Cybersecurity Challenges and Centralized Monitoring Solutions for e-Governance in Zambia: A Literature Review

LUKUMBA PHIRI, STEVE MUWOWO
Department of Electrical and Electronic Engineering
University of Zambia
Lusaka
ZAMBIA

Abstract: E-government digital platforms are often attacked by sophisticated cybersecurity threats because of the sensitive nature of the information and services they provide. The analysis finds that these systems have vulnerabilities due to fragmented security architectures, not enough skilled personnel, limited budgets, and reactive security approaches, particularly within developing countries such as Zambia. This study reviews existing research on cybersecurity challenges affecting e-government systems, focusing on Government-to-Business (G2B) digital platforms in developing countries. It also examines established cybersecurity frameworks, including Defence-in-Depth (DiD), NIST CSF, ISO/IEC 27001, and the Zero Trust model. The study also reviews the role of Centralized Security Monitoring Platforms (CSMPs) integrated with Intrusion Detection and Prevention Platforms (IDPPs) in improving threat visibility, event correlation, and coordinated incident response. A lightweight validation approach is carried out using a virtualized environment, which relies on open-source platforms such as pfSense, Suricata, and Wazuh to show how the centralization of monitoring increases situational awareness and correlates events to show the relevance of the proposed solution within a resource-constrained environment. The study further identified some operational and technical challenges that affect the adoption of effective cybersecurity practices within e-government infrastructures and highlights the importance of scalable, cost-effective, and integrated monitoring infrastructures to manage cybersecurity proactively in developing countries.

Key-Words: - Centralized Security Monitoring, Cybersecurity, Intrusion Detection and Prevention, e-Governance, Frameworks.

Received: March 28, 2026. Revised: May 27, 2026. Accepted: June 19, 2026. Published: July 15, 2026.

1 Introduction

1.1 Background

The global shift towards e-governance has transformed public service delivery, enhancing efficiency, transparency, and accessibility [1]. Governments now commonly interact with citizens (G2C), businesses (G2B), employees (G2E), and other government entities (G2G) through digital platforms [2]. However, such an increase in digital platform interactions has significantly increased the attack surface, making government networks prime targets for cybercriminals and threat actors. This has made cybersecurity even more critical to ensure service continuity, citizen data is protected, and to maintain integrity and trust [3].

Governments that provide digital G2B services through public sector digital platforms in institutions in developing countries such as Zambia are becoming increasingly vulnerable to advanced cyber-attacks, due to a lack of infrastructure integration, knowledge, and financial resources [4]. These public institutions like any other are now facing an evolving and complex threat landscape marked by advanced persistent threats (APTs), zero-day exploits, insider attacks, data tampering, unauthorised access, and attacks that disrupt the operation of systems [5], leading to a negative impact on the confidentiality, integrity and availability of digital data, which undermines public trust in government data management [6]. Similar institutions have security controls consisting of fragmented architectures, old integration settings, and poorly configured access controls [7]. This makes it difficult for security teams to obtain a centralized

view of organisational threats, contributing to delayed detection, reduced situational awareness, and ineffective incident response [8]. As a result, many security operations remain reactive. Threats may exist without being detected within network environments until a significant disruption occurs.

1.2 Review Methodology

A structured literature review was done to analyze the literature on cybersecurity challenges, cybersecurity measures, and intrusion detection methodologies that apply to e-governance systems. This included selected academic articles from IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. Official guidelines on cybersecurity standards were put into consideration.

This review involved literature written from 2010 to 2025, using keywords such as "e-governance cybersecurity," "centralized security monitoring," "SIEM," "IDS," "IPS," "cybersecurity in governments," and "cybersecurity frameworks". The following inclusion criteria were set to select the relevant literature:

- works addressing cybersecurity challenges specific to e-governance systems or governments;
- articles discussing centralized monitoring, SIEMs, IDSs, or IPSs;
- papers focusing on security frameworks and operational security issues;
- publications that provide implementation strategies.

Literature unrelated to cybersecurity challenges faced by public institutions and not involving technical aspects of centralized monitoring and intrusion prevention was ruled out. The collected literature was analyzed further to identify common cybersecurity challenges, existing frameworks, approaches to centralized security monitoring and IDS/IPS implementation, and knowledge gaps relevant to e-governance.

1.3 Research Contributions

This paper makes the following contributions:

- It provides a structured overview of cybersecurity challenges that affect e-governance systems in developing countries.
- Evaluates the relevance of key cybersecurity frameworks within resource-limited environments.
- Proposes a CSMP-IDPP framework utilizing open-source technologies.
- Supports the proposed approach with lightweight validation derived from simulated cyberattack scenarios.
- Identifies existing research gaps related to integration, governance and operational cyber security monitoring

1.4 Organisation of the Paper

The rest of this paper is structured as follows: Section 2 gives an overview of the cybersecurity challenges affecting e-governance platforms. Section 3 reviews cybersecurity frameworks relevant to public institutions. Section 4 examines CSMP-IDPP approaches. Section 5 discusses the problem framework validation and security analysis. Section 6 summarises research gaps identified in the literature. Section 7 concludes the review.

2 Cybersecurity Challenges in e-Governance.

Government platforms face threats including Advanced Persistent Threats (APTs), zero-day exploits, ransomware, insider threats, and data tampering [9].

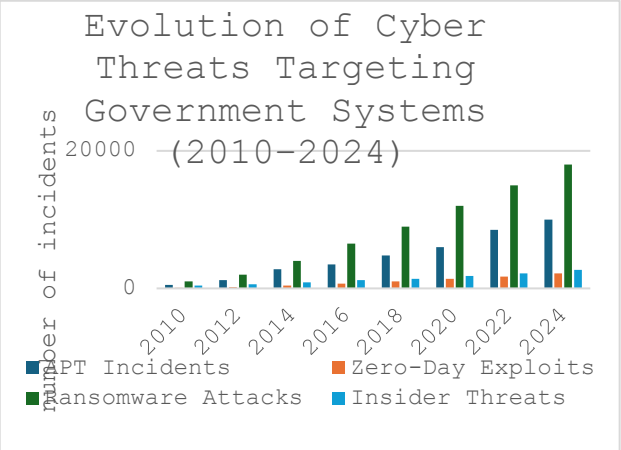

Fig. 1 Cyber threats targeting Public Institutions

Fig. 1 shows some of the evolution of cyber threats targeting public institutions.

These threats exploit fragmented architectures, a lack of centralized monitoring, and poorly configured access controls that remain common in public administration [10] The lack of a centralized monitoring platform leads to delayed detection and inefficient incident response, reinforcing the need for integrated monitoring solutions [11]. These systems are kept in

a regulated environment with limited budgets and complex governance models, yet with the need for high availability [9]. Studies show that fragmented cybersecurity controls are used to address challenges that lead to delayed incident detection and response due to a lack of real-time intrusion monitoring, a lack of log correlation, and full visibility of the entire threat landscape on the network, hence reactive approaches to cyber threats [8]. Research further indicates that the use of fragmented structures, as is often the case in many developing countries, frequently results in the deployment of isolated and outdated security tools, leaving critical systems vulnerable to attacks [12]. During cybersecurity incidents, outdated reporting systems are downright brittle, especially where uncertain responsibilities, unclear roles, and a misaligned governance framework often lead to ineffective decision-making [13], [14]. Fig 2 shows a summary of cybersecurity challenges experienced by e-Governance systems.

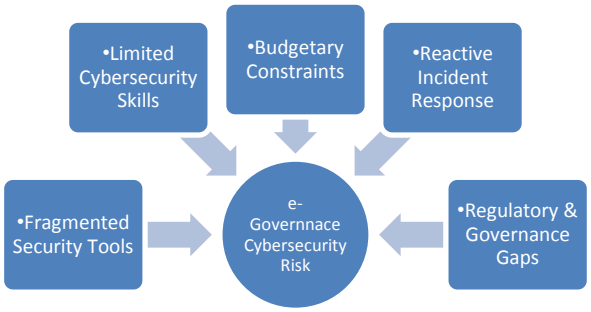

Fig. 2 Cybersecurity Challenges Affecting Government E-governance Platforms.

These challenges affect government institutions responsible for managing confidential data related to the public sector. This lack of a common cybersecurity framework mirrors the overall national problem of fragmented system architecture and little cybersecurity expertise [15]. Therefore, the literature highlights the importance of a Centralized Security Monitoring Platform (CSMP) integrated with Intrusion Detection and Prevention (IDP), and how a hybrid architecture may improve the cybersecurity posture while offering a scalable and cost-effective Solution.

Zambia's cybersecurity threats have shown a trend of segmentation, fragmentation, lack of skills, and insufficient institutional coordination [16]. Table 1 outlines cybersecurity challenges affecting registry platforms. These cybersecurity threats highlight the importance of having effective monitoring systems that increase visibility, incident detection, and coordination in e-governance systems.

Table 1 Key Cybersecurity Challenges Affecting e-Governance Platforms.

Challenge	Description	Impact on e-Governance Security	References
Fragmented Security Architecture	Firewalls, IDS, and VPNS operating independently	Delayed threat detection and weak correlation	Khan et al. (2024)
Limited Skilled Personnel	Shortage of skilled analysts for information security	Slow response and misconfigured controls	Nuraeni, Nugraha, and Aminanto (2025)
Budget Constraints	High cost of proprietary tools	Too much reliance on minimal or outdated solutions	Nuraeni, Nugraha, and Aminanto (2025)
Reactive Security Posture	Focus on incident response rather than proactive monitoring and measures	Increased dwell time of attackers	Bellamkonda (2026)
Governance & Policy Gaps	Limited alignment between policy guidelines and technical controls	Compliance risk and inconsistent enforcement	Rebeiro (2025), Anil and Babatope (2024)

The cybersecurity challenges highlighted above indicate the need for more systematic and coordinated cybersecurity approach to improve visibility, control, resilience, and incident management across public digital infrastructure. The importance of a centralized security monitoring platform integrated with intrusion detection and prevention systems is widely recognised as critical for boosting efficiency in an e-government environment. It is therefore important to discuss the existing cybersecurity framework, which is relevant to e-governance ecosystems.

3 Frameworks for Securing e-Governance Platforms.

To address these challenges, several established frameworks and models provide structured guidance for building cybersecurity resilient systems [17]. These frameworks ensure that the confidentiality, integrity, and availability of important information, as it enables organisations to systematically identify assets, assess threats, implement safeguards, and ensure rapid recovery, hence facilitating a safe and efficient online system for the administration and operations of the government [18]. The development of cybersecurity frameworks has been influenced by the need to deal with technologies and changing security threats [19].Fig 3 show a conceptual representation of these frameworks which include:

- The National Institute of Standards and Technology Cybersecurity Framework [3].
- ISO/IEC 27001 Information Security Management System [20].
- The Zero Trust security model [21].
- The Defence-in-Depth model [22].

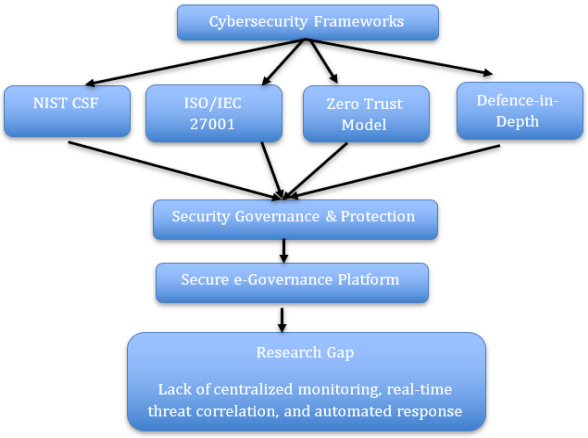

Fig. 3 Cybersecurity frameworks for securing e-Governance

These frameworks help address cybersecurity challenges. While these frameworks provide strategic guidance, they do not explicitly define implementation mechanisms for centralized monitoring and real-time threat correlation, creating a gap between policy and operational security. Table 2 shows a summary of the cybersecurity frameworks relevant to the study.

Table 2 Comparison of Cybersecurity Frameworks Relevant to e-Governance Platforms

Framework / Model	Core Focus	Applicability in Zambia	References
Defence-in-Depth (DiD)	Layered security controls across systems and networks	Provides redundancy, but fragmented deployment may limit centralized monitoring integration.	Caballero (2013)
NIST Cybersecurity Framework	Risk-based cybersecurity management	Provides structured governance but requires mature implementation capacity.	NIST CSF (NIST, 2018)
ISO/IEC 27001	Governance, risk management, and compliance	Supports accountability and continuous improvement but may be resource intensive.	Culot et al. (2021)
Zero Trust Security Model	Continuous verification and least-privilege access	Strengthens access control but requires advanced identity infrastructure and skills.	Gajbhiye, Jain, and Goel (2023)
Combined Framework Relevance	Strategic cybersecurity alignment	Supports policy alignment, but no single framework provides unified centralized monitoring.	Salman and Alsajri (2023)

4 Centralized Security Monitoring and Intrusion Prevention Roles.

4.1 Centralized Security Monitoring Platform (CSMP).

Centralized security monitoring refers to the process of consolidating security events and system log messages generated by different infrastructure components in an integrated monitoring environment for

analysis and reporting purposes [23]. The major components of CSMP include log collection tools, an event correlation and analysis component, the dashboard component, and alert components [24]. Centralized monitoring improves the detection of suspicious activities such as repeated authentication attempts, unusual scanning of the network, attempts to escalate privileges, and malicious traffic behaviour. In this regard, CSMP provides more supportive evidence in an investigation as it enables a fast detection of the vectors of attacks.

4.2 Intrusion Detection and Prevention Platform (IDPP).

Intrusion Detection and Prevention Platforms (IDPPs) combine the capabilities of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) [25]. IDPPs perform signature-based and anomaly-based strategies that enable real-time identification of threats and facilitate preventive actions such as dropping a packet, IP blockage, and execution of automated tasks [25],[26]. Most Intrusion detection and Prevention technologies use multiple methodologies, either separately or integrated, to provide broader and more accurate detection [27].

When integrated into the CSMP, IDPP allows for the real-time analysis of network activity and system behaviour, permitting the platform not only to identify threats but also to block malicious network activity. Table 3 shows a comparison of the features of CSMP and IDPP. Integrating IDPP capabilities into a CSMP ensures that security monitoring does not stop at alert generation but is linked to enforcement and mitigation controls.

Table 3 CSMP vs IDPP Comparison

Concept	CSMP (SIEM-focused)	IDPP (IDS/IPS-focused)	Reference
Role	Visibility + correlation	Detection + prevention	Kent and Souppaya (n.d.)
Input	Logs from various systems	Network traffic patterns	Pekarčík et al. (2025)
Output	Alerts, dashboards	Alerts, drops/blocks	Ravindran, Ojha, and Kamboj (2025)
Key benefit	Central intelligence	Real-time defence	Ravindran, Ojha, and Kamboj (2025)

4.3 CSMP-IDPP Integration Architecture.

Existing literature indicates that a practical Centralized Security Monitoring Platform (CSMP) integrated with Intrusion Detection and Prevention Platform (IDPP) capabilities can be realised through the integration of multiple security components operating at different layers of the network [28]. In such architectures, network traffic is monitored at the perimeter, internal network, and endpoint levels, enabling comprehensive visibility of security events.

Within such integrated systems, each component takes up a specific role. Firewalls like pfSense act as the perimeter enforcement layer responsible for controlling traffic flow and logging the activity on the network [29],[30]. Intrusion detection systems represented by Suricata provide deep packet inspection and generate alerts based on known attack signatures and suspicious behaviour[31]. Security Information and Event Management (SIEM) systems, such as Wazuh, aggregate logs collected from different machines, analyze the collected logs, and provide centralised dashboard views for better interpretation [32],[33]. The proposed architecture corresponds to the concept of defence in depth, which means that although some attacks may not be detected in one layer, they will certainly be identified in another [21], [34]. This approach increases situational awareness and supports proactive cybersecurity management in e-government.

Table 4 Functional Roles of Components within Proposed CSMP-IDPP Architecture

Component	Function	Key Logs	References
pfSense Firewall	Used as the perimeter gateway for routing, enforcement of access control, and firewall log generation	Firewall events, blocked connections, and allowed traffic logs	Senthilkumar and Muthukumar (2018)
Suricata IDS/IPS Service	Analyzes network traffic, generates intrusion alerts, and performs prevention actions when operating in IPS mode	IDS alerts and IPS drop logs	Guo, Guo, and Zhang (2022)
Wazuh SIEM	Provides centralized log aggregation, event correlation, dashboard visualization, and alert generation for security monitoring	Correlated alerts, dashboards, and SIEM event records	Dixit and Tripathi (2025)

4.4 CSMP Benefits and Challenges.

Available literature indicates various advantages of central monitoring, including enhanced situational awareness and reduced investigative time through unified evidence collection. There are challenges, however, including tuning the correlation rules and coping with false positives without performance overheads on log ingestion, challenges that are often made even worse by resource-constrained environments.

The centralization of logs and alerts across these components significantly enhances cybersecurity processes by making it possible to correlate the information collected from multiple data sources. In addition to analysing logs from different systems, security analysts can observe a sequence of events, facilitating faster identification of attack patterns and improved response coordination. This addresses the limitations of fragmented security deployments commonly reported in public sector environments. Table 5 shows the typical benefits and challenges of the CSMP IDPP.

Table 5 CSMP Benefits and Challenges

CSMP Benefit	Typical Challenge	References
Central visibility	False positives & noise	Ozkan-Okay et al. (2021)
Faster investigations	Log volume overload	Pekarčík et al. (2025)
Better correlation	Integration complexity	Dixit and Tripathi (2025)
Compliance evidence	Skills gap	Hamid and Huda (2025)

5 Framework Validation and Security Analysis

In e-governance systems, there is continuous interaction between public-facing services, internal users, network gateways, endpoints, and databases, and monitoring systems. As such, from a cybersecurity perspective, all these elements may be viewed as an interconnected combination of nodes, services, and events that need to be correlated to derive security insights. Cyberattacks usually exploit weaknesses in authentication mechanisms, exposed services, network exposure, lack of policy enforcement, and lack of proper monitoring mechanisms. Therefore, an effective centralized security monitoring system becomes important for improving visibility and cybersecurity for e-government platforms.

5.1 Security Monitoring Model.

Let the e-governance environment under consideration be described as the set of assets as presented in equation 1 below:

$$A = \{a1, a2, ..., an\} \quad \text{Equation 1}$$

Where A represents the set of assets with e-government environment, theses may include servers, endpoints, gateways, applications, as well as monitoring components. Also, let

$$T = \{t1, t2, ..., tm\} \quad \text{Equation 2}$$

T represents the set of threats targeting these assets represented by equation 2. These include phishing attacks, unauthorized access, malware activity, reconnaissance scans, denial of service, and insider threats.

In the centralized security monitoring design model, any security events that arise from any of the elements contained in set A will be monitored and analyzed to determine if any of them represent potential threats, which will be categorized under set T. This monitoring process includes the logging of security events and sending out of security alerts through different infrastructures.

Security monitoring in the e-governance may then be defined as a problem of detecting malicious activities within a system, correlating alerts generated by different tools, and taking actions in time. However, when security monitoring tools generate alerts independently leads to problems of delayed alerts, duplicates, and lack of overall situational awareness. The proposed CSMP-IDPP addresses challenges through its ability to integrate firewall technologies and intrusion detection/prevention systems and SIEM monitoring systems within a comprehensive security management monitoring infrastructure.

5.2 Threat Landscape in e-Government Systems

The common types of cyber-attacks on the infrastructures in e-governance are reconnaissance scanning, brute-force attacks on authentication services, web application exploitation, communication between machines that have been infected with malicious software, privilege escalation, and violation of the integrity of files [5]. The purpose of reconnaissance is to find out live hosts, open ports, services, and vulnerabilities.

In brute-force attacks, different passwords and usernames are used to break into authentication services [5]. Web application exploitation refers to exploiting public portals [35], whereas file integrity violations could suggest a possible intrusion and attempts to make changes to files. Advanced persistent threats should be mentioned because of their long-term nature and high-value targets [36]. Although the complete replication of APTs in a laboratory environment is difficult, it is possible to study the behaviour of such attacks by analyzing suspicious access attempts, privilege escalations, and abnormal communication patterns with the outside world through the network.

To improve cybersecurity visibility and ensure proper incident response, the use of a centralized monitoring architecture ensures that security events generated from different infrastructure elements are continuously monitored and correlated. In the SIEM system, the security logs generated by various components such as the firewall, IDS, endpoint, authentication, and network devices are collected and analyzed in case of suspicious activity for further investigation. This process is illustrated in Fig. 4.

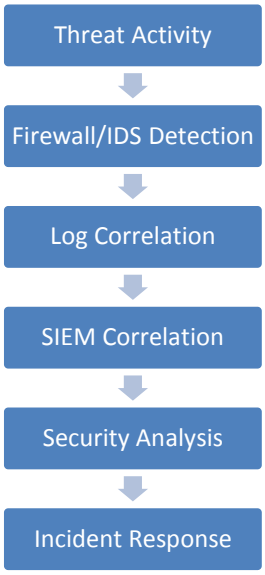

Fig. 4 Centralized Security Monitoring Workflow in E-Governance Systems.

In conclusion, the above discussion shows the need for a security architecture that capable of processing events from different sources.

5.3 Existing Defences Against the Identified Threats.

Existing defences used against attacks on e-governance include firewalls, intrusion detection systems (IDS), intrusion prevention system (IPS), endpoint monitoring tools, access controls, and security information and event management (SIEM) solutions [23]. Firewalls act as traffic filtering devices at the boundary between the internal network and Internet connections. IDS/IPS analyzes network flows looking for abnormal traffic and known attack signatures. Endpoint monitoring tools help in capturing events related to the activities on individual computers [37].

Even as these security controls provide critical protection mechanisms, devices operating independently often lead to fragmented visibility and delayed response coordination. A firewall could generate an

alert regarding connection attempts, IDS might raise alerts for scans, while endpoint monitoring raises alerts for failed login attempts. Centralized monitoring addresses this challenge through integration of log analysis, alerts, and other event data from various security tiers in a centralized monitoring platform. Centralized monitoring helps improve situational awareness and allows for better threat detection or response.

Table 6: Example Security Controls and Monitoring Roles

Security Control	Monitoring Role	References
Firewall	Traffic filtering and logging	Senthilkumar and Muthukumar (2018)
IDS/IPS	Threat detection and prevention	Suricata Documentation (2026)
SIEM	Event correlation and centralized monitoring	Wazuh Documentation (2026)
Endpoint Monitoring	Host activity visibility	Caballero (2013); R et al. (2025)
Access Control Systems	Authentication monitoring	Gajbhiye et al. (2023); Culot et al. (2021)

5.4 Detection Performance Metrics

The following equations are conceptually utilized to measure the efficiency of detection, alert reduction, and false positives.

(1) $Detection\ Rate = \frac{(Number\ of\ Detected\ Attacks)}{Total\ Simulated\ Attacks} x100$

Detection rate refers to the percentage of attacks that are detected by the security monitoring system.

(2) $Alert\ Reduction = \frac{(Initial\ Alerts - Reduced\ Alerts)}{Initial\ Alerts} x100$

The reduction in alerts means the level to which duplicate alerts are eliminated thanks to correlation and rules optimization.

(3) $False\ Positive\ Rate = \frac{Incorrect\ Alerts}{Total\ Normal\ Events} x100$

False positive rate is used to measure the percentage of false alarms that are generated based on benign system events.

(4)

$Latency = Detection\ time - Attack\ Initiation\ Time$

Latency is measured as the time between attack execution and alert generation.

(5)

$Resource\ Utilisation = \frac{consumed\ system\ resources}{Total\ Available\ Resources} x100$

Resource utilization shows how much of the system's resources such as CPU and memory have been used by the monitoring system.

(6) $TPR = TP/(TP + FN)$

True Positive Rate (TPR) is another name for Recall or Sensitivity, which describes the percentage of the total number of true positives detected by the system out of the entire dataset.

(7) $FPR = FP/(FP + TN)$

False Positive Rate (FPR) is the ratio of the number of true events incorrectly classified as malicious events.

(8) $Precision = TP/(TP + FP)$

Precision is the percentage of the total number of true positives out of all positive decisions made by the monitoring system.

(9) $Recall = TP/(TP + FN)$

Recall represents the percentage of correctly detected malicious events by the monitoring system.

(10) $ROC = \{(FPR, TPR)\}$

A receiver operating characteristic curve (ROC) graphically displays the interplay between false positive rate (FPR) and true positive rate (TPR) when classifying events.

(11) $AUC = \int TPR(FPR)\, d(FPR)$

The Area Under the Curve (AUC) is used to measure the discriminative power of classifiers for identifying malicious events.

Confusion matrices are to assess the effectiveness of detection using true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN).

5.5 Framework Validation Environment

A virtual, lightweight validation environment based on open-source cybersecurity solutions was conceptually designed to evaluate the feasibility of applying the CSMP-IDPP architectural design. The validation environment involved the use of pfSense firewall as the network gateway device, Suricata as an intrusion detection and prevention engine, and Wazuh as a centralized SIEM platform. The environment also included internal virtual machines acting as user devices and application services commonly found in e-government systems. Generated logs and security events from various sources were aggregated and analyzed in the centralized monitoring server.

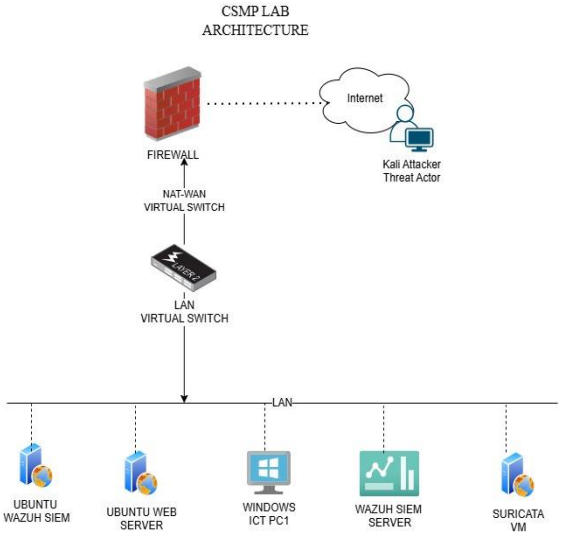

Fig. 5 Proposed CSMP-IDPP Architecture

As such, the purpose of the validation exercise was not to perform comprehensive penetration testing but to show how a central cybersecurity monitoring solution improves visibility and management of security threats in resource-limited environments. Fig. 5 illustrates the overall structure of the proposed CSMP-IDPP architecture.

5.6 Threat Validation Scenarios.

Several typical cyber-attack scenarios potentially applicable to e-government systems were selected for the validation process. The following scenarios have been chosen:

5.6.1 Reconnaissance scanning

The alerts are triggered by the intrusion detection module due to any suspicious scan targeting the public services on the network. The alerts were then correlated with firewall events on the SIEM platform to improve visibility and centralize the analysis process.

5.6.2 Brute force attacks

Brute force attack scenarios are used to generate alerts in the intrusion detection system, which led to the triggering of correlation rules in the centralized monitoring platform, which helped detect unusual authentication actions.

5.6.3 File integrity violation.

A few scenarios are designed for testing file integrity monitoring to see how the changes to important files can be identified and reported via centralized event correlation.

5.6.4 Suspicious Network Traffic Pattern

Any unusual network traffic and communication attempts are analyzed to demonstrate the effectiveness of centralized monitoring in identifying suspicious network activities.

The results of the validation showed that integration of intrusion detection alerts and firewall logs with centralized event correlation enhances cybersecurity in e-government systems.

5.7 Validation Results and Operational Analysis

The validation results show that the suggested CSMP-IDPP framework improves visibility, event correlation, and collaboration among the security monitoring processes on various infrastructure layers. Events related to the security system generated by firewalls, IDSs, and endpoint monitoring were

successfully correlated in the centralized SIEM system.

The utilization of centralized monitoring capabilities helped in the detection of suspicious behaviors because of the correlation of events created by different security systems, therefore preventing issues with monitoring security events on an isolated basis.

Moreover, it can be seen from the validation experiment that centralization helps in increasing awareness due to the fact that it enabled security operators to analyze related attacks within one dashboard rather than analyzing each event separately.

While the experimentation occurred within virtualized lab conditions, the findings confirm that centralized monitoring and intrusion prevention can be efficiently implemented within resource-limited public sector entities with the use of open-source technology-based solutions.

However, the validation approach used during the experiment helped in understanding some of the operational difficulties encountered when implementing cybersecurity within developing nations, such as a lack of expertise, complex infrastructure, difficult tuning of alerts, and other resource constraints.

As a result, the current research highlights the importance of designing and utilizing integrated and cost-efficient cybersecurity architecture.

6 Research Gaps and Analytical Discussion

Existing literature provides valuable insights into cybersecurity architectures and threat mitigation strategies in e-governance environments [5],[8]. The principal contributions and associated limitations of studies related to this research area are illustrated in Table 8 below. Despite the contributions made by such studies, however, several critical gaps still exist, especially concerning the connection between CSMP and IDPP in government organizations [8]. Such gaps include the absence of empirical studies validating hybrid cost-effective solutions, the lack of studies analyzing long-term sustainability, and the lack of country-specific research conducted in developing countries such as Zambia [4],[12].

In addition, one may observe that while separate cybersecurity tools have been described in detail in previous works [23]-[33], few efforts have been devoted to researching the process of implementing such components into an integrated monitoring system. Challenges related to log correlation, interoperability, and alert tuning have not been analyzed properly, thus hampering the organization's ability to move from an ad-hoc security system to a coordinated, centralized monitoring environment.

This challenge is especially pronounced in the case of public sector organizations that face certain budget constraints [7]. While open-source software offers a good solution to proprietary products, its efficient implementation remains to be researched [21].

Table 8: Summary of related works in CSMP-IDPP literature

Study Focus	Key Contribution	Identified Gap	References
Government cybersecurity frameworks	Established best practices for risk management and governance	Limited focus on developing-country implementation	NIST (2018); Culot et al. (2021)
Open-source security tools	Cost-effective security monitoring solutions	Limited large-scale validation	Dixit and Tripathi (2025); Guo et al. (2022)
Proprietary SIEM solutions	Advanced event correlation and analytics	High implementation and operational costs	Pekarčík et al. (2025)
African case studies	Contextual relevance to developing countries	Limited empirical validation	El Gohary (2017); Egwuatu (2025)

Governance and policy studies	Legal and compliance perspectives	Weak linkage to technical implementation	Anil and Babatope (2024)

Despite the availability of a variety of security solutions, analysts have a hard time monitoring multiple dashboards simultaneously and correlating events from different security devices. Moreover, these devices generate a huge amount of data (logs) in multiple formats, thus overwhelming the log management. This issue is particularly important for SMEs that usually have limited human resources, and managing security can often be a part-time job for a single individual [38]. Table 9 provides a summary of the identified knowledge Gaps in the literature.

Table 9: Summary of Identified Knowledge Gaps in Literature.

Gap Category	Description	Research Impact	References
Integration Gap	Limited SIEM integration across security platforms	Restricts centralized monitoring capabilities	Pekarčík et al. (2025); Dixit and Tripathi (2025)
Validation Gap	Limited empirical validation in African e-governance contexts	Weak evidence base for implementation	El Gohary (2017); Egwuatu (2025)
Sustainability Gap	Limited cost-benefit and long-term sustainability analysis	Difficulties in supporting adoption	Culot et al. (2021)
Governance Gap	Weak alignment between compliance and technical design	Reduces institutional trust and coordination	Vielberth et al. (2020)
Human Capacity Gap	Limited cybersecurity and SOC operational skills	Restricts scalability and operational maturity	Hamid and Huda (2025)

The literature review further shows that despite advancements in the deployment of CSMP-IDPS worldwide, there is still a gap in effective, feasible, and economically viable solutions that are focused on developing countries, as well as public institutions [39]. Few studies have been found to have proven their designs using hybrid open-source and proprietary cybersecurity models in Zambia.

7 Conclusion

In conclusion, the cybersecurity challenges faced by e-governance systems and wider e-governance systems involve a range of issues, including fragmented security infrastructure, lack of skilled manpower, funding issues, and reactive cybersecurity management approaches. Although existing frameworks like Defence in Depth, NIST CSF, ISO/IEC 27001, and Zero Trust offer useful guidance on cybersecurity management, they fall short in terms of the need for integrated monitoring and responses to cybersecurity threats, particularly in the public sector context.

The reviewed literature provides a rationale for adopting a framework involving the integration of the Centralized Security Monitoring Platform (CSMP) and Intrusion Detection and Prevention Platform (IDPP). This combination of tools leads to improved cybersecurity management.

On the other hand, research limitations still exist in areas such as practicality, scalability, and sustainability of hybrid CSMP–IDPP in the context of developing countries. The issue requires further study through research into effective methods of implementing such an approach to cybersecurity.

References:

[1] G. Wirata, M. S. Gunawan, L. Judijanto, A. D. A. Sarmento, and A. R. Permono, "The Role of E-Government Innovation in Enhancing Public Service Performance and Strengthening Transparent Governance," *International Journal of Accounting and Economics Studies*, vol. 12, no. 6, pp. 710–717, Sep. 2025, doi: 10.14419/ZXPZP606.

[2] Satyarth Dwivedi, "All Types of E Governance Models: G2C, G2B, G2G, G2E Explained." Accessed: Jul. 22, 2025. [Online].

Available: https://plutuseducation.com/blog/types-of-e-governance/

[3] I. A. Shah, R. A. A. Habeeb, S. Rajper, and A. Laraib, "The Influence of Cybersecurity Attacks on E-Governance," pp. 77–95, Apr. 2022, doi: 10.4018/978-1-7998-9624-1.CH005.

[4] E. M. El gohary, "E-government Implementation in Developing Countries: A Literature Review," *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, vol. 16, no. 1, pp. 7510–7524, Mar. 2017, doi: 10.24297/IJCT.V16I1.8371.

[5] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics 2023, Vol. 12, Page 1333*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/ELECTRONICS12061333.

[6] S. Hamid and M. N. Huda, "Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023," *Social Sciences and Humanities Open*, vol. 11, Jan. 2025, doi: 10.1016/j.ssaho.2024.101234.

[7] E. S. M. Kala and E. S. M. Kala, "Challenges of Technology in African Countries: A Case Study of Zambia," *Open Journal of Safety Science and Technology*, vol. 13, no. 4, pp. 202–230, Dec. 2023, doi: 10.4236/OJSST.2023.134011.

[8] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[9] A. Nuraeni, Y. Nugraha, and M. E. Aminanto, "Revisiting Cyber Threats in Government Sectors: A Systematic Review of Attacks, Challenges, and Policy-Level Defenses," *International Journal of Advances in Data and Information Systems*, vol. 6, no. 2, pp. 447–459, Aug. 2025, doi: 10.59395/IJADIS.V6I2.1404.

[10] S. K. Khan, N. Shiwakoti, A. Diro, A. Molla, I. Gondal, and M. Warren, "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100724, Dec. 2024, doi: 10.1016/J.IJCIP.2024.100724.

[11] Srikanth Bellamkonda, "(PDF) Network Device Monitoring and Incident Management Platform: A Scalable Framework for Real-Time Infrastructure Intelligence and Automated Remediation." Accessed: May 22, 2026. [Online]. Available: https://www.researchgate.net/publication/391836537_Network_Device_Monitoring_and_Incident_Management_Platform_A_Scalable_Framework_for_Real-Time_Infrastructure_Intelligence_and_Automated_Remediation

[12] "Protecting Outdated and Unsupported Systems - Nextron Systems." Accessed: Apr. 30, 2026. [Online]. Available: https://www.nextron-systems.com/2025/03/25/protecting-outdated-and-unsupported-systems/

[13] Anna Rebeiro, "OT cybersecurity reporting remains a structural weakness as threats outpace legacy governance models - Industrial Cyber." Accessed: Oct. 05, 2025. [Online]. Available: https://industrialcyber.co/features/ot-cybersecurity-reporting-remains-a-structural-weakness-as-threats-outpace-legacy-governance-models/

[14] Vishal Kumar Seshagirirao Anil and Adeoluwa Bennard Babatope, "The role of data governance in enhancing cybersecurity resilience for global enterprises," *World Journal of Advanced Research and Reviews*, vol. 24, no. 1, pp. 1420–1432, Oct. 2024, doi: 10.30574/WJARR.2024.24.1.3171.

[15] Supriya Dhananjay Paigude, "A Review of Cybersecurity Policies in the Public Sector: Challenges and Solutions," *Computer Fraud and Security*, pp. 07–12, Nov. 2024, doi: 10.52710/CFS.28.

[16] C. Simfukwe and A. P. Shemi, *Advancing Cybersecurity Measures to Safeguard Critical Infrastructure and Data: Is Zambia Ready?*

[17] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Apr. 2018, doi: 10.6028/NIST.CSWP.04162018.

[18] J. A. Lewis, "CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION," *Homeland Security: Protecting America's Targets: Volume 1-3*, vol. 1–3, pp. 324–338, Jan. 2006, doi: 10.1016/B978-0-12-817137-0.00008-0.

[19] H. A. Salman and A. Alsajri, "The Evolution of Cybersecurity Threats and Strategies for Effective Protection. A review," *SHIFRA*, vol. 2023, pp. 73–85, Aug. 2023, doi: 10.70470/SHIFRA/2023/009.

[20] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Jul. 2021, doi: 10.1108/TQM-09-2020-0202.

[21] Bipin Gajbhiye, Shalu Jain, and Om Goel, "Defense in Depth Strategies for Zero Trust Security Models," *Darpan International Research Analysis*, vol. 11, no. 1, pp. 27–39, Dec. 2023, doi: 10.36676/dira.v11.i1.70.

[22] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[23] P. Pekarčík, E. Chovancová, M. Chovanec, and M. Štancel, "A Centralized Approach to Intrusion Detection System Management: Design, Implementation and Evaluation," *Acta Polytechnica Hungarica*, vol. 22, no. 1, pp. 2025–2032.

[24] K. Kent and M. Souppaya, "Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology."

[25] NIST Information, "SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) | CSRC." Accessed: Jun. 02, 2025. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/94/final

[26] Vasudev Karthik Ravindran, Sharad Shyam Ojha, and Arvind Kamboj, "A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems," *International Journal of Latest Technology in Engineering Management & Applied Science*, vol. 14, no. 5, pp. 209–214, Jun. 2025, doi: 10.51583/IJLTEMAS.2025.140500026.

[27] K. Scarfone and P. Mell, "Intrusion Detection and Prevention Systems," 2010.

[28] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[29] P. Senthilkumar and M. Muthukumar, "A study on firewall system, scheduling and routing using pfsense scheme," *Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018*, pp. 14–17, Dec. 2018, doi: 10.1109/I2C2SW45816.2018.8997167.

[30] Medium, "PFSense: Comprehensive Guide to Installation, Configuration, and SYN Flood Attack log Analysis: pfSense-CE-2.6.0-RELEASE-amd64.iso | by IritT | Medium." Accessed: Jan. 19, 2026. [Online]. Available:

https://iritt.medium.com/pfsense-comprehensive-guide-to-installation-configuration-and-syn-flood-attack-analysis-441a5419f467

[31] Suricata, "23.1. IPS Concept — Suricata 9.0.0-dev documentation." Accessed: Jan. 19, 2026. [Online]. Available: https://docs.suricata.io/en/latest/ips/ips-concept.html

[32] S. Dixit and P. Tripathi, "Strengthening Cybersecurity with Wazuh: Log-Based Threat Detection for a Resilient Digital World," *International Journal of Advanced Research in Computer and Communication Engineering Impact Factor*, vol. 8, no. 1, 2025, doi: 10.17148/IJARCCE.2025.14162.

[33] "Log data collection - Capabilities · Wazuh documentation." Accessed: Jan. 19, 2026. [Online]. Available: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/index.html

[34] A. Caballero, "Information security essentials for IT managers: Protecting mission-critical systems," *Managing Information Security, 2nd Edition*, pp. 1–45, Jan. 2013, doi: 10.1016/B978-0-12-416688-2.00001-5.

[35] S. E. Sadat, M. F. Naseri, and K. Salamzada, "Identifying and Mitigating Web Application Vulnerabilities: A Comparative Study of Countermeasures and Tools," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 4, no. 3, pp. 1109–1127, Dec. 2024, doi: 10.35870/IJSECS.V4I3.3138.

[36] "(PDF) Advanced Persistent Threats (APTs): Detection Strategies and Mitigation Techniques." Accessed: May 24, 2026. [Online]. Available: https://www.researchgate.net/publication/385292498_Advanced_Persistent_Threats_APTs_Detection_Strategies_and_Mitigation_Techniques

[37] S. R, A. Taranum, Karthik, and M. U. Hussain, "Endpoint Security Agent: A Comprehensive Approach to Real-Time System Monitoring and Threat Detection," pp. 1–6, Dec. 2025, doi: 10.1109/CSITSS67709.2025.11295748.

[38] F. Mijnhardt, T. Baars, and M. Spruit, "Organizational characteristics influencing sme information security maturity," *Journal of Computer Information Systems*, vol. 56, no. 2, pp. 106–115, 2016, doi: 10.1080/08874417.2016.1117369.

[39] O. V. Egwuatu, "Cybersecurity Readiness in Developing Countries' Enterprises: A Comparative Multi-Case Analysis," *Magna Scientia Advanced Research and Reviews*, vol. 15, no. 1, pp. 068–083, Sep. 2025, doi: 10.30574/MSARR.2025.15.1.0110.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Steve Muwowo carried out a literature review and was responsible for editing.

Lukumba Phiri was responsible for supervision, guidance, and proofreading.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.