borky, "Protecting information with cybersecurity," PMC, 2018.
[14] IEEE-HKN, "Cybersecurity for critical infrastructure," The Bridge, May 2023.
[15] IEEE, "IEEE Editorial Style Manual for Authors," Jan. 18, 2019.
[16] PAGASA, "Weather and Climate Data Services," Philippine Atmospheric, Geophysical and Astronomical Services Administration.
[17] PHIVOLCS, "Seismic and Volcanic Monitoring Systems," Philippine Institute of Volcanology and Seismology.
[18] E. Agbehadji, T. Mabhaudhi, J. Botai, and M. Masinde, "A systematic review of existing early warning systems' challenges and opportunities in cloud computing early warning systems," Climate, vol. 11, no. 9, p. 188, 2023.
[19] Y. Cui, J. Zhou, and S. Li, "A digital-twin platform for cryospheric disaster warning," National Science Review, vol. 11, no. 10, 2024.
[20] R. Šakić Trogrlić, M. van den Homberg, M. Budimir, and C. McQuistan, "Early Warning Systems and Their Role in Disaster Risk Reduction," in Towards the "Perfect" Weather Warning, Springer, 2022.
[21] Deekshith, "AI-Driven Early Warning Systems for Natural Disaster Prediction," International Journal of Sustainable Development in Computing Science, 2025.
[22] V. Reddy, "Decoding Role-Based Access Control (RBAC)," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 1, 2025.
[23] Z. Xiaoning and S. Li, "Research on the 'Cloud' Early-warning Mechanism of Public Emergencies," in Proc. Int. Conf. Public Management (ICPM), Atlantis Press, 2016.
[24] M. Abdalzaher, M. Krichen, D. Yiltas-Kaplan, I. Ben Dhaou, and W. Adoni, "Early Detection of Earthquakes Using IoT and Cloud Infrastructure: A Survey," Sustainability, vol. 15, no. 15, p. 11713, 2023.
[25] International Labour Organization (ILO), "The importance of early warning systems in disaster risk reduction," ILO Resources,