Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 02, Issue 09, pp 1-9, September 2025

Development of an Enhanced Cybersecurity System using Blockchain Technology for Quick Incident Response Processes

Obansola O. Y[1], Olaniran R. A[2], Oyelowo O. R[3], Alawode M. O[4].

[1,2,3,4]Department of Computer Science, Federal School of Surveying Oyo, Oyo State Nigeria
[*]obansolatoyin@gmail.com

ABSTRACT

The cyberspace is a virtual environment of computers on various network based on diverse technologies. Due to increase in the volume of data and users in the cyberspace, the cyberspace is facing a lot of challenges in terms of security making it more vulnerable to various cyber threats. Traditional incident management systems often face challenges related to data integrity, response time, and coordination among various stakeholders. Hence, there is need for a more robust technology to leverage on in order to securely record incident data, ensuring that records are tamper-proof and auditable. Blockchain technology, with its decentralized and immutable nature, offers a promising solution that enhances the security of the cyberspace. The web application system was developed using Python and Django while Figma was employed as the primary design tool due to its robust capabilities in creating detailed blueprints. User interfaces smart contracts are integrated to automate response protocols, reducing human intervention and response time. The system was tested through unit testing, integration testing, and user acceptance testing (UAT). The results demonstrated that the blockchain-based system effectively met its objectives, offering secure and immutable incident records, while automation significantly enhanced response efficiency.

Keywords: Blockchain, Cyberspace, Cybersecurity, Quick Incidence Response, Response protocol.

1. Introduction

Cybersecurity encompasses the strategies, processes and technologies designed to protect networks, devices, programs and data from attack, damage, or unauthorized access (Gourav & Ashok, 2024). In the contemporary digital era, the proliferation of sophisticated cyber threats necessitates robust cybersecurity measures to safeguard sensitive information and maintain the integrity of digital infrastructure. Cybersecurity incidents, which can include data breaches, malware attacks, and denial-of-service attacks, pose significant risks to organizations and individuals alike (Saravanan & Satahya, 2019). Effective incident response mechanisms are essential to mitigate these risks and ensure timely recovery from cyber incidents (Clare *et al*., 2023).The field of cybersecurity is constantly evolving to address emerging threats and vulnerabilities. Key components of cybersecurity include risk management, threat detection, incident response, and recovery strategies (Gustava, 2021). Risk management involves identifying, assessing, and prioritizing potential security risks, followed by the implementation of appropriate measures to mitigate them. Threat detection relies on advanced technologies such as intrusion detection systems (IDS) and security information and event management (SIEM) systems to identify and analyze potential security incidents (Adabi et al., 2023). Incident response entails a coordinated approach to managing and addressing security breaches, including containment, eradication, and recovery efforts.

An incident reporting system is a critical component of cybersecurity infrastructure, facilitating the structured and systematic documentation of security incidents (Simone & Francesco, 2025). These systems enable organizations to capture and record details of incidents, including the nature of the threat, the affected assets, and the response actions taken

(Michail, 2020). Effective incident reporting systems provide a comprehensive log of security events, which is essential for post-incident analysis and future threat mitigation. Traditional incident reporting systems, however, often face challenges related to data integrity, tamper-proofing, and efficiency in handling large volumes of incident data. With the increase in cybercrime, many solutions have been proposed still, the blockchain is considered the most promising infrastructure technology that has the potential to be used in a variety of cybersecurity applications (Vinden et al., 2020).

Blockchain technology offers a transformative approach to incident reporting systems by addressing these challenges through its decentralized and immutable ledger capabilities (Chikelue et al., 2020). By utilizing blockchain, incident reports can be securely recorded and stored in a tamper-proof manner, ensuring that once data is entered, it cannot be altered or deleted. This feature is particularly crucial in maintaining the integrity and authenticity of incident records, which are often scrutinized during forensic investigations and compliance audits. Furthermore, the decentralized nature of blockchain eliminates the risk of a single point of failure, enhancing the reliability and resilience of the incident reporting system (Ravi et al., 2022). Blockchain technology is renowned for its capacity to ensure data integrity and security, two critical components in cybersecurity. Data integrity refers to the accuracy and consistency of data over its lifecycle, which is crucial for maintaining the reliability of incident response systems. According to Duggineni et al. (2023), blockchain achieves data integrity through its immutable ledger, where every transaction is securely recorded and cannot be altered or deleted. This immutability ensures that incident data remains accurate and trustworthy, providing a reliable source of information for analysis and decision-making.

Blockchain's consensus mechanisms play a pivotal role in maintaining data integrity and security. Lasla et al. (2022) reported that consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), ensure that all participants in the network agree on the validity of transactions before they are added to the blockchain. This collective agreement process prevents malicious actors from manipulating the data and ensures that only legitimate transactions are recorded. These mechanisms reinforce the trustworthiness of the blockchain, making it an ideal solution for secure data management in cybersecurity incident response (Shamsad *et al.*, 2025).

2. Design Methodology

An enhanced cybersecurity system using blockchain technology for incidence response processes was designed using high-level Python web framework, Django for building secure and scalable web applications while WSGI server handles the HTTP requests. Figma was also utilized as the design tool due to its robust capabilities in creating detailed blueprints and user interfaces. An embedded SQL database, Microsoft SQL Server was used for local storage accommodating feedback and modifications with ease.

2.1 Cbir-System Architecture

The Cyber-Block Incident Response system (CBIR-SYS) was designed to leverage blockchain technology to facilitate real-time incident reporting for enhancing cybersecurity system. The system consists of several interconnected components that work together to provide a secure and efficient platform for incident reporting, analysis, and response.

The system includes users representing various stakeholders, such as cybersecurity teams, incident reporter, incident responders, and organizational management. Users access into the platform to securely report and analyze incidents in a real-time environment. The system (user interface) enabled users to report cyber threat incidents with relevant details captured in a tamper-proof ledger. The incident data are cryptographically secured to ensure that authorized individuals could access it. The crypto data are analyzed and recorded into nodes via the permission ledger to ensure immutability and transparency of the reported incidents. All reported incidents and associated data are stored in a decentralized database for data integrity. Also, the system incorporates secure communication channels, smart contract, to facilitate collaboration and coordination among stakeholders, ensuring that incident responses are timely and effective. Finally, blockchain network securely manage incident data, automate responses, and facilitate real-time analysis and was visualized on the dashboard to display incident status and identify patterns.

The architectural view of CBIR-SYS system is shown in Figure 1 and the interaction between the system and the nodes was illustrated in the UML Use Case diagram depicted in Figure 2. The process flow of the system was structured in Figure 2 and the database model of the system was depicted in Figure 4.

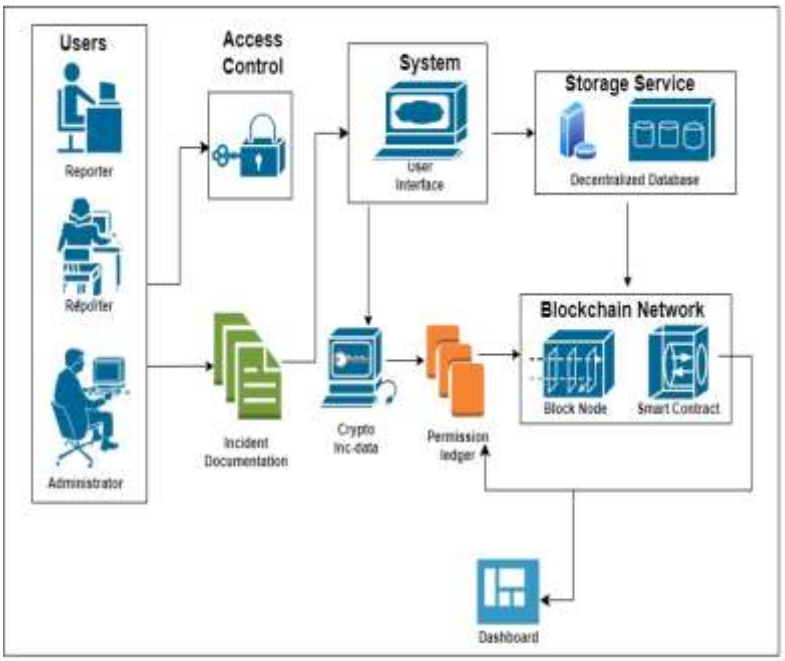

Fig. 1- Cbir system architecture

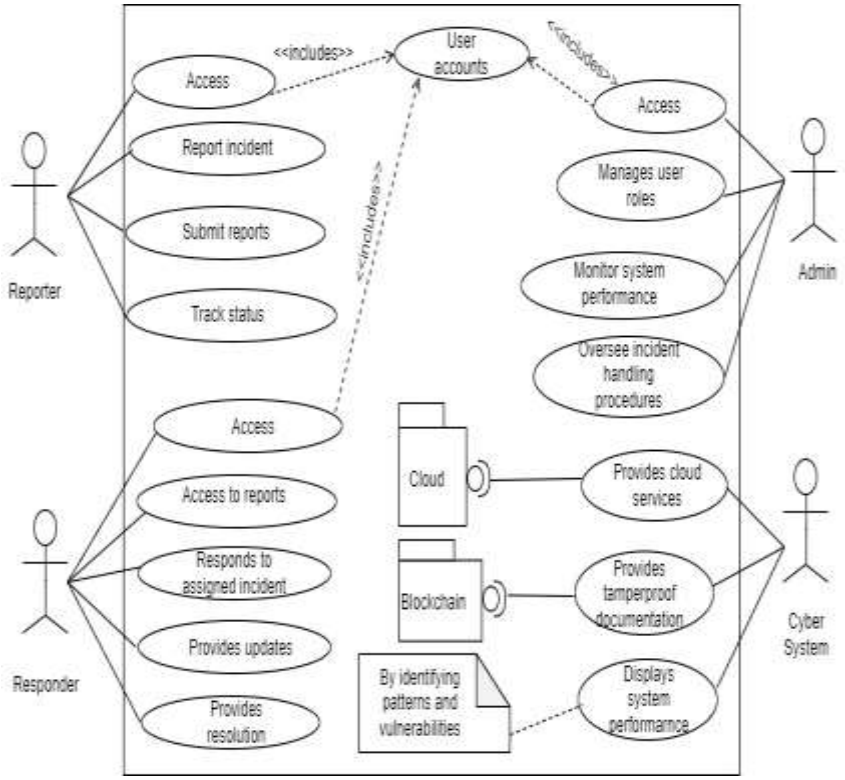

Fig. 2- Cbir – sys use case diagram

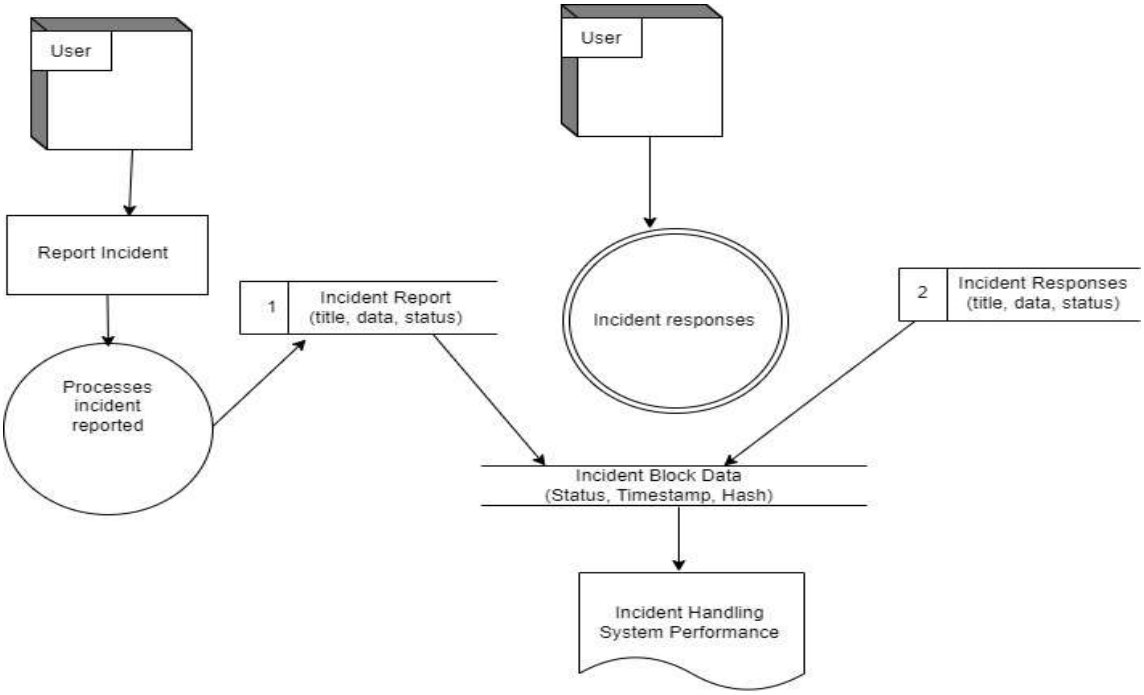

Fig. 3- Process flow of cbir-system

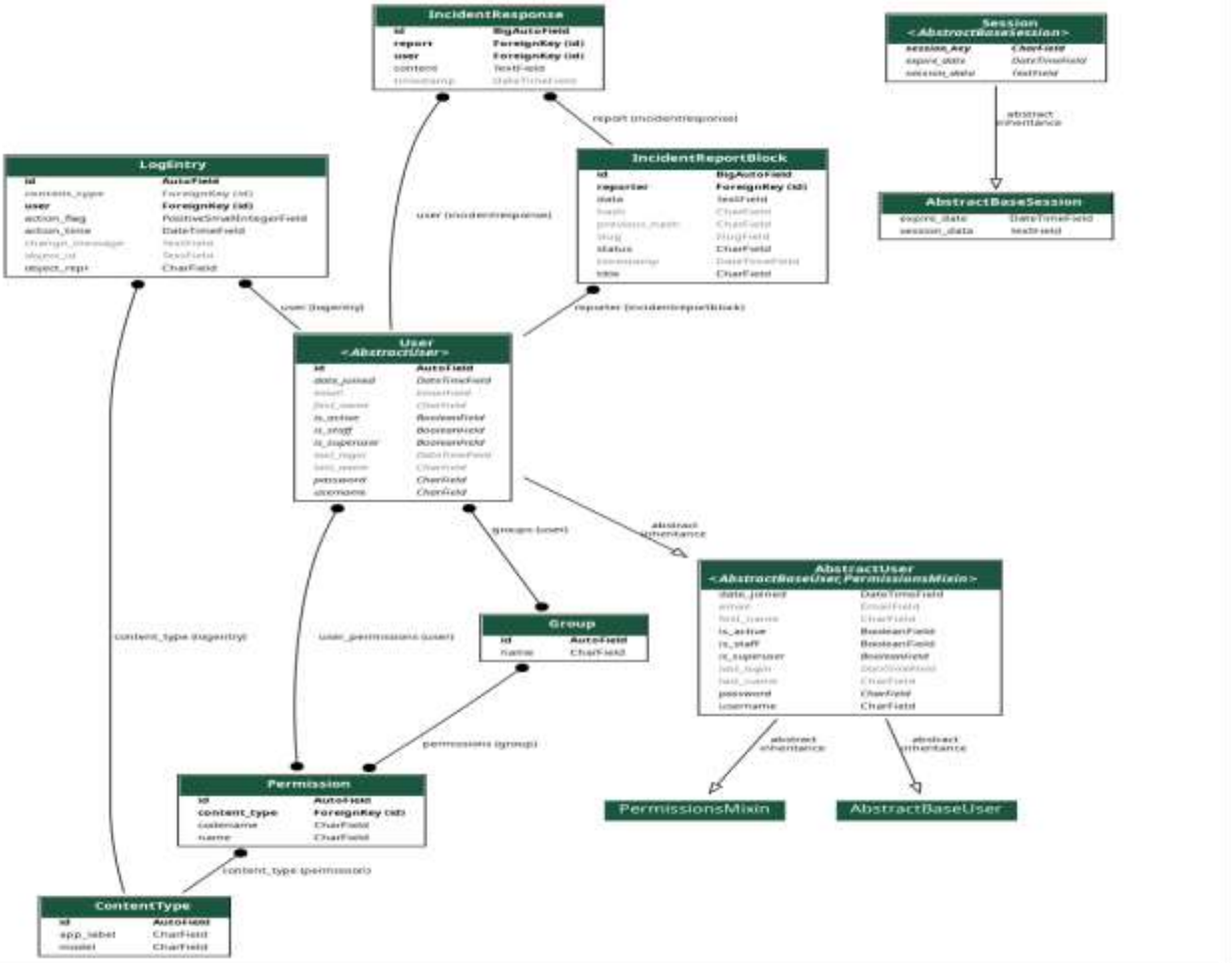

Fig. 4- Data model of cbir-system

3. Results and Discussion

The results of the CBS system were analyzed across several key dimensions, including functionality, security, efficiency, and user experience through system's design, development, and testing phases to enhance cybersecurity incident management. The system was implemented on a web application using Python and Django with minimum hardware requirement of Processor Intel Pentium class 1GHz or higher, 2GB RAM or higher, 60Gb Hard-Disk or higher (recommended), 1GB RAM and 1GHz Processor (for phone), that can run on the server. The software requirements for this application include: Windows 7/ 8, Microsoft SQL server, Internet Information Service (IIS) and Microsoft.Net Framework, Anti-virus software to prevent unwanted attack to the system. Figure 5 depicts the homepage that serves as the landing page and navigation links to other sections.

Fig. 5- Home page

Users can securely access their accounts with their login credentials or alternatively create an account with required information and terms of use as shown in Figure 6 and 7 respectively. Figure 8 depicts an interface where users can report detailed information about potential security breaches or incidents.

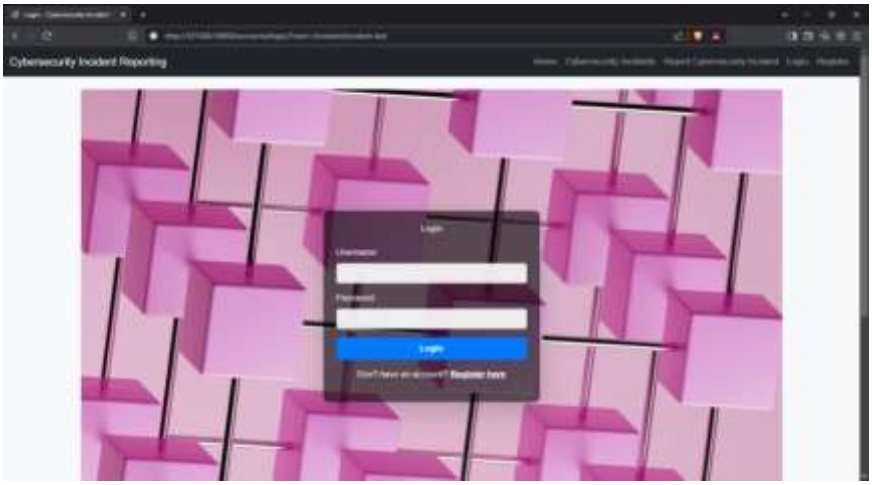

Fig. 6- User login page

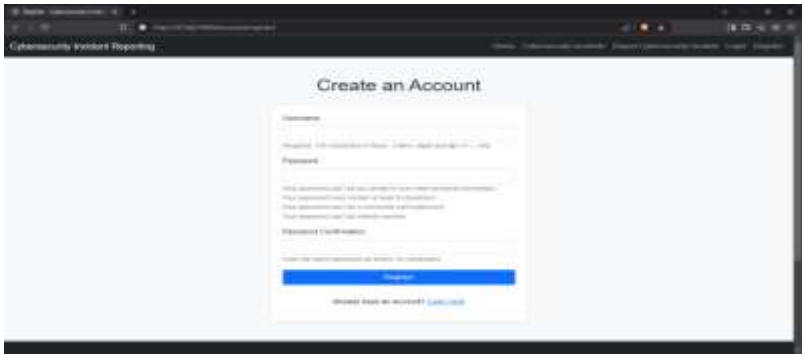

Fig. 7- User registration/signup page

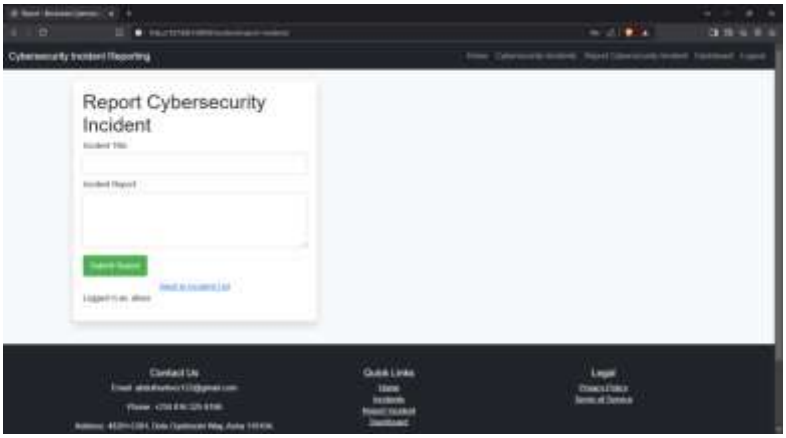

Fig. 8- Cyber incident report page

Analysis of the incident reported is viewed with fields like incident date, status, incident type, reporter and link to the full incident details in Figure 9 while the process of lodging in the incident report by the reporter was shown in Figure 10.

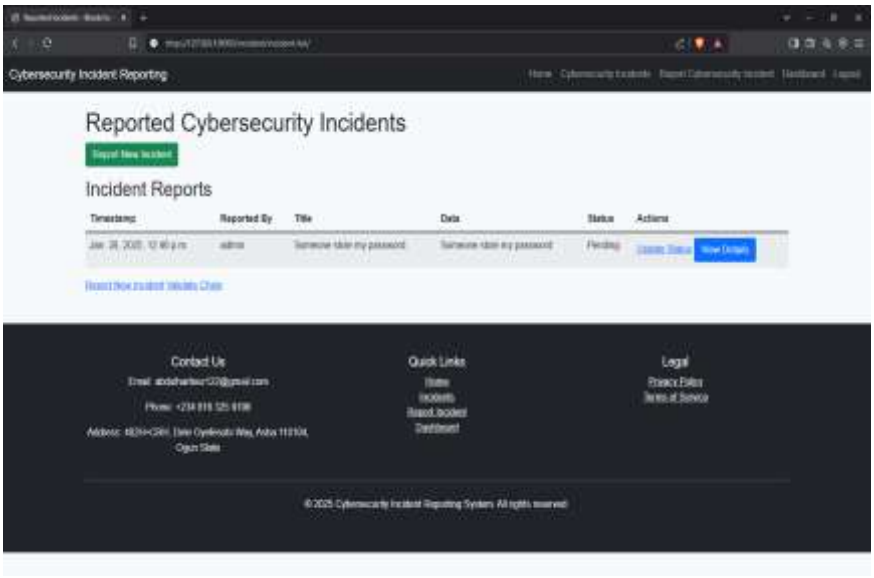

Fig. 9- List of **c**yber incident report page

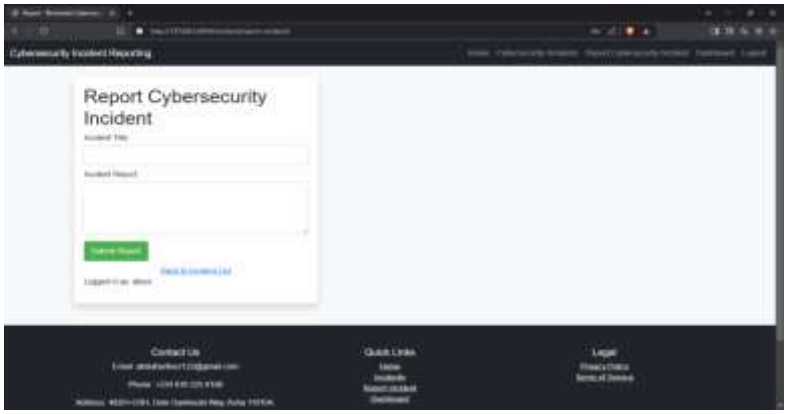

Fig. 10- User reporting a cyber threat incident page

An update and further details on the status of the reported incident was displayed in Figure 11 while the current status of the report and steps taken to resolve and respond to it was shown in Figure 12. The interface that manages the user's profiles, approve/deny reports after scrutinized by blockchain network and manages the incident flows on the dashboard is displayed in Figure 13.

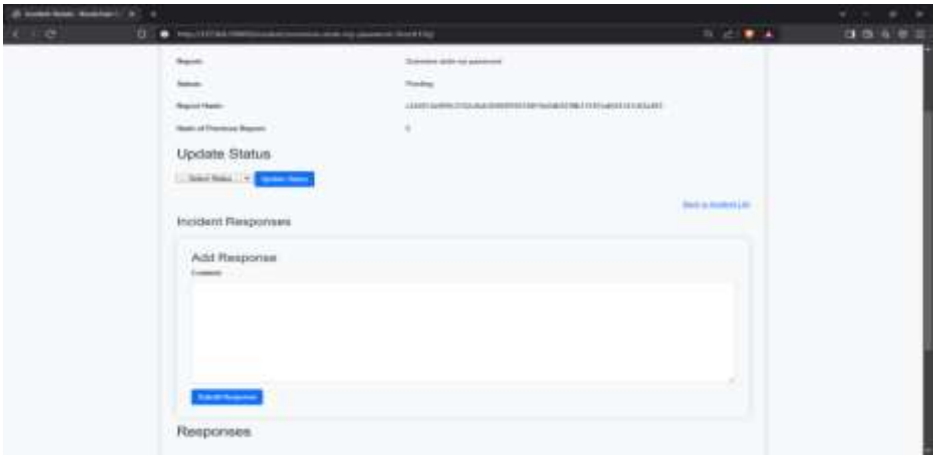

Fig. 11- Incident update page

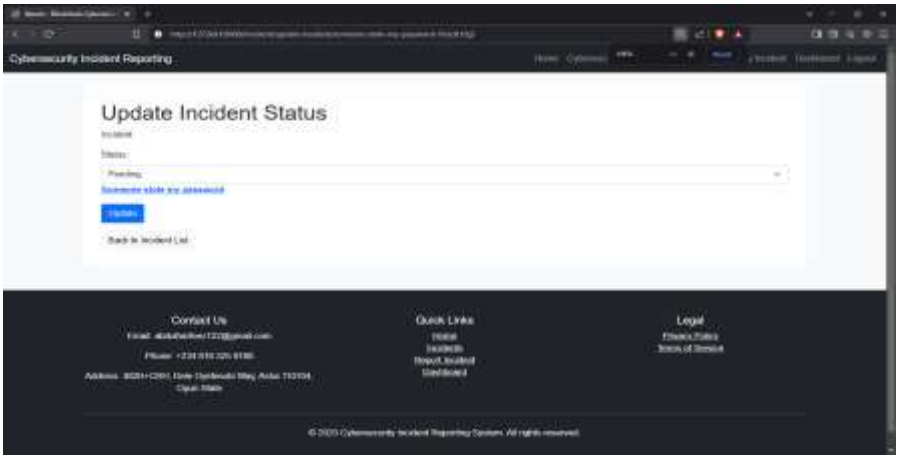

Fig. 12- Incident update status response page

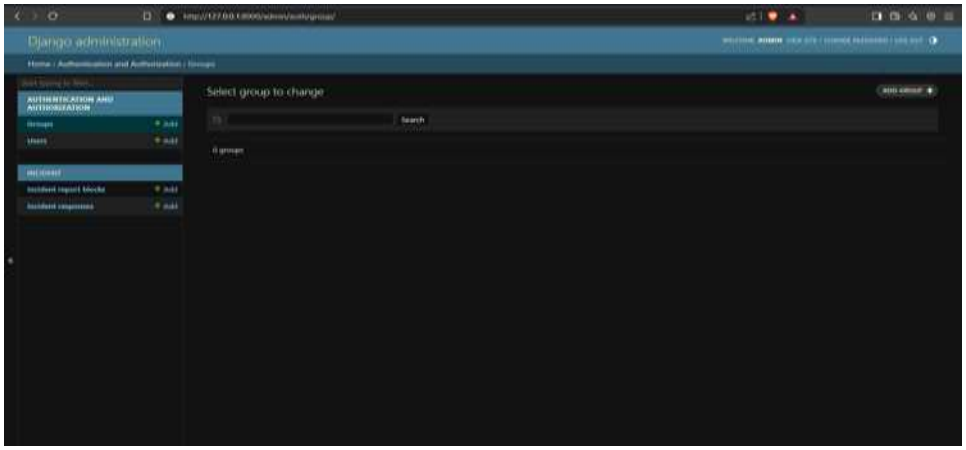

Fig. 13- Incident admin dashboard page

4. Conclusion

The testing and validation of the blockchain-based system for cybersecurity incident response demonstrated that the system functions as intended, offering secure, efficient, and automated tools for incident reporting, analysis, and response. The decentralized nature of the blockchain provides enhanced data integrity, while the integration of smart contracts offers automation capabilities that improve response times and reduce manual workload. The blockchain-based system could serve as a valuable tool in modern cybersecurity incident management, offering a more secure, transparent, and efficient approach to handling cybersecurity threats.

5. References

Adabi, R. M., Parman, S. & Aulia, A. W. (2023). Integrated Security Information & Event Management (SIEM) with Intrusion Detection System (IDS) for live Analysis based on machine Learning. *4th International Conference on Industry 4.0 and Smart Manufacturing*. *217* (2023) ISSN 1406-1415

Chikelue, C. N., Vincent, A. O. & Austine, A. (2020). Blockchain Technology for cybersecurity performance implications on emerging markets multinational corporations: Overview of Nigerian International Banks. *International Journal of Scientific & Technology Research. 9* (08), August 2020. ISSN 2277-8616

Clare, M. P., Jason, R. C., & Virginia, N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *The International Journal of Innovation for the Information security and IT Audit Professional, 132*, September 2023, *https://org/10.1016/j.cose.2023.103309*

Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. *Int. J. Math. Sci. Comput*, *3(1)*, 46-57.

Gourav, N. & Ashok, M. (2024). Understanding the threat Landscape: A Comprehensive Analysis of Cyber-security Risks. *International Journal of Modernization in Engineering Technology and Science*, June *(03)* ISSN 5706-5713

Gustava, G., Maria, F., Iberia, M., Rui, A. & Susana, G. (2021). ETIP: An Enriched Threat Intelligence Platforms for Improving OSINT Correlation, Analysis, Visualization and sharing Capabilities. *Journal of Information Security and Applications*. *58*, May 2021, 102715 *https://doi.or/10.1016/j.jisa.2020.102715*

Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2022). Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Computer Networks*, *214*, 109118.

Michail, A. (2020). Tackling the challenges of information security incident reporting: A decentralized approach. *Phd Thesis, University of East London.* https://repository.uel.ac.uk/item/88q0y

Ravi, P., Sanoop, V. & Asharaf, S. (2022). Blockchain Technology for security: A text Mining Literature Analysis. *International Journal of Information Management Data Insights.* 2(2), November 2022, 100112

Saravanan, A. & Sathya, S. B. (2019). A review on Cyber security and fifty generation cyberattacks. *Oriental Journal of Computer Science and Technology*, ISSN 0974-6471, 2(2), 50-56

Shamsad, B. E., Najmus, M. S. & Ayan, M. K. (2025). Blockchain-Based Security Solution for Secure Financial Transactions in Digital Banking Systems. *International Journal of Computer Applications*. *186* (59), https://doi.org/10.5120/ijca2024294247

Simone, B., & Francesco, M. S. (2025). Evaluating Incident Reporting in Cybersecurity from Threat Detection to Policy Learning. *Government Information Quarterly 42*. 102000

Vinden, W., Nisha, R., John, L., Rushil, B., Edmond, P., Ambikesh, J., Imtiaz, K., Chaminda, H. & Jon P. (2022). Cybersecurity, Data Privacy and Blockchain: A review. *SN Computer Science* (2022) *3*,127. https://doi.org/10.1007/s42979-022-01020-4