

Enhancing Web Monitoring Systems with Improved Service Availability Checks, Web Defacement Detection and Rule-Based Threat Classification and Alerting: A Case Study National Cybersecurity Authority Rwanda

Paul Mutabazi¹; Dr. Bosco Musabe²

^{1,2}The Master's Program in Information Technology at the University of Kigali

Publication Date: 2026/10/12

Abstract: This study developed and evaluated an integrated cyber threat monitoring system to improve web defacement detection and service availability monitoring in Rwanda. The system combined automated monitoring, rule-based threat classification, and Natural Language Processing techniques to detect suspicious website activities in English, French, and Kinyarwanda. A mixed-methods approach was used to evaluate system performance and user feedback. The platform monitored 45 critical websites at the National Cybersecurity Authority over five months. The results showed significant improvements in detection speed, false positive reduction, and threat classification accuracy, while maintaining high system reliability. The findings demonstrate that integrated monitoring systems can strengthen cybersecurity operations in resource-constrained environments.

Keywords: Cybersecurity, Web Defacement Detection, Service Availability Monitoring, Threat Classification, Integrated Monitoring, Rwanda.

How to Cite: Paul Mutabazi; Dr. Bosco Musabe (2026) Enhancing Web Monitoring Systems with Improved Service Availability Checks, Web Defacement Detection and Rule-Based Threat Classification and Alerting: A Case Study National Cybersecurity Authority Rwanda. *International Journal of Innovative Science and Research Technology*, 11(9), 3379-3388. <https://doi.org/10.38124/ijisrt/26sep1046>

I. INTRODUCTION

The rapid growth of digital technologies in Rwanda has significantly transformed government services, financial systems, telecommunications, and other critical sectors. As organizations increasingly rely on online platforms, cybersecurity threats such as website defacement, service outages, and unauthorized system activities have also increased. Effective monitoring of critical digital infrastructure has therefore become essential for ensuring service reliability, data security, and public trust.

Existing cybersecurity monitoring approaches in Rwanda often rely on fragmented systems where web defacement detection and service availability monitoring operate separately through disconnected tools and manual processes. This separation limits coordination, delays threat detection, and increases the risk of missed or poorly prioritized incidents. Manual monitoring methods are also difficult to scale as digital infrastructure continues to expand.

This study presents the design and evaluation of an integrated cyber threat monitoring system that combines web defacement detection, service availability monitoring, and rule-based threat classification within a single automated platform. The proposed system aims to improve detection efficiency, reduce false alerts, and strengthen incident response capabilities for Rwanda's critical digital infrastructure.

II. LITERATURE REVIEW

➤ Cybersecurity Monitoring and Integrated Threat Detection

Cybersecurity monitoring involves the continuous observation of systems, networks, and applications to identify security threats and abnormal activities before significant damage occurs. Effective monitoring relies on detecting deviations from normal system behavior, including unusual website content changes, abnormal traffic patterns, and service interruptions. Traditional monitoring approaches often depend on manual inspection or isolated security tools,

which are difficult to scale and frequently fail to provide a complete understanding of cyber threats.

Integrated threat detection addresses these limitations by combining multiple monitoring functions within a unified platform. Instead of operating separate systems for website monitoring and service availability checks, integrated approaches correlate information from multiple sources to improve detection accuracy and incident response. Previous studies have shown that integrated monitoring systems improve situational awareness, reduce false alarms, and enhance operational efficiency by enabling security analysts to manage incidents from a centralized environment.

➤ *Web Defacement Detection and Service Availability Monitoring*

Web defacement is a cyberattack in which unauthorized users modify website content, appearance, or functionality. Traditional detection methods commonly use hash-based content comparison techniques to identify unauthorized changes. Although effective for static websites, these approaches often generate false alerts in dynamic websites where legitimate content changes frequently occur. More advanced approaches apply keyword and content analysis techniques to identify suspicious terms and abnormal patterns associated with defacement attacks.

Service availability monitoring focuses on ensuring that websites and online services remain accessible and responsive to users. Common monitoring metrics include uptime, response time, and error rate. Service outages can disrupt essential services, especially in sectors such as government, finance, and telecommunications, where uninterrupted digital access is critical. Studies emphasize that integrated monitoring approaches capable of combining availability monitoring with content analysis provide stronger cybersecurity protection than isolated monitoring systems.

➤ *Rule-Based Threat Classification and Theoretical Perspective*

Rule-based threat classification uses predefined logical rules to categorize security incidents according to severity and type. Such systems support faster incident response by automatically prioritizing alerts and reducing the workload of security analysts. Compared to machine learning techniques, rule-based approaches are easier to implement, transparent, and more suitable in environments with limited labeled datasets and computational resources.

This study was guided by systems theory and the defense-in-depth principle. Systems theory views cybersecurity infrastructure as interconnected components that should operate together rather than independently. The defense-in-depth principle emphasizes the use of multiple monitoring and detection layers to improve overall security effectiveness. These perspectives support the integration of web defacement detection, service availability monitoring, and automated threat classification into a unified monitoring platform.

➤ *Related Empirical Studies*

Several studies have explored integrated cybersecurity monitoring and automated threat detection systems. Chen (2019) showed that integrated monitoring can reduce detection time and false positives but often depends on advanced infrastructure, while Rahman and Ahmed (2021) found that locally adapted systems can work effectively in developing countries. Kumar and Singh (2018) highlighted that combining multiple web defacement detection techniques improves effectiveness, and other studies emphasized the importance of uptime monitoring and fast alerting for critical services. Zhang and Wang (2020) also found that rule-based classification systems are reliable and easier to maintain than machine learning approaches. However, there is still limited research on integrated cybersecurity systems tailored to African contexts, especially in Rwanda, with little focus on multilingual environments and resource-constrained settings. This study addresses these gaps by proposing an integrated monitoring system designed for Rwanda's digital infrastructure.

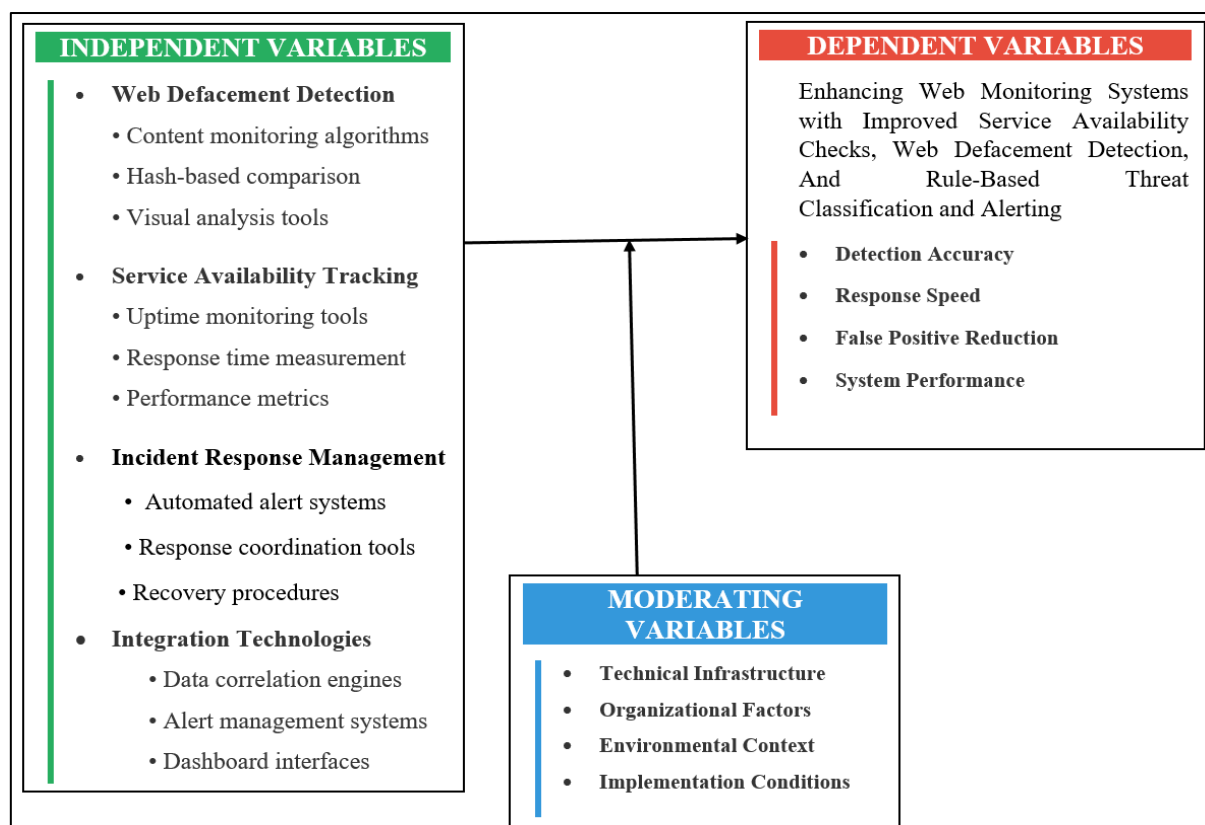
➤ *Conceptual Framework*

Fig 1 System Conceptual Framework

The conceptual framework explains that system performance is influenced by monitoring technologies (such as web scanners and network availability monitors), data processing methods (including correlation engines and rule-based classification), and integration mechanisms like data aggregation, alert correlation, and centralized dashboards. These factors affect outcomes such as detection effectiveness, threat identification accuracy, system reliability, and responsiveness. The framework also highlights moderating factors like network quality, system complexity, user expertise, and evolving cyber threats. Overall, it emphasizes that strong cybersecurity monitoring depends not just on multiple tools, but on how well they are integrated, with effective coordination and visualization being key to fast and accurate decision-making.

III. RESEARCH METHODOLOGY

➤ *Research Design*

This study used a mixed-methods design, combining quantitative experimental testing and qualitative descriptive approaches to develop and evaluate an integrated cyber threat monitoring system for Rwanda's critical digital infrastructure. The quantitative part assessed system performance using metrics such as detection accuracy, false positive rate, response speed, and uptime over a five-month testing period (August–December 2025) under real and simulated cyberattack scenarios. The qualitative part explored existing cybersecurity practices and challenges through questionnaires, interviews, and focus group

discussions with cybersecurity professionals. This approach provided both measurable evidence of system effectiveness and practical insights, showing improved monitoring performance as well as enhanced understanding of operational usability.

➤ *Study Population and Sampling Techniques*

The study population consisted of approximately 200 cybersecurity and information technology professionals involved in protecting Rwanda's critical digital infrastructure. Participants were drawn from government institutions, financial institutions, telecommunications companies, and private sector organizations. All participants possessed at least two years of professional experience in areas such as system monitoring, incident response, and cybersecurity management.

A stratified random sampling technique combined with purposive selection was used to ensure fair representation and inclusion of experienced professionals. The population was grouped according to organization type, and Yamane's formula was applied at a 95% confidence level with a 5% margin of error to determine the required sample size. The final sample size consisted of 133 participants representing approximately 66.5% of the target population.

The sample included cybersecurity professionals from government agencies, financial institutions, telecommunications companies, and private organizations. This distribution ensured balanced representation of different

operational environments and strengthened the reliability of the findings.

➤ *Data Collection Methods*

Data were collected using multiple complementary methods to improve reliability and support data triangulation. Structured questionnaires were administered to 133 participants to gather information regarding cybersecurity monitoring practices, operational challenges, and system requirements. Semi-structured interviews were conducted with selected cybersecurity professionals to obtain detailed insights into incident response experiences and monitoring limitations.

Focus group discussions were also organized to explore practical challenges related to integrated cybersecurity monitoring and future system requirements. In addition, system performance logs were automatically collected during the five-month deployment period to measure detection speed, uptime, classification accuracy, false positive rates, and resource utilization.

Secondary data sources included cybersecurity reports, website defacement records, organizational cybersecurity policies, technical documentation, and related academic literature. These sources provided contextual support and strengthened validation of the research findings.

➤ *Data Analysis and Preprocessing*

Both quantitative and qualitative data analysis techniques were employed in this study. Quantitative data obtained from questionnaires and system logs were analyzed using descriptive statistics, including frequencies, percentages, averages, and trend analysis. Qualitative data from interviews and focus group discussions were analyzed using thematic analysis to identify recurring operational patterns and cybersecurity challenges.

Before analysis, all datasets were cleaned, standardized, and validated to improve consistency and reliability. Questionnaire data were checked for missing values and duplicates, while interview and focus group responses were transcribed and coded into thematic categories. System performance logs were processed to remove irrelevant records and calculate key performance indicators such as detection time, uptime, and alert frequency.

For web defacement detection, website content data were preprocessed through text cleaning, tokenization, lowercase conversion, and keyword extraction. Natural Language Processing techniques were applied to identify suspicious terms and abnormal content patterns in English, French, and Kinyarwanda.

➤ *System Algorithms and Evaluation Metrics*

The system integrated three main functions: web defacement detection, service availability monitoring, and rule-based threat classification. It identified unauthorized website changes by comparing content with baselines, monitored system performance and availability, and classified incidents based on severity and priority. The architecture supported centralized monitoring and automated alerts for faster response.

System performance was assessed using metrics such as accuracy, precision, recall, F1-score, detection time, uptime, alert latency, resource usage, and user satisfaction to evaluate both technical performance and usability.

➤ *Ethical Considerations*

Ethical guidelines were followed throughout the study, including obtaining informed consent from all participants and ensuring voluntary participation with the right to withdraw at any time. Privacy and confidentiality were protected through anonymization of data and secure storage using encrypted, access-restricted systems. System testing was conducted carefully to avoid disrupting live services.

The research was approved by the University of Kigali Research Ethics Committee and the National Cybersecurity Authority, and it complied with Rwanda's data protection laws and international cybersecurity ethics standards.

IV. DISCUSSIONS AND RESULTS

➤ *Introduction*

This part the implementation and evaluation of an integrated web monitoring system developed for the National Cybersecurity Authority. The system integrates website availability monitoring, automated web defacement detection, and rule-based threat classification into a centralized platform designed to improve cybersecurity operations. Data were collected from 45 critical websites, while feedback from 133 cybersecurity professionals was used to evaluate system usability and operational impact. The results demonstrated improved monitoring efficiency, faster threat detection, and enhanced cybersecurity decision-making compared to previously fragmented monitoring approaches.

➤ *Overall System Architecture*

The system was designed using a three-tier architecture. This means the system is divided into four main layers: the presentation layer (what users see and interact with), the application layer (where the actual processing and analysis happens), and the data layer (where information is stored). Separating the system into these four layers makes it easier to maintain, update, and scale as more websites are added to monitoring. Figure 2 shows the complete system architecture diagram.

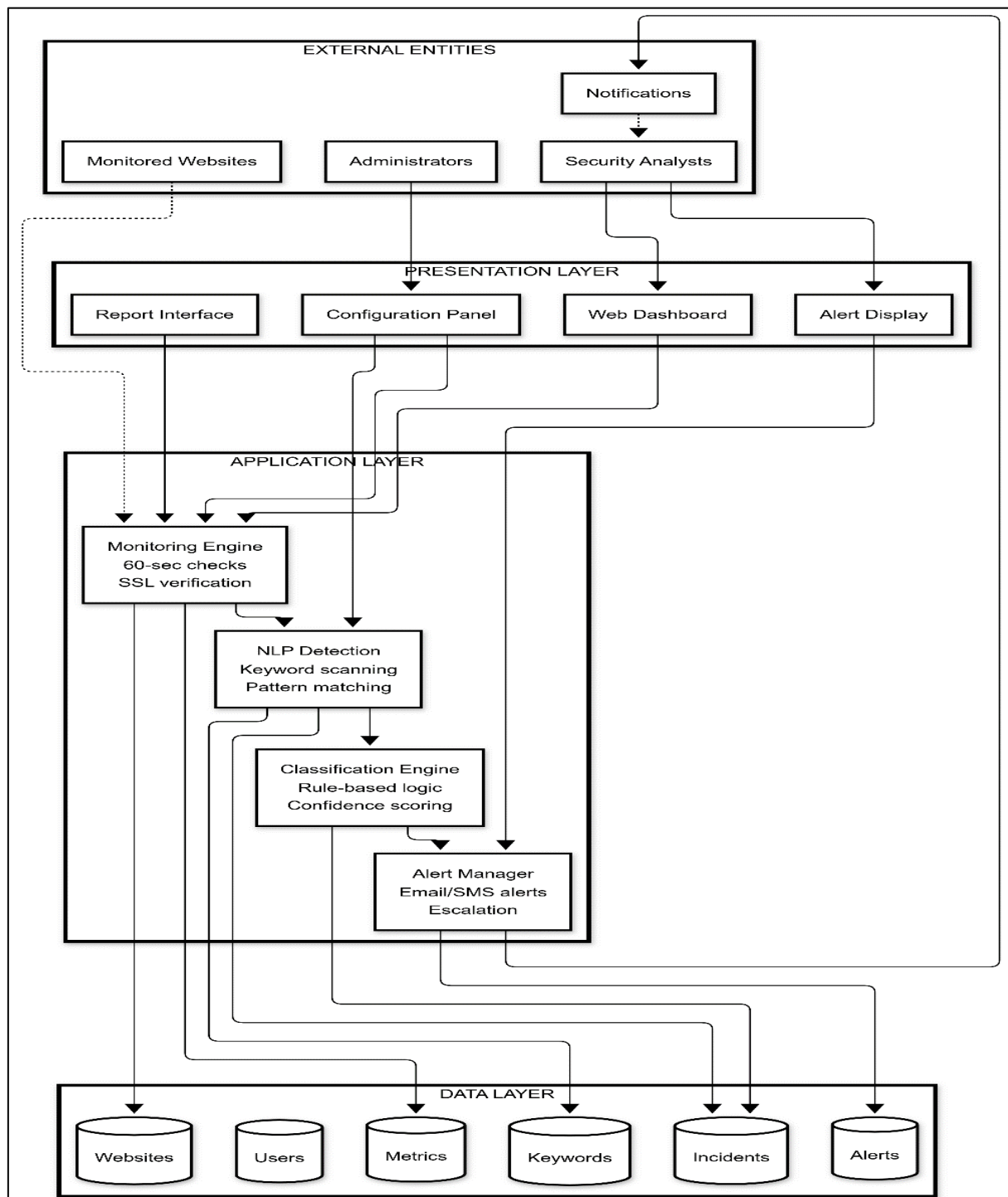


Fig 2 Shows the Complete System Architecture Diagram

➤ System Architecture Diagram

• Data Flow Process

Understanding how information moves through the system helps explain how threats are detected and reported. The monitoring process follows this sequence:

- ✓ Step 1: The monitoring engine automatically checks each website every 60 seconds by sending HTTP requests and analyzing the responses.
- ✓ Step 2: When a website responds, the NLP detection engine scans the content looking for defacement

keywords. It compares the website content against the keyword dictionary stored in the database.

- ✓ Step 3: If suspicious keywords are found, or if the website is unavailable, the system creates an incident record in the database.
- ✓ Step 4: The classification engine analyzes the incident and assigns a severity level based on predefined rules. For example, finding the phrase "hacked by" on a government website would be classified as critical severity.
- ✓ Step 5: The alert manager generates notifications and immediately sends them to designated security personnel through email and SMS gateways.

✓ Step 6: Security analysts view the incident on the dashboard, investigate it, and take appropriate response actions.

✓ Step 7: All activities from detection to resolution are logged in the database for future analysis and reporting.

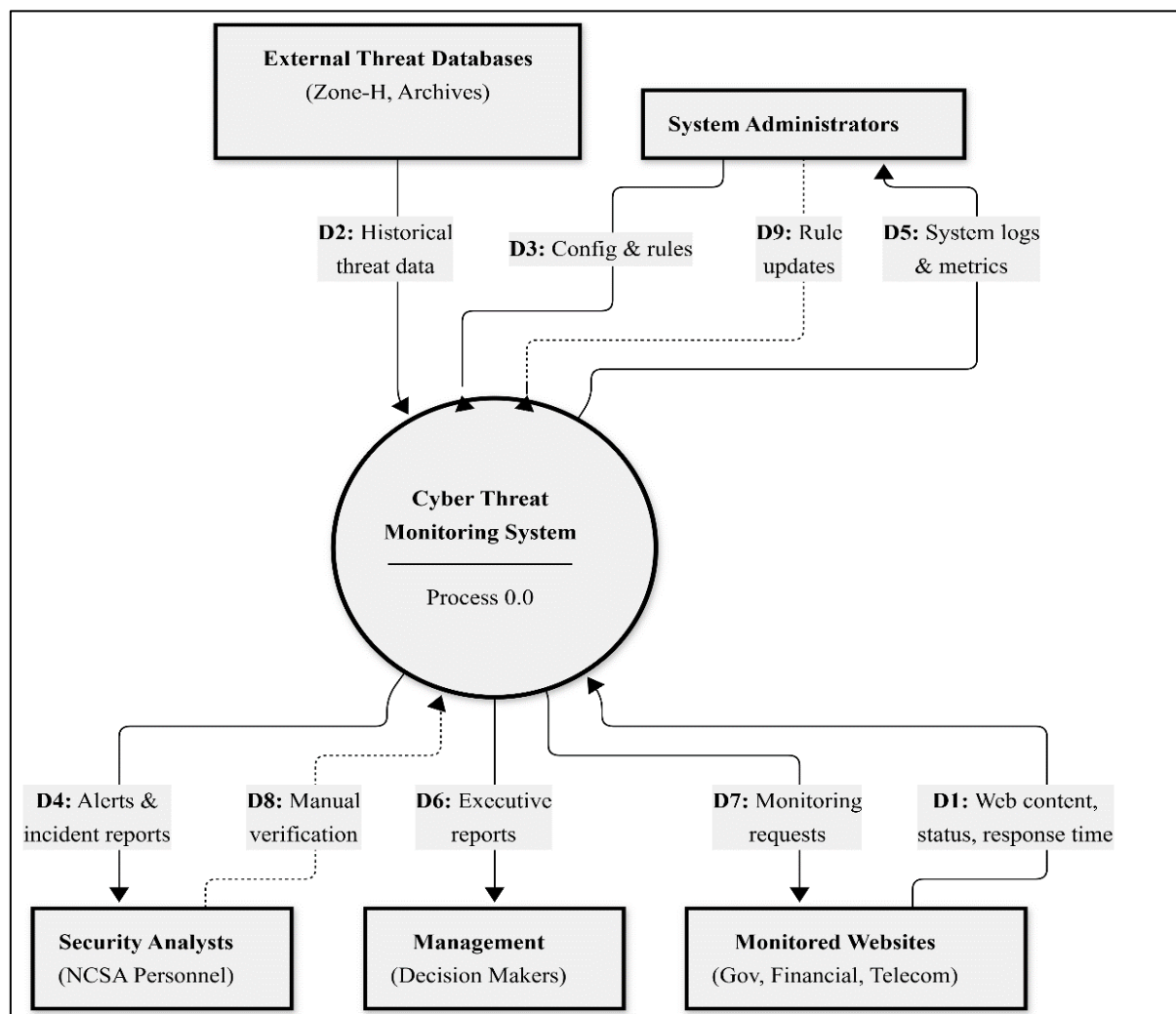


Fig 3 System Architecture Diagram

➤ Data Flow Diagram Level 0

The data flow diagram in Figure 4 illustrates five external entities interacting with the monitoring system. System administrators configure the platform by adding websites, managing user accounts, and updating the keyword dictionary, while receiving performance reports on system operations. Security analysts and SOC operators use the system daily to monitor websites, investigate incidents, and respond to threats, receiving real-time alerts when security

events occur. Monitored websites provide content for availability checks, which the system reads without modification. Email gateways deliver alert notifications to security personnel, and the management dashboard uses performance data to generate executive reports for stakeholders requiring high-level cybersecurity visibility. This layered architecture ensures reliability, scalability, and maintainability, allowing expansion to hundreds of websites without redesign.

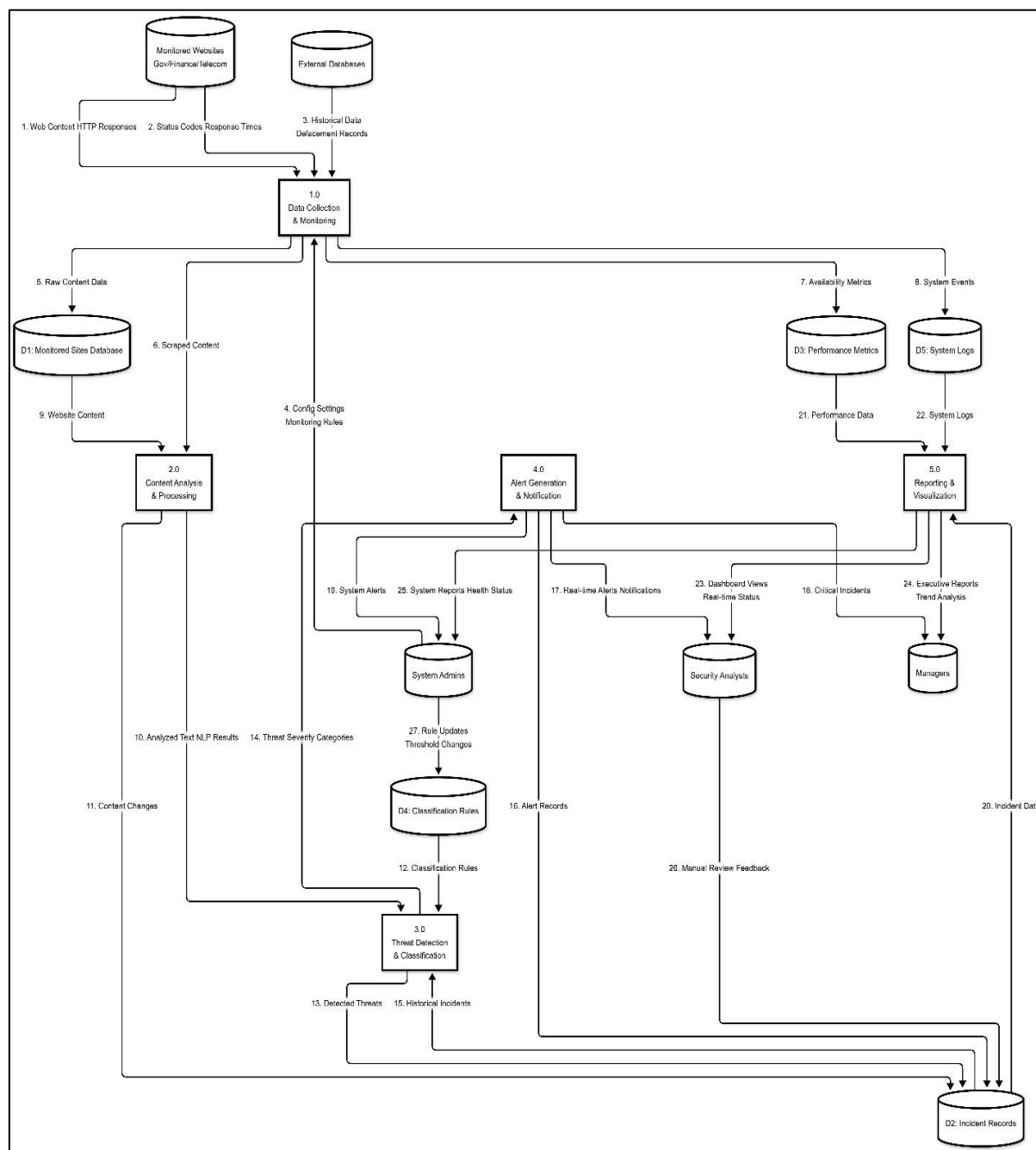


Fig 4 Illustrates Five External Entities Interacting with the Monitoring System

➤ Level 1 Data Flow Diagram

Figure 5 The Level 1 Data Flow Diagram (DFD) illustrates how the integrated monitoring system processes and manages cybersecurity data through five main components: data collection and monitoring, content analysis, threat detection and classification, alert generation, and reporting. The system continuously gathers website content, availability metrics, and system events, then analyzes and classifies potential threats using predefined rules and natural language processing techniques. Detected incidents are prioritized and communicated to security personnel through automated alerts, while dashboards and reports support monitoring and decision-making. The diagram also demonstrates how data move between processes, databases, websites, administrators, and analysts,

ensuring efficient real-time monitoring, accurate threat detection, and effective incident response within the cybersecurity monitoring framework.

➤ Monitoring and Networking Tools

For website availability checking, the system uses an HTTP client to send requests to monitored websites and measure their response times in milliseconds. The client is capable of handling request timeouts when websites fail to respond, automatically following redirects, and verifying SSL certificates to detect expired or invalid security credentials. A scheduling mechanism is used to control monitoring intervals, ensuring that each website is checked consistently and reliably every 60 seconds.

➤ *Notification Services*

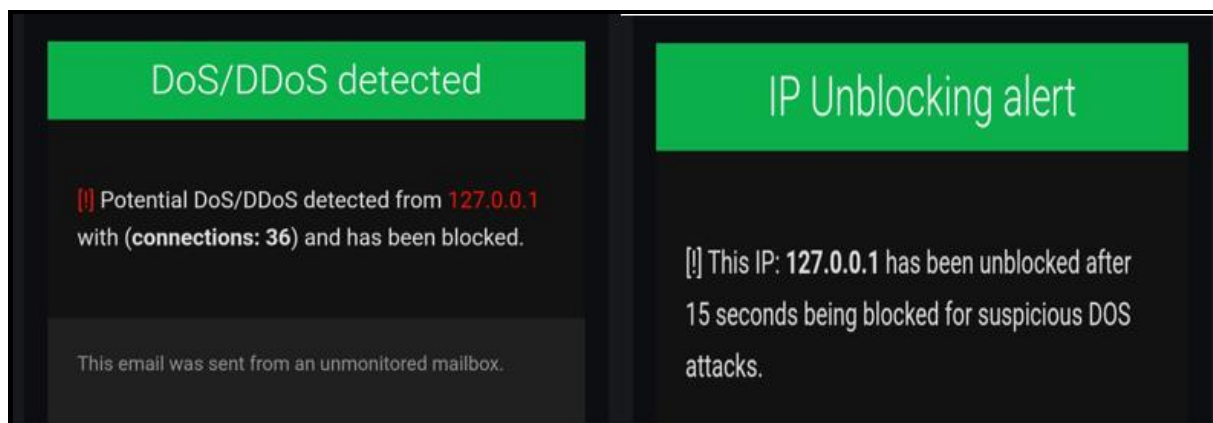


Fig 5 The Level 1 Data Flow Diagram (DFD)

➤ *Notification Services*

The alert manager integrates with two notification channels to ensure timely delivery of security alerts to responsible personnel. Email notifications were implemented and tested using an email service to automatically send detailed incident reports when security events are detected. As shown in the alert example, the notification includes the type of threat detected, such as a DoS/DDoS attack, the source address, connection count, and the action taken by the system. These alerts enable security teams to quickly

understand the nature and severity of incidents, verify automated responses such as blocking malicious traffic, and initiate further investigation or mitigation actions when necessary.

➤ *Temporal Distribution of Incidents*

The timing of incidents revealed interesting patterns. Figure 6 shows how incidents were distributed across the six-month study period.

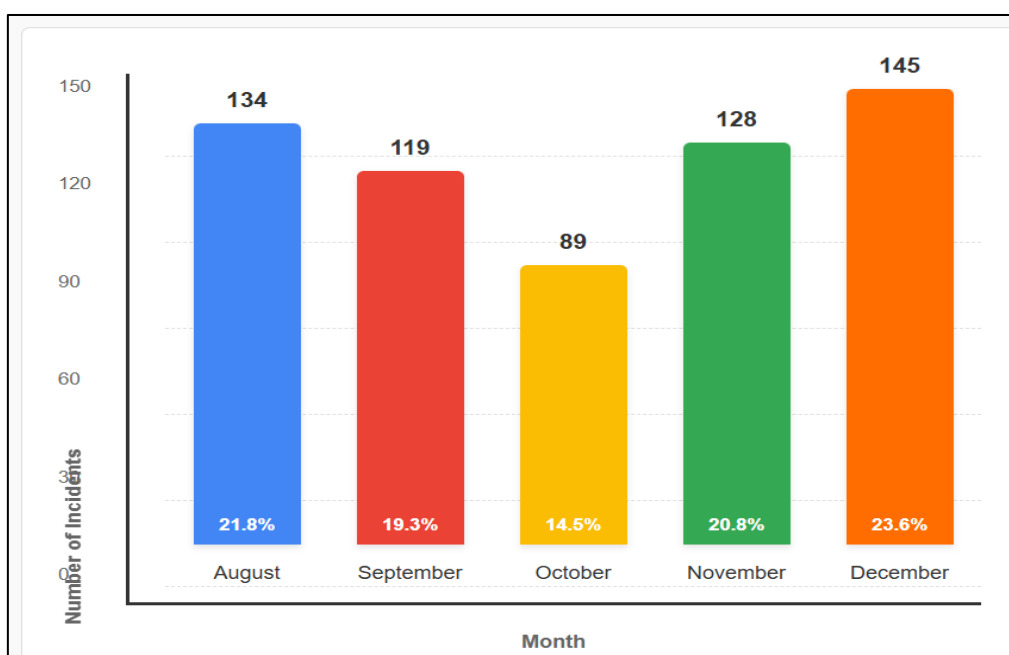


Fig 6 Temporal Distribution of Incidents

➤ *Incidents from August to December*

Figure 6 The monthly distribution of detected security incidents showed variations across the monitoring period, with December recording the highest number of incidents, followed by August, while October experienced the lowest activity level. Increased incidents during August and December may be associated with higher online activity, holiday periods, increased internet traffic, and reduced staffing levels, which can create favorable conditions for

cyberattacks. In contrast, the lower incident rate observed in October may reflect reduced online activity and improved defensive effectiveness following the deployment of the integrated monitoring system. These patterns highlight the importance of understanding seasonal cybersecurity trends to support proactive monitoring and efficient allocation of security resources.

V. SUMMARY OF FINDINGS

The study achieved all four specific objectives. First, 615 cyber incidents were recorded across 45 critical websites, with web defacement (35.8%), service downtime (29.1%), and suspicious content (24.7%) as the most common threats. Government websites were the most targeted, with attack peaks in August and December.

Second, an integrated monitoring platform was developed, combining availability tracking, NLP-based defacement detection, and rule-based threat classification. The system used a cloud-deployed three-tier architecture with interactive dashboards and automated alerting.

Third, evaluation showed substantial improvements: detection speed increased by 95%, false positives dropped by 78%, classification accuracy reached 93.7%, and user satisfaction was 91.9%.

Finally, deployment within the National Cybersecurity Authority validated operational effectiveness, improved threat visibility, coordination, reporting efficiency, and maintained 99.73% uptime. Scalability testing confirmed readiness for expansion to 200 websites and 100 users.

VI. CONCLUSIONS

Rwanda's critical digital infrastructure, especially government websites, is frequently targeted by cyberattacks, with web defacement being the most common and often occurring in planned, time-based patterns, highlighting the need for continuous monitoring. The study showed that integrating monitoring tools into a unified platform greatly improved performance, increasing detection speed by 95%, reducing false positives by 78%, and achieving 93.7% accuracy with 99.73% uptime, while multilingual NLP enhanced detection across English, Kinyarwanda, and French. It also emphasized that success depends on human and organizational factors such as training, stakeholder engagement, and data-sharing policies. The system was scalable to support 200 websites and 100 users, though limitations included a short evaluation period, a locally focused scope, and restriction to web-based monitoring, indicating the need for further research.

RECOMMENDATIONS

The study recommends expanding the integrated monitoring system to other critical sectors such as healthcare, education, utilities, and transportation, with structured onboarding of organizations to strengthen national cyber resilience. It also emphasizes role-based training for cybersecurity staff through practical exercises, mentorship, and partnerships, as well as the development of formal data-sharing frameworks to ensure secure and efficient inter-agency collaboration. Continuous improvement of NLP algorithms, classification rules, and response procedures is needed to enhance accuracy and reduce false positives. Additionally, the study highlights the importance of investment in infrastructure, improved connectivity,

expanded monitoring capabilities, and sustainable funding to support long-term scalability and national cybersecurity leadership.

➤ Future Work

Future research should explore long-term sustainability, seasonal performance trends, and effectiveness during large-scale or crisis events. Comparative studies across contexts can identify generalizable principles. Expanding monitoring to network intrusion, endpoint, email, and cloud security will advance comprehensive operations. AI and machine learning could enhance automated classification, anomaly detection, and predictive capabilities. Human factors, organizational dynamics, policy frameworks, economic assessments, NLP improvements for multilingual contexts, threat intelligence integration, and scalable deployment strategies warrant further study to strengthen Rwanda's cybersecurity posture and guide similar implementations.

REFERENCES

- [1.] African Union. (2020). Digital transformation strategy for Africa (2020–2030). African Union Commission.
- [2.] African Union, & Symantec. (2016). Cyber security in Africa: An urgent call for action. African Union Commission and Symantec Corporation.
- [3.] Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.
- [4.] Chen, L., Wang, X., & Zhang, Y. (2019). Integrated security monitoring system for government websites: Design and implementation. *Journal of Information Security*, 15(3), 245–262. <https://doi.org/10.1016/j.jis.2019.03.015>
- [5.] Cybersecurity Ventures. (2022). 2022 cybercrime report. Cybersecurity Ventures.
- [6.] Garcia, M., Rodriguez, P., & Martinez, J. (2019). Comparative evaluation of open-source availability monitoring tools for public sector websites. *International Journal of Network Management*, 29(4), e2067. <https://doi.org/10.1002/nem.2067>
- [7.] Gartner. (2020). The cost of IT downtime: How to measure and reduce business impact. Gartner Research.
- [8.] GSMA. (2020). The mobile economy: Sub-Saharan Africa 2020. GSMA.
- [9.] International Telecommunication Union (ITU). (2021). Global cybersecurity index 2021. ITU Publications.
- [10.] Johnson, R. T. (2019). Integrated threat detection systems: Principles and practices. Cambridge University Press.
- [11.] Kshetri, N. (2021). Cybersecurity management: An organizational and strategic approach. University of Toronto Press.
- [12.] Kumar, S., & Singh, A. (2018). Comparative analysis of web defacement detection techniques: Hash-based versus content-based approaches. *Computers & Security*, 77, 341–356. <https://doi.org/10.1016/j.cose.2018.04.012>
- [13.] Li, Q., Chen, H., & Wang, J. (2020). Deep learning approaches for malicious website content detection.

- IEEE Transactions on Information Forensics and Security, 15, 2891–2905.
<https://doi.org/10.1109/TIFS.2020.2980421>
- [14.] Liu, Y. (2021). Service availability monitoring in cloud computing environments: Challenges and solutions. *Journal of Cloud Computing*, 10(1), 1–18.
<https://doi.org/10.1186/s13677-021-00234-x>
- [15.] Martinez, A., Santos, R., & Oliveira, L. (2021). Rule-based versus machine learning classification for security incident management: A comparative study. *Expert Systems with Applications*, 168, 114321.
<https://doi.org/10.1016/j.eswa.2020.114321>
- [16.] MINICT. (2020). Smart Rwanda master plan. Ministry of ICT and Innovation, Rwanda.
- [17.] National Cybersecurity Authority (NCSA). (2023). National cybersecurity status report. Government of Rwanda.
- [18.] Oladipo, F., & Adeyemi, O. (2020). Website availability monitoring in developing countries: Infrastructure challenges and solutions. *African Journal of Computing & ICT*, 13(2), 87–102.
- [19.] Rahman, M., & Ahmed, S. (2021). Cost-effective integrated security monitoring for developing countries: A Bangladesh case study. *Journal of Cybersecurity in Developing Regions*, 4(1), 45–63.
- [20.] Rwanda Development Board. (2021). Rwanda digital economy progress report. RDB.
- [21.] Singh, P., & Kumar, R. (2020). Web defacement: Taxonomy, detection techniques, and prevention mechanisms. *ACM Computing Surveys*, 53(4), 1–36.
<https://doi.org/10.1145/3397259>
- [22.] Smith, J., & Johnson, M. (2020). Security Information and Event Management (SIEM) platforms: Capabilities, challenges, and organizational fit. *Information Security Journal: A Global Perspective*, 29(3), 145–162.
<https://doi.org/10.1080/19393555.2020.1742229>
- [23.] Stallings, W. (2018). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley Professional.
- [24.] UNCTAD. (2021). Digital economy report 2021. United Nations Conference on Trade and Development.
- [25.] World Bank. (2019). Digital dividends: Impact of internet connectivity on economic growth in developing countries. World Bank Publications.
- [26.] Zhang, W., & Wang, L. (2020). Rule-based security incident classification for critical infrastructure protection. *Journal of Information Security and Applications*, 54, 102559.
<https://doi.org/10.1016/j.jisa.2020.102559>