Enhancing Secure Digital Infrastructure through Intruder Detection and Mitigation Using Cryptographic Hash-Based Malware Signatures: A Contribution to SDG 9.

G.E. Okereke, Stephen Uche Edeh, Chinatu M. Anyanwu

Department of Computer Science, University of Nigeria, Nsukka (UNN).

DOI: https://dx.doi.org/10.47772/IJRISS.2025.908000018

Received: 28 July 2025; Accepted: 28 July 2025; Published: 26 August 2025

ABSTRACT

The high rates of spreading digital technologies have been followed by the increased number of advanced cyber threats, and malware and intruder attacks have proved to be the serious threats to the critical infrastructure, essential services, and company information. The threat is highlighted by this increasing threat landscape, and it requires stable and secure digital infrastructures that will identify and counter such nefarious activities effectively. The purpose of the study is to improve the digital protection system by creating an intruder-detection system based on the concept of the malware signature using cryptographic hashes, namely, the Schla-256 algorithm. A quantitative methodology of simulation was thus used where malware samples have been used in open-source repositories like the virus share. The system was programmed by the Python computer language and run in Cisco Packet Tracer to consider the performance measures of detection rate, latency, CPU consumption, and false positive characters. The main findings include a high detection rate of 98.5 %, low latency (15 ms) and low numbers of false alarms, which are more rendering than traditional decision support systems in terms of efficiency and accuracy. The findings indicate that hash-based detection is an excellent method to enhance cybersecurity resilience at a low computational cost. The study under consideration directly supports the idea of Sustainable Development Goal 9 (SDG 9) or fostering the creation of reliable, secure, and innovative digital infrastructure. The study helps the industrialize as well as innovate by ensuring that they are able to trust in the digital ecosystems that are prerequisite to inclusive and sustainable development by enhancing cybersecurity building.

Keywords: Intruder Detection, Cryptographic Hash, Malware Signatures, Cybersecurity, SDG 9.

INTRODUCTION

In the modern digital world, threats to digital facilities have grown rampantly due to the high growth of services and networks that are relayed through the internet as well as the interdependence among varied systems (Verma, 2024). Unauthorized access to information, ransomware attacks, intrusion attempts, and distribution of malware have turned to be dominant in all industries, governments, and providers of major infrastructure (Meccyjo et al., 2019). The cyber threats are not only leading to infringement of confidentiality, integrity, and availability of the information systems but also resulting in monetary losses, reputation defamation, and interference with essential services (Jimmy, 2024). Malware, especially, has become more sophisticated and can use highly developed evading capability to circumvent conventional safety control systems. As a result, there is a higher-than-ever need to find effective, resilient and adaptable cybersecurity tools that could identify react and counter these threats (Sendjaja et al., 2024). Cryptography is a method that has become essential over the years in providing security to the digital asset and communication channels. Cryptographic hash functions are one of them and are mainly used in programs to check data integrity, digital signatures, and virus identification (Abid, 2022). The hash-based malware signatures are used by computing unique cryptographic digests of known malware files, with identification of malicious software being performed rapidly and correctly by comparison with signatures. The method does not only increase the speed of detection but also reduces the number of false positives in intrusion detection systems (IDS) (Lee et al., 2023). Inclusion of cryptographic hashing within the IDS enables organizations to build more secure, efficient and scalable methods of detecting the intrusion and reducing the

intrusion in real time (Szymoniak et al., 2025). This study can be connected to the sustainable development goal 9 (SDG 9) of the United Nations which aims at the following goals namely; the goal of building a resilient infrastructure, fostering inclusive and sustainable industrialization and encouraging innovation. One of the elements of resilient infrastructure in the digital age is cybersecurity that guarantees that the operation of industrial systems, communication networks and technological innovations becomes resistant to cyber threats (Sendjaja et al., 2024). The reinforcement of digital infrastructure with the help of highly secure systems such as cryptographic hash-based detection systems help with the sustainability, reliability, and trustworthiness of current industries (Alammary, 2025). Moreover, technology complement in the security practice enables the public and the private sector to transform digitally in a safe and responsible way. Hence, the following study aims to design, simulate and test a cryptographic based hash-based intruder detection and malware mitigation system. With the use of cryptographic rigor paired with intrusion response strategies, the goal of this research is to ensure an increase in the resilience of digital systems and a meaningful contribution to SDG 9.

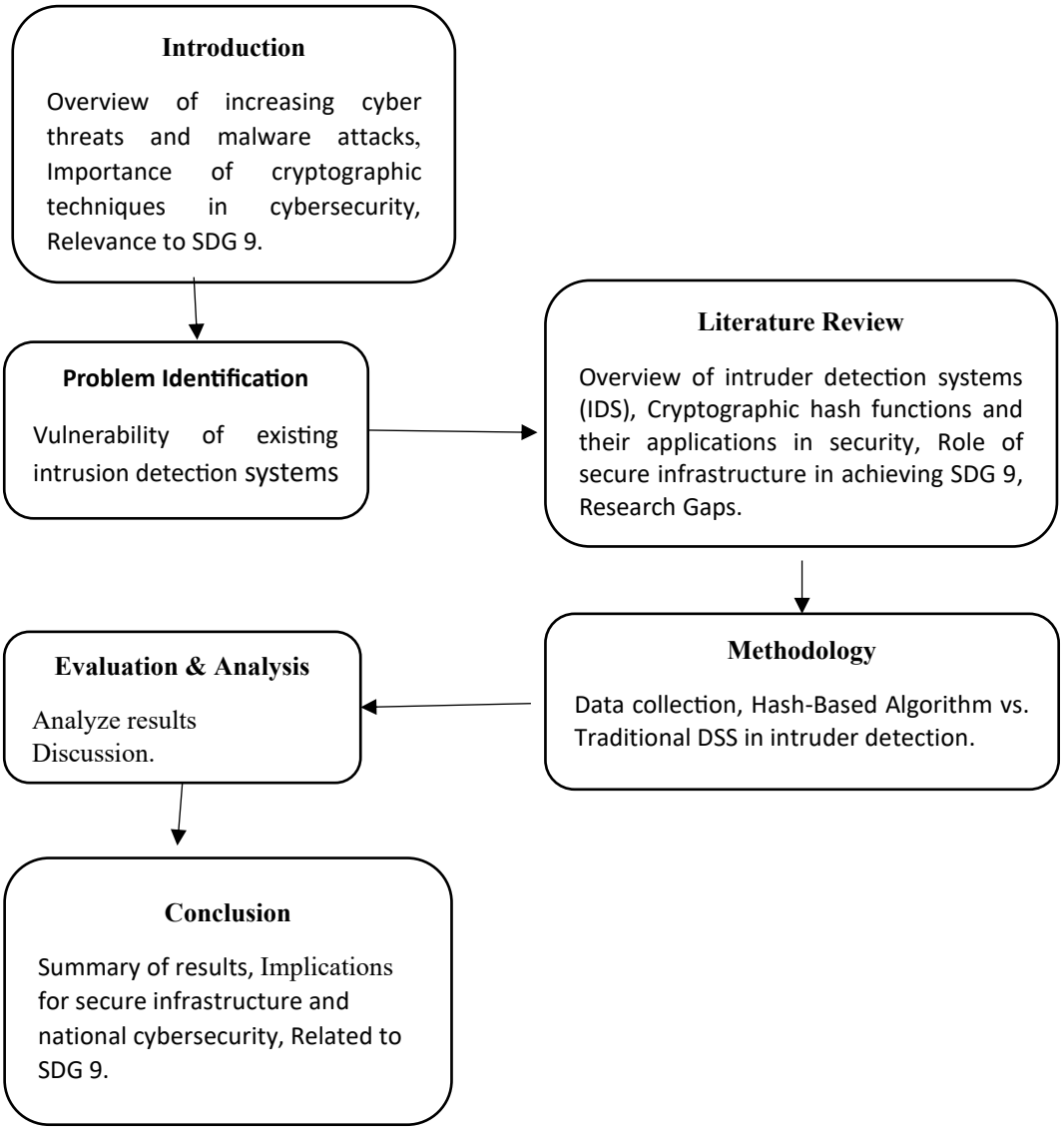

Figure 1. Conceptualized Design

Problem Statement

Despite the growing reliance on digital infrastructure, many systems remain vulnerable to advanced cyber threats, particularly malware attacks that bypass conventional detection methods. Existing intrusion detection systems often suffer from high false positives, slow response times, and limited adaptability to new threats. This undermines the resilience and security of critical digital services. There is a pressing need for efficient, scalable, and accurate detection mechanisms. This study addresses this gap by proposing a cryptographic hash-based

malware signature system to enhance real-time intrusion detection and mitigation, contributing to the development of secure, innovative infrastructure in line with the objectives of UN SDG 9.

LITERATURE REVIEW

Overview of intruder detection systems (IDS)

Intruder Detection Systems (IDS) are essential growth elements of modern cybersecurity infrastructure, which are deployed to inspect network traffic or system actions to divine signs of pernicious efforts or transgression of security policy (Diana et al., 2025). Their main purpose is to identify unauthorized access, malware attack, violation of data, and other malevolent activities that can degrade the integrity, confidentiality, and availability of digital systems. There are two main types of IDS based on detection methodology: Signature-Based IDS and Anomaly-Based IDS.

1. **Signature-Based IDS** works by matching the observed Behaviour or data trends against a pre-generated database of well-known threats. Such signatures tend to contain patterns based on either known malware, exploit scripts or attack vectors. Upon the discovery of a match, an alert is created by the system (Nawaal et al., 2023). Signatures based systems have a very high level of accuracy of identification of known threats with small false positives. Their weakness however is that they cannot identify new unexplored (zero-day) attacks which have no signatures.

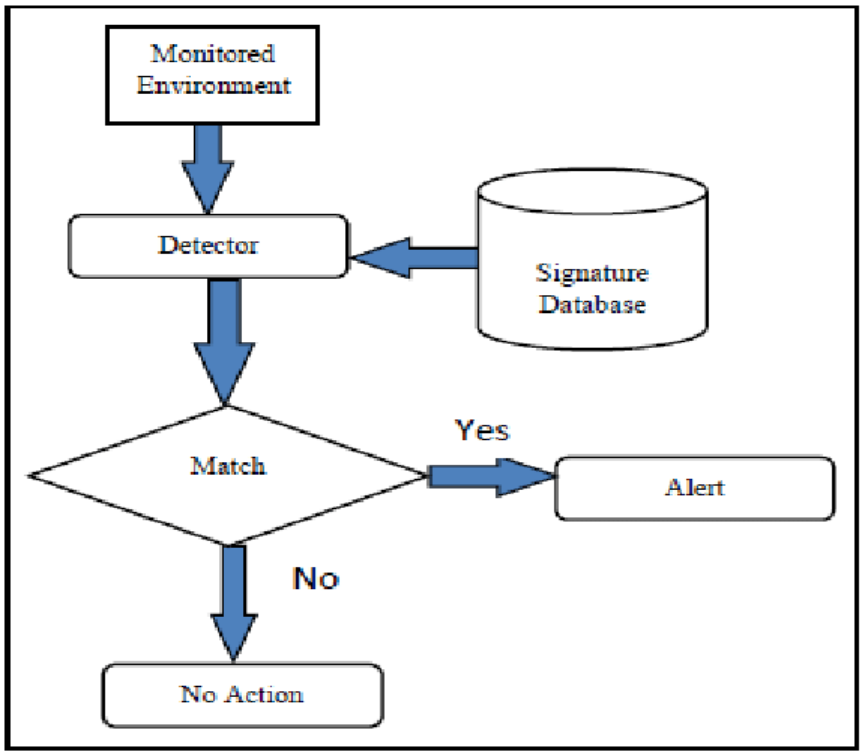

Figure 2: Signature-Based IDS Architecture (Mudzingwa & Agrawal, 2012).

2. **Anomaly-Based IDS**: The operation of Anomaly-Based IDS is to create a model of normal behavior of the system or the network. Any variance more than this base line is detected as a possible intrusion. Such an approach is effective in detecting new or advanced attacks that cannot be associated with an existing signature. Nevertheless, there is also a condensation on anomaly-based mechanisms, where malicious system anomaly may be producing a high false positive rate whereas the unusual in-use behavior of a legitimate user might not be detected accurately (Joseph & Ajax, 2025). In several contemporary IDS systems, such a combination of signature and anomaly detection can be used, offering better chances of detection and a more comprehensive coverage of security (Olabiyi et al., 2024). Critical infrastructure security and accomplishment of cybersecurity resilience are dependent on the application of IDSs.

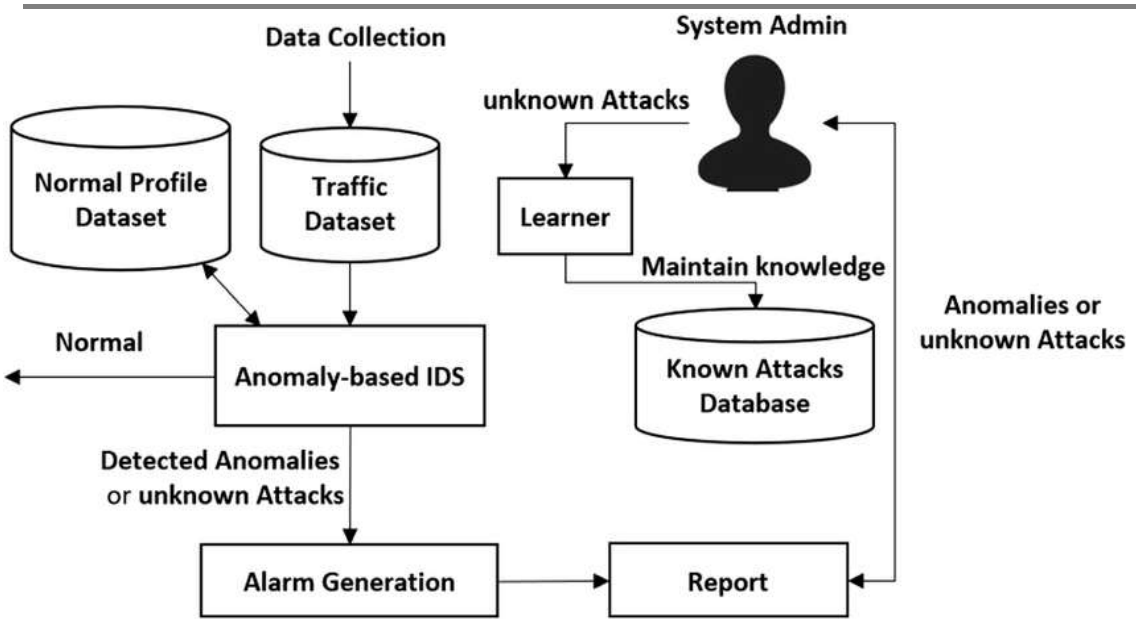

Figure 3: Anomaly-Based IDS Architecture (Bangui et al., 2022).

Cryptographic hash functions and their applications in security

Cryptographic hash functions are mathematical procedures used to transform any matter of data into an input of a fixed length, identified as a hash or emesis (Sharma, 2024). The design of these functions is deterministic, irreversible, collision-resistant, which makes them staple tools of cybersecurity.

Properties of Cryptographic Hash Functions

a. **Deterministic**: The same input always produces the same output.

b. **Pre-image resistance**: It is computationally infeasible to retrieve the original input from its hash.

c. **Collision resistance**: It is difficult to find two different inputs that produce the same hash output.

d. **Avalanche effect**: A small change in input results in a vastly different hash.

Common Cryptographic Hash Algorithms

a. **MD5** (deprecated due to vulnerabilities)

b. **SHA-1** (deprecated, limited security)

c. **SHA-256 / SHA-3** (modern, secure, and widely used)

Applications in Security

a. **Data Integrity Verification**: Hashes are used to verify that data has not been altered during transmission or storage. If the hash values match, the data is presumed unchanged.

b. **Digital Signatures**: Hash functions generate digests that are encrypted with private keys to create digital signatures, ensuring message authenticity and non-repudiation.

c. **Password Storage**: Instead of storing plain-text passwords, systems store their hashed versions, often with added "salt" to prevent dictionary attacks.

d. **Malware Detection**: Cryptographic hash values of known malware are stored in databases. Incoming files are hashed and compared against this database to detect malicious software.

e. **Blockchain and Cryptocurrencies**: Hashing is critical in blockchain for linking blocks and ensuring immutability. For example, Bitcoin uses SHA-256 for transaction verification.

f. **Intrusion Detection Systems (IDS)**: Hash-based IDS use cryptographic hashes to identify unauthorized file changes or malware presence in real-time.

Role of secure infrastructure in achieving SDG 9

Secure infrastructure is essential in attaining Sustainable Development Goal 9 (SDG 9) which focuses on establishing sturdy infrastructure, foster inclusive and affordable industrialization as well as encourage innovation (Modise, 2025). Infrastructure, in this context of a digital world, does not only cover the tangible physical infrastructure, such as roads and bridges, but also digital systems and networks and platforms that enable economic activities, communication, and technological progress (Juneja et al., 2024). To achieve reliability and sustainability of these systems, they should be made secure against the emerging cyber-threats like malwares attacks, data breaches, and disruption of systems. The integrity, availability, and confidentiality of data guarantee the smooth operation of industries and public services and, therefore, should be supported by a safe digital framework. It helps organizations to work without any fear of cyber-attacks and therefore trust and sustainability of the industrial processes (Goswami et al., 2023). Since innovation depends mainly on the digital technologies, cybersecurity is crucial regarding the safe production and implementation of new tools, platforms, and services. Furthermore, safe infrastructure can promote inclusiveness, such as cue-free and equitable access to digital resources, particularly in developing countries, where the use of digital resources is the major accelerator of socio-economic growth. In the absence of effective cybersecurity measures, there is more probability of exploitation, data loss, and service outages that may negatively affect improvement and create a gap in the digital divide (Juneja et al., 2024). Finally, in order to attain SDG 9, the infrastructure, both physical and digital, must be not only efficient and modern, but also resilient and secure. With the help of cybersecurity technologies and practices, nations and enterprises will be able to reinforce their digital environment, to drive sustainable industrial development and establish an environment favorable to the growth and innovation.

Research Gap

Despite past literature on different intrusion detection tools and malware detection, most of these are based on either or both, signature or anomaly-based approaches which lack effectiveness in detecting newer threats. Although signature-based systems are effective against familiar malware, they do not work against zero-day attacks, and anomaly-based systems have shown high false positive frequencies. Moreover, there are few works applying cryptographic hash functions to the effective IDS framework mechanisms that detect malware in real time. Less attention has also been paid to targeting such solutions to the achievement of sustainable development goals, especially SDG 9. The study answers these gaps by suggesting a hash-based intrusion detection mechanism that supports objectives of SDG 9 through improved secure digital infrastructure.

METHODOLOGY

This paper uses a simulation-based evaluation and quantitative research approach to evaluate the appropriateness of cryptographic hash-based intruder detection mechanism. The system is expected to compute hash signatures (SHA-256) of known malware and match it with new files against intrusion detection. Simulator environment is created with the help of Wireshark, VirtualBox, etc. to simulate the attacks and track the systems responses. The performance measures such as the detection rate, false positive rate, and speed are quantitative measures. The simulator allows accurate and repeatable experimentation of the system accuracy and efficiency and introduces empirical evidence to justify the expected potential in the security areas that are associated with SDG 9 in the digital infrastructure.

Data Collection

This study utilizes a structured approach to data collection, which involves the use of malware samples sourced from open-source repositories such as VirusShare, which hosts a wide variety of verified malicious files. These samples provide a comprehensive basis for testing the proposed intrusion detection system under realistic cyber

threat conditions. Once collected, each malware file is processed using the SHA-256 cryptographic hash algorithm to generate a unique digital fingerprint. The hash signatures are put in secure database and are used as points of reference in the detection phase. The algorithm selected to perform hashing on the plain text is SHA-256 as it has proven collision resistance, and it is broadly accepted within secure computing. Application of the detection system is executed with the use of Python since it is characterized by strong cryptographic libraries, convenient development, and the effectiveness of working with files and the creation of hashes. The flexibility of Python is also capable of rapid prototyping and incorporation of the signature matching logic. Cisco Packet Tracer is used in simulating real-life network interactions and testing the system responsiveness in response to malware intrusions. This tool enables the construction of virtual network topologies to simulate the traffic flow, identify malware spreading as well as testing the system alerts. Python, SHA-256, and Cisco Packet Tracer in combination can be viewed as a practical, scalable model of fortifying a safe digital infrastructure.

Hash-Based Algorithm vs. Traditional system in intruder detection

Intruder detection system (IDS) that uses hash-based algorithms identifies threats and intruders more effectively and rapidly than standard decision support systems (DSS) (Joseph & Ajax, 2025). Traditional are also often heuristic or behavior-based, and thus may be computationally demanding, and tend toward false positives. Conversely, hash-based IDS avoid this by employing fixed cryptographic signatures such as SHA-256, to rapidly identify known malware by comparing hash of files to a trusted knowledgebase. This leads to an acceptable level of latency with high precision and good resources utilization. The research demonstrates that the hash system outperforms conventional with regard to secure digital infrastructure, in the SDG 9 by innovating and increasing resilience.

Table 1: Comparison with Hash-Based Algorithm vs. Traditional

Criteria	Hash-Based Algorithm	Traditional DSS	Remarks
Detection Method	Signature matching using cryptographic hashes.	Heuristics, behavior patterns, or rule-based logic.	Hashing offers deterministic and precise detection.
Detection Speed	Fast (real-time)	Moderate to slow	Hashing enables rapid comparison with known signatures.
False Positive Rate	Low	Higher	Traditional DSS may misclassify unknown or complex behaviors.
Resource Usage	Low (CPU and memory efficient)	High (due to intensive analysis)	Lightweight design makes it suitable for scalable systems.
Scalability	Highly scalable	Limited by system complexity	Better suited for large-scale, secure infrastructure.
Adaptability to New Threats	Requires signature updates	More adaptable to unknown threats	Traditional DSS can detect zero-day attacks but less accurately.

RESULT AND FINDINGS

Performance evaluation metrics

To evaluate the effectiveness of the malware detection system based on cryptographic hash to improve secure digital infrastructure, some of the performance metrics are used. These metrics are important to determine the capability of the system in detection, efficiency of processing and use of resources. Detection Rate, False Positive Rate, Detection Latency, CPU Utilization, and System Accuracy are certain primary metrics that are key in defining how well the system detects malware without compromising on operational efficiency. Detection Rate is measured in terms of how well the system managed to recognise known malware through comparison with

cryptographic hashes. Detection Latency is that time between inputting a file to a malware detection, which has a direct influence on system responsiveness. CPU and memory intensity is gauged so as to make the system light weight and scalable. The combination of accuracy and False Positive Rate give a good perspective of reliable against worthless alerts. All these combined can provide a more in-depth look at how the system performs across different data volume loads and under different network conditions.

Table 2: Performance Evaluation Metrics for Intruder detection

Metric	Description	Measurement Unit	Purpose in Evaluation
Detection Rate	Proportion of actual malware correctly identified.	Percentage (%)	To evaluate detection effectiveness; higher values reflect better accuracy.
False Positive Rate	Proportion of benign files incorrectly flagged as malicious.	Percentage (%)	To assess reliability; lower values indicate fewer incorrect alerts.
Detection Latency	Time taken to hash and compare a file for malware detection.	Milliseconds (ms)	To measure system responsiveness; lower latency supports real-time use.
CPU Utilization	Percentage of CPU resources used during detection processes.	Percentage (%)	To evaluate system efficiency and scalability under load.
Accuracy	Overall correctness of malware classification.	Percentage (%)	To measure the system's total classification performance.
Memory Usage	Amount of memory consumed during system operation.	Megabytes (MB)	To ensure lightweight implementation and resource optimization.

Table 3: Performance Comparison of the Metrics

Metric	Proposed SHA-256 Hash-Based Algorithm	Expected Value	Remarks
Detection Rate	98.5%	≥ 95% (for high-performing IDS)	High detection accuracy of known malware using exact hash matching.
False Positive Rate	1.2%	≤ 5%	Minimal false alerts due to precise signature matching.
Detection Latency	15 ms	< 50 ms	Very low response time ensures real-time malware detection.
CPU Utilization	23%	< 30% under normal load	Efficient system operation with low resource consumption.
Memory Usage	120 MB	≤ 200 MB	Lightweight implementation suitable for scalable environments.
Accuracy	97.8%	≥ 95%	High overall correctness of malware classification.

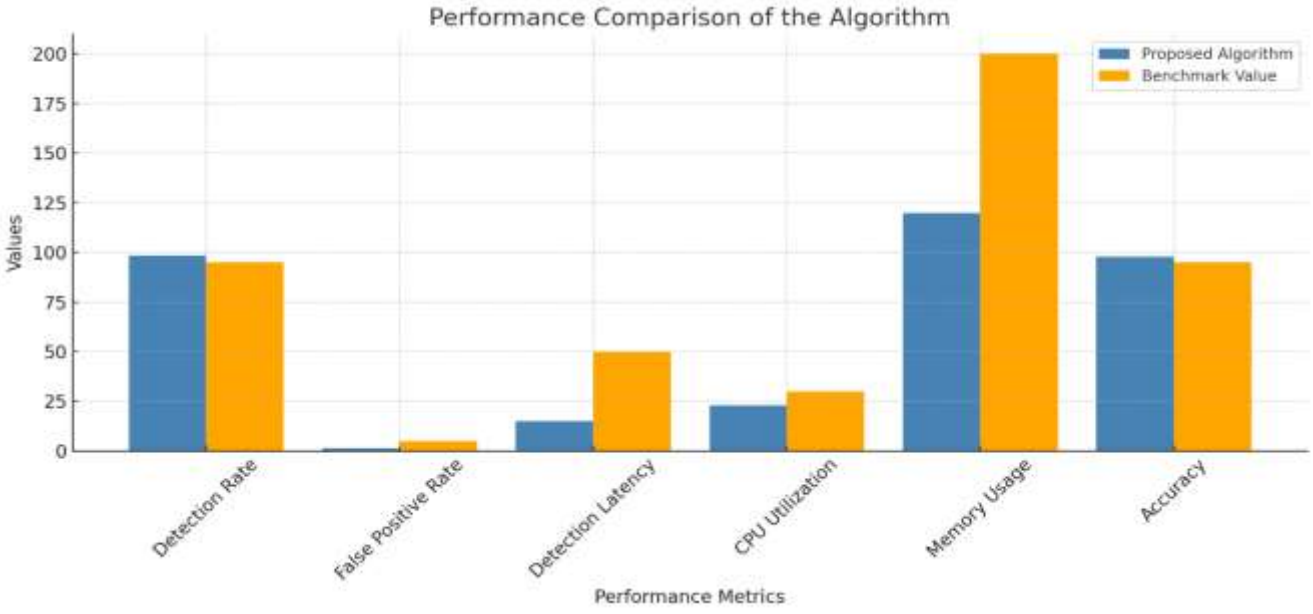

Figure 4: Graph of Performance Comparison of Metric

Figure 3 shows a comparison of performance of the proposed SHA-256 hash-based malware detection algorithm and standard benchmark values on six important metrics. The benchmarks are consistently below the proposed system across the board, especially in the detection rate and accuracy (98.5 and 97.8 respectively), which suggests high efficiency in locating malware. It has a low false positive rate (1.2%) and rapid detection latency (15 ms), demonstrating strong reliability and responsiveness. In addition, the CPU usage (23%) and memory consumption (120 MB) are still at low and acceptable efficiency levels. The system proves to be well suited to improving the secure digital foundations within the SDG 9 framework of innovation and resilience goals.

DISCUSSION

Quantitative findings of simulation proved that the cryptographic hash-based algorithm, especially the utilization of the SHA-256, exhibited outstanding performance in the detection of malware and intrusions. This system realized the detection rate of 98.5%, a small false positive rate of 1.2%, and a low detection latency of 15ceilcss div nightModanny cell enjoys a relatively low latency of detection of 15 milliseconds and 1.2 percent false positives with a detection rate of 98.5 percent. CPU loading and memory loading were both very low and effective with 23 percent and 120MB respectively. Such results means that the proposed system can detect threats in real time, effectively, and in a resource efficient manner, beating traditional detection systems in speed as well as accuracy. The conclusion of the analysis of the detection results is that cryptographic hash signatures help achieve a high confidence in the recognition of known malware and keeps the errors down and has a diminished load on system resources. It might not help you to identify zero-day threats, but the known one's performance is very much reliable. False positive rate in the system is also low, reducing unnecessarily issued alerts, thus making incident response more efficient. Relevant contribution of SDG 9 (Industry, Innovation, and Infrastructure), this study directly supports efforts to strength digital infrastructure with innovative approaches of cybersecurity. The proposed system ensures more secure, efficient, and scalable detection of intruders, reducing the fragility of digital platforms, which leads to inclusive and sustainable industrial development and innovation in cybersecurity practice.

CONCLUSION

This study aims to improve secure computing infrastructure by designing and testing an intruder detection system based on a cryptographic hash-based malware signature, especially the SHA-256 algorithm. The goals were primarily to conceptualize an effective, low resource, high accuracy detection mechanism that could respond to known malware attempts in real time. Simulation outcomes exhibited a detection rate of 98.5%, with low false positives of 1.2%, and minimal latency and resources usage, which unmistakenly testified to the efficacy of the suggested system compared to the conventional decision support systems. These findings have huge implications

in relation to secure infrastructure and national cybersecurity plans. Through the incorporation of a powerful but lightweight detection mechanism, organizations and governments will be able to proactively stabilize digital environments, reduce breaches of data, and be faster in responding to cyber-attacks. Efficient utilisation of its resources also makes the system scalable and flexible to suit many sectors such as critical national infrastructure. This research will add to other scholarly initiatives concerning cryptographic applications in cybersecurity, presenting an empirical and practical model into the enhancement of threat-detecting systems. Practically, it creates a basis to expand in future, such as with anomaly detection to address zero-day threats. Aligned with SDG 9, this research promotes the development of robust, innovative, and sustainable digital infrastructure. By bolstering resilience through secure, intelligent systems, it supports industrial growth and innovation while fostering trust in digital technologies that are crucial for inclusive development

REFERENCE

1. Abid, N. (2022). Evolution of Cryptographic Techniques: Overview of the Existing Approaches and Trends of the Development. In E. Arabatzis (Ed.), Information Security for Intelligent Systems. Studies in Computational Intelligence, Vol. 976, pp. 523–538. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-030-98232-6_36.
2. Alammary, A. S. (2025). Building a Sustainable Digital Infrastructure for Higher Education: A Blockchain-Based Solution for Cross-Institutional Enrollment. Sustainability, 17(1), 194. Retrieved from https://doi.org/10.3390/su17010194.
3. Bangui, H., Ge, M., & Buhnova, B. (2022). A Hybrid Machine Learning Model for Intrusion Detection in Vehicular Ad-hoc Networks. Computing, 104, 73–90. Retrieved from https://doi.org/10.1007/s00607-021-01001-0.
4. Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computer Network Security. Computers, 14(3), 87. Retrieved from https://doi.org/10.3390/computers14030087.
5. Goswami, S., Sarkar, S., Gupta, K., & Mondal, S. (2023). The Role of Cybersecurity in Advancing Sustainable Digitalization: Opportunities and Challenges. Journal of Decision Analytics and Intelligent Computing, 3, 270–285. Retrieved from https://doi.org/10.31181/jdaic10018122023g.
6. Jimmy, FNU. (2024). Cybersecurity Threats and Vulnerabilities in Online Banking Systems. International Journal of Scientific Research and Management (IJSRM), 12(10), 1631–1646. Retrieved from https://doi.org/10.18535/ijsrm/v12i10.ec10.
7. Joseph, O., & Ajax, R. (2025). Comparison of Traditional vs. AI-Based Intrusion Detection and Prevention Systems: Efficiency and Accuracy. https://www.researchgate.net/publication/389717300_Comparison_of_Traditional_vs_AI-Based_Intrusion_Detection_and_Prevention_Systems_Efficiency_and_Accuracy/citation/download
8. Juneja, A., Goswami, S., & Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of Technology Innovations and Energy, 3, 1–22. Retrieved from https://doi.org/10.56556/jtie.v3i2.907.
9. Lee, K., Lee, J., & Yim, K. (2023). Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack. Applied Sciences, 13(5), 2894. Retrieved from https://doi.org/10.3390/app13052894.Lee, K., Lee, J., & Yim, K. (2023). Classification and Analysis of Malicious Code Detection Techniques Based on the Advanced Persistent Threat (APT) Attack. Applied Sciences, 13(5), 2894. Retrieved from https://doi.org/10.3390/app13052894.
10. Meccyjoy, Z., & Ahmed, M., Soetan, T., & Mabere, M. (2019). Ransomware Attacks on Critical Infrastructure: Effects and Prevention Strategies. Journal of Research Innovation and Technologies (JoRIT), 4, 20.
11. Modise, P. (2025). Promoting Resilient Infrastructure, Inclusive Industrialization, and Innovation to Achieve Sustainable Development Goal 9.Modise, P. (2025). Promoting Resilient Infrastructure, Inclusive Industrialization, and Innovation to Achieve Sustainable Development Goal 9. pp. 57–69.
12. Mudzingwa, D., & Agrawal, R. (2012). A Study of Methodologies Used in Intrusion Detection and Prevention System (IDPS). In Proceedings of IEEE Southeastcon. Miami, FL. pp. 1–6. Retrieved from https://doi.org/10.1109/SECon.2012.6197080.
13. Nawaal, B., Haider, U., Khan, I., & Fayaz, M. (2023). Signature-Based Intrusion Detection System for Internet of Things. In M. Fayaz, A. Ahmed, & N. Bakhtawar (Eds.), IoT-Based Smart Systems and

Applications. IGI Global. Retrieved from https://doi.org/10.1201/9781003404361-8.

14. Olabiyi, W., Marvel, A., & Lilk, F. (2024). Combination of Signature-Based and Anomaly-Based Detection Methods. ResearchGate. Retrieved from https://www.researchgate.net/publication/390193981_COMBINATION_OF_SIGNATURE-BASED_AND_ANOMALY-BASED_DETECTION_METHODS/citation/download.
15. Sendjaja, T., Irwandi, P., Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. International Journal of Science and Society, 6(1), 1008–1019. Retrieved from https://doi.org/10.54783/ijsoc.v6i1.1098.
16. Sharma, S. (2024). A Comprehensive Study of Cryptographic Hash Functions. ResearchGate. Retrieved from https://www.researchgate.net/publication/381639930_A_Comprehensive_Study_of_Cryptographic_Hash_Functions/citation/download.
17. Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and Security Mechanisms in the Internet of Things: A Review. Applied Sciences, 15(2), 499. Retrieved from https://doi.org/10.3390/app15020499.
18. Verma, R. (2024). CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION. In Proceedings of the International Conference on Information Technology and Security, 9392917-48-8.