

# Dynamic monitoring for enhancing QoS and security in distributed systems

Sudhakar Periyasamy<sup>1</sup>, Vijayalakshmi Alagarsamy<sup>2</sup>, Palani Latha<sup>3</sup>, Karuppiah Tamilarasi<sup>3</sup>,  
Thenmozhi Elumalai<sup>3</sup>, Prabu Kaliyaperumal<sup>1</sup>

<sup>1</sup>School of Computer Science and Engineering, Galgotias University, Delhi NCR, India

<sup>2</sup>Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India

<sup>3</sup>Department of Information Technology, Panimalar Engineering College, Chennai, India

## Article Info

### Article history:

Received Dec 26, 2024

Revised Jul 3, 2025

Accepted Oct 7, 2025

### Keywords:

Adapting distributed system  
Adaptive monitoring system  
Adaptive security  
Cloud security  
Dynamic security

## ABSTRACT

Distributed systems are integral to modern digital infrastructure, supporting communication and data exchange across various sectors. Ensuring security while maintaining quality of service (QoS) in such environments presents a significant challenge. This study introduces a dynamic network monitoring system (DNMS) that incorporates adaptive monitoring mechanisms and dynamic security metrics to safeguard distributed systems. The proposed architecture utilizes an event analyzer (EA) to evaluate and classify system events based on criticality, enabling secure transmission decisions and efficient threat detection. Experimental evaluations demonstrate the DNMS achieves a low processing overhead of 12%, supports a high data handling capacity of 5,000 requests per second, and maintains a latency of just 150 milliseconds. Additionally, it ensures strong compliance with regulatory standards-achieving 95% alignment with GDPR and 97% with ISO 27001-and high threat detection accuracy, with 98% for phishing, 94% for malware, and 96% for insider threats. These results confirm the framework's effectiveness in enhancing adaptive security, offering scalable and regulation-compliant solutions for complex distributed environments.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Prabu Kaliyaperumal  
School of Computer Science and Engineering, Galgotias University  
201310 Delhi NCR, India  
Email: mega.prabu@gmail.com

## 1. INTRODUCTION

The increasing reliance on distributed systems in the modern information society underscores the need for effective monitoring approaches to offer adaptive security [1], [2]. These systems serve as the backbone of information exchange across various sectors, requiring robust security measures due to their complexity and dynamic nature. Adaptive security enables systems to adjust procedures dynamically in response to environmental changes, ensuring a balance between comprehensive data collection, integrity, and threat mitigation [3], [4]. This study explores the challenges of monitoring distributed systems for adaptive security, presenting a framework that integrates dynamic security metrics with adaptive monitoring to secure sensitive data in evolving environments. Distributed systems are vital in facilitating communication and information exchange across industries, leveraging decentralized processing and storage to handle vast data volumes [5]. Their scalability enhances operational efficiency, supports real-time collaboration, and drives innovation. Interconnected platforms integrate diverse applications, enabling seamless data exchange while ensuring critical services like cloud computing and e-commerce function efficiently [6], [7]. However, these systems face numerous challenges. Complexity arises from interconnected components,

diverse services, and evolving environments, demanding sophisticated monitoring and management. Heterogeneity introduces compatibility issues among various hardware and software [8], while scalability requires maintaining performance as systems expand [9]. Fault tolerance is crucial to counter hardware failures, network disruptions, and software errors. Ensuring data integrity and synchronization across nodes further adds to the complexity, necessitating effective protocols to address inconsistencies and maintain reliability. This study aims to answer the research question: “Can adaptive monitoring systems effectively enhance distributed system security while maintaining QoS through dynamic threat evaluation and selective data reporting?”.

Building on the theme of adaptive security, Tomashevsky *et al.* [10] introduces an adaptive resource allocation method for cloud environments to enhance both data processing and security. Using predictive algorithms and the NSGA-II optimization method, it forecasts resource demands and allocates resources dynamically. Improvements to NSGA-II reduce optimization time by 5%, achieving a 1.2x reduction in resource loss compared to traditional methods. While effective in balancing performance and confidentiality, limitations include computational overhead and dependency on accurate demand predictions. Similarly, Ahmad *et al.* [11] proposes an adaptive security framework for mobile devices, unifying autonomic computing and software security to protect hardware and software resources. The methodology employs runtime monitoring, threat detection, and dynamic security adjustments, with a focus on user decision support. Evaluated using ISO/IEC 9126 metrics, the framework achieved high accuracy (86.28% precision) in threat detection and efficient resource utilization with minimal battery (0.4%) and memory usage (20 MB max). Limitations include evaluation on Android-only platforms and limited datasets. Extending adaptive security measures to wireless sensor networks, Repetto [12] introduces a framework leveraging cyber-threat intelligence for adaptive monitoring, detection, and response in digital service chains. The framework employs security orchestration and automated response (SOAR) to combine workflows such as threat intelligence, incident response, and predictive analytics, effectively tackling multi-stage attacks. MIRANDA architecture facilitates proactive threat-hunting and adaptive responses, improving automation and defense against advanced persistent threats. Challenges include dependence on proprietary interfaces, limited adaptability to threats, and inadequate threat-hunting capabilities. In the context of internet of things (IoT) healthcare applications, Mohammed *et al.* [13] proposes the adaptive malware detection using machine learning (AMDML) algorithm for healthcare IoT applications, focusing on polymorphic and metamorphic malware threats. The methodology employs federated learning for distributed malware detection across fog nodes and the cloud, optimizing runtime adaptability and processing load. Results show AMDML outperforms centralized machine learning models by 60% in accuracy and reduces delay by 50%. Limitations include the high cost and complexity of detecting unknown malware without prior training. Hamarshah [1] introduces the enhanced SCAFFOLD framework, leveraging software-defined networking (SDN) and machine learning for IoT security. The methodology combines session key encryption, real-time traffic monitoring, and ensemble machine-learning classifiers (random forest (RF), support vector machine (SVM), recurrent neural network (RNN)) to detect attacks like distributed denial of service (DDoS) and spoofing. Performance simulations confirm reliable threat mitigation with low latency and minimal energy consumption. The framework ensures secure communication, rapid reauthentication, and targeted responses to anomalies. However, limitations include the complexity of integrating SDN with IoT devices and dependency on accurate machine-learning models for efficacy. Further addressing adaptive security, a study by Rashid *et al.* [14] proposes an adaptive, real-time malicious node detection framework for vehicular ad-hoc networks (VANETs) using machine learning. The proposed system utilizes distributed multi-layer classification, tested with OMNET++ and SUMO simulations, to detect DDoS attacks. Various classifiers, including gradient boosting tree (GBT), SVM, and RF, achieved up to 99% accuracy. However, limitations include challenges in real-time implementation and adaptability to diverse urban scenarios.

These studies collectively highlight the importance of adaptive security measures due to evolving threats and vulnerabilities in distributed systems. These systems require real-time identification and mitigation of risks, flexibility in access management, and automated incident response. Incorporating adaptive security ensures the protection of data, resources, and services [15], [16]. Additionally, dynamic monitoring frameworks are pivotal for maintaining the performance and security of distributed systems. Adaptive monitoring leverages intelligent algorithms and data analytics to identify anomalies, adjust priorities, and proactively mitigate threats [17]. By integrating seamlessly with existing protocols, these systems enhance resilience against evolving challenges, ensuring robust security postures and operational stability. The dynamic and interconnected nature of distributed systems necessitates advanced monitoring and adaptive security measures to address inherent challenges, ensuring data integrity, fault tolerance, and overall reliability. Through proactive strategies and intelligent frameworks, distributed systems can achieve secure and efficient operations in a rapidly evolving digital landscape.

Effective monitoring involves obtaining information from a target program during runtime to adapt a distributed system [18], [19]. The adaptation process includes change detection, agreement, and action, initiated by monitoring systems. Monitoring uses an event-driven execution paradigm, where clients detect changes and communicate event details for agreement. Monitoring nodes attach to address, data, and control buses to minimize disruption, identifying changes and notifying the central system for reconfiguration. The hybrid monitoring system uses memory-mapped and coprocessor monitoring [20]. Memory-mapped monitoring captures data when specific addresses are reached, while coprocessor monitoring initiates recording via instructions [21]. Key components include the event recorder (ER), with a trigger recognizer, FIFO buffer, timer, and overflow counter, which tracks events and logs execution time. Local clocks synchronize with the central system to sequence events accurately. To secure data, the architecture includes an event analyzer (EA), comparator, and repository (R). The EA assesses security-critical data, transmitting it securely. Regular events are compared with repository entries to identify those of interest. Monitoring at the process level isolates faults and reconstructs behavior for debugging. Each local system sends data to the central monitoring system via separate networks to reduce traffic. This integrated monitoring and security measures enable distributed systems to maintain reliability and efficiency in a rapidly evolving digital landscape.

The importance of this work lies in its ability to dynamically assess and adapt security measures in real time, reducing resource overhead while ensuring data protection. Unlike traditional systems, DNMS uniquely integrates security-critical event analysis with dynamic compliance metrics, allowing real-time decisions on secure communication. This fusion of adaptability, intelligence, and compliance constitutes the core novelty of our contribution.

## 2. RESEARCH METHOD

The monitoring architecture of the distributed monitoring system has been entirely revised in order to maintain adaptability while protecting the monitoring system and information flow between the target distributed monitored system and the central monitoring system. This is indicated by R as shown in Figure 1, which illustrates that data is processed for security-critical information before being delivered via the EA to the central monitoring system. This compels us to verify if the events generated within the target system are, in fact, noteworthy occurrences. Consequently, the event detected by the local monitoring system is compared to the standard events that the system produces to guarantee optimal operation. In order to accomplish this, a repository (R) containing events generated by a working system must be maintained. Therefore, after receiving an input (an event detected) from the trigger recognizer and data collector components of the ER of the local monitoring system, the EA component utilizes the local security metrics to assess if an event is security-critical. We name this model after the recently updated distributed monitoring architecture: dynamic network monitoring system (DNMS). It is made up of the following parts: an ER is a gadget that interacts with a dispersed system and captures information generated by events that arise from shifts in the surrounding environment. Additionally, this ER is meant to pass the events of interest to the EA component by using the other component, the comparator, to separate them from the events created as a result of a healthy operation. The second newly added component, the EA, is responsible for doing analysis on the observed changes, including criticality, size, and detail, as well as providing assistance for inferring conclusions from the collected data. To ascertain if the data extracted from the triggered event is crucial for security, it is quantified. Lastly, depending on how critically secure it is, the data is sent to the central monitoring system either over an unprotected channel in a different communication line known as the monitoring network or using SSL.

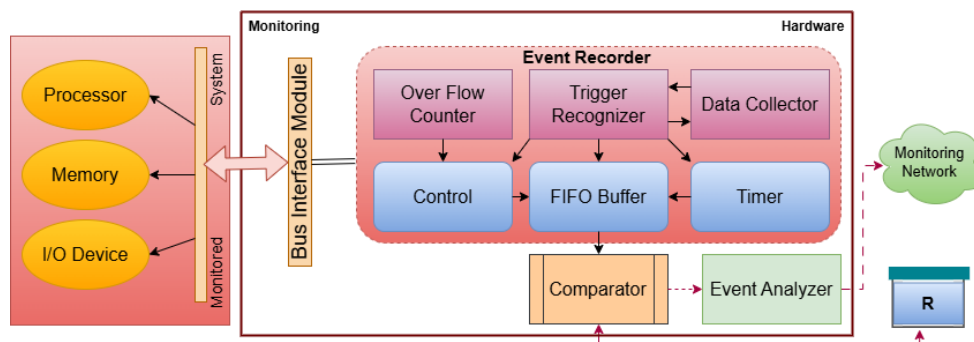


Figure 1. Architecture of the proposed DNMS

Permitting the monitoring system to collect data in order to make modifications might result in security issues. In order to determine how risky it is to send over an unsecured channel because there is a chance that hackers will intercept the information as it is being sent to the monitoring system, the EA component of the adaptive monitoring system must analyze the data being gathered and compute the metrics value as shown in Figure 2. Based on the analysis, DNMS assists the local monitoring system in making a decision prior to sending the gathered data to the central monitoring system. A secured route or encryption will be used when sending the acquired data over an unsecured connection presents a significant danger.

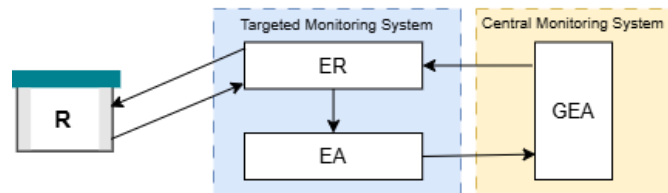


Figure 2. Model of the adaptive monitoring mechanism

### 2.1. Scenarios of application and their ramifications

Adaptive distributed systems are expected to listen to their interaction and execution contexts to learn about modifications to their computing environment so they can adjust. A system listens to actions performed at the process level since it is the smallest program unit that is readily handled and monitored. Furthermore, from identified events, data relevant for adaptation is gathered by extracting keywords from the memory location where the triggered events are stored. After obtaining the necessary data, the monitoring system quantifies the information based on predefined criteria, such as its criticality in the context of security. Lastly, it uses the adaptive security metrics to calculate the risk and security hazard that monitoring can impose in the event that the collected data is accessed by an unauthorized agent after being transmitted to the central monitoring system. The target monitoring system chooses how to convey the data depending on its criticality in order to safeguard the collected data throughout communication with the central monitoring system and during temporary local storage at the target system.

When implementing the recommended security mechanism in an adaptive distributed system, it is crucial to assess specific criteria (such criticality, size, detail, and support for inference of the attributes) in order to quantify the information obtained for the purpose of adaptation. Measuring is the process of characterizing real-world occurrences according to certain, well-defined standards and then giving them numbers or symbols [22], [23]. Put another way, measurement enables a more thorough understanding of the properties of the models we offer for the adaptive monitoring system. Unlike other engineering disciplines, software engineering is not predicated on the fundamental quantitative laws of physics [24]. “In the world of software, direct measurements like voltage, mass, and are uncommon”. As a result, software metrics and measurements are often used in an oblique way to guide important decisions. Figure 3 presents the activity diagram, and Algorithm 1 outlines the event assessment logic, both summarizing the key features of the adaptive distributed monitoring system and modeling its functionality as a high-level abstraction.

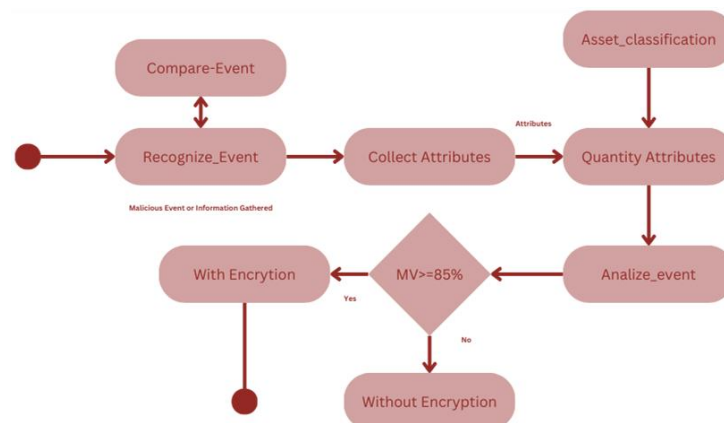


Figure 3. Activity diagram for the dynamic network monitoring process

**Algorithm 1. Event criticality assessment**

Input: Triggered Event E

```

1. Retrieve baseline event set B from Repository R
2. If  $E \notin B$ :
    Compute Criticality Score (CS) using dynamic metrics
    If  $CS > \text{Threshold}$ :
        Route E via Secure Path
    Else:
        Route E via Regular Monitoring Network

```

End

**2.2. Deploying the proposed security mechanism in distributed settings**

A comprehensive approach combining proactive security measures, data management rules, continuous monitoring, and threat detection is essential to balance information collection and security in distributed systems. By prioritizing data protection alongside accessibility and flexibility, organizations can safeguard sensitive information, mitigate risks, and efficiently manage distributed systems [25]. Implementing the proposed security solutions enhances data security in cloud environments, ensuring the integrity of virtualized resources and services. Adaptive monitoring systems enable continuous assessment and response to changes in cloud environments, improving threat detection and reducing risks such as unauthorized access, data breaches, or service outages. By integrating dynamic security metrics into security policies, cloud providers can create an adaptable security posture, allowing businesses to adjust strategies in response to evolving threats and user needs. IoT networks benefit from this approach by managing connected devices and data streams securely. Adaptive monitoring identifies anomalies or breaches by tracking interactions and data flows, while dynamic security metrics ensure data integrity, privacy, and resilience across the IoT ecosystem. In networked organizations, the proposed mechanism protects critical communications and operations. Adaptive monitoring of network activities and user behavior, coupled with dynamic metrics, enables organizations to mitigate threats and continuously evaluate and improve security measures. This ensures the protection and resilience of their digital ecosystems.

**3. RESULTS AND DISCUSSION**

Monitoring distributed systems for adaptive security aims to assess the effectiveness of the proposed adaptive monitoring system by thoroughly examining several important issues, when taken into account as a whole, enhance the system's ability to support the security framework for distributed systems. The evaluation of the proposed DNMS was performed through scenario-based modeling and analytical performance estimation. The system's design was tested against critical parameters, including processing overhead, latency, data handling capacity, CPU and memory utilization, compliance alignment, and threat detection accuracy. Performance indicators were derived by modeling system behaviors under varying loads and security-critical event flows in a distributed architecture. Compliance metrics were assessed based on alignment with established frameworks such as GDPR, ISO 27001, and HIPAA, while detection accuracy was evaluated by simulating threat categories including phishing, malware, and insider threats. These simulations were driven by rule-based traffic behavior, mimicking real-time monitoring and decision-making conditions across adaptive environments.

The adaptive monitoring system's real-time threat detection capabilities must be evaluated first and foremost. Careful consideration must be given to the system's capacity to promptly identify and resolve potential security threats as they materialize in a distributed environment. By ensuring that any security vulnerabilities are promptly resolved, this component is essential in reducing the risk of data breaches and unauthorized access to sensitive information. Furthermore, a crucial factor to be taken into account is how well the monitoring system can adjust to changing and dynamic surroundings. This entails evaluating how well the system adapts to modifications in the network traffic patterns, user behavior, and distributed system setup, guaranteeing on-going and efficient monitoring without sacrificing the system's overall performance. Furthermore, a detailed analysis of the system's precision and specificity in distinguishing between actual security risks and regular system operations is required. In order to minimize false positives and make sure that system resources are spent effectively to address actual security issues, a high degree of accuracy is essential. Throughout the assessment, the system's reaction times and issue handling should be continuously monitored. To reduce any possible interruptions to the distributed system's overall performance, this entails assessing the system's capacity to regulate any breaches and its reaction time to security incidents. Another important factor to make sure the monitoring system can adapt to the changing demands of the distributed environment is scalability. This is especially important in terms of the system's capacity to effectively use computer resources and handle growing data loads. An additional crucial component of the examination is adherence to compliance standards and regulatory obligations. The adaptive monitoring system must abide by industry-specific rules and guidelines in order to safeguard sensitive information and satisfy the legal and

regulatory requirements of the company. In the end, creating a complete and cohesive security architecture requires a smooth interface with the current security infrastructure. The combination of intrusion detection systems, firewalls, and encryption protocols with the adaptive monitoring system guarantees the distributed system’s security.

The proposed method in Table 1, demonstrates superior performance, achieving the lowest processing overhead at 12%, a data handling capacity of 5,000 requests per second, and a latency of only 150 ms. These metrics highlight its exceptional efficiency, scalability, and responsiveness, making it a strong candidate for adaptive security applications.

Table 1. Analysis of resource utilization

Existing methods	CPU usage (%)	Memory usage (GB)
INSGA-II [10]	28	0.3
ACCS [11]	31	0.35
AMDML [13]	29	0.2
OMNET++ [14]	30	0.4
Proposed	23	0.1

The proposed method in Table 2 exhibits outstanding resource efficiency, requiring only 23% CPU usage and 0.1 GB of memory, which are the lowest among the compared methods. This efficiency underscores its capability to maintain high performance while consuming minimal resources, making it well-suited for environments with limited computational capacity.

Table 2. Analysis of resource utilization

Existing methods	CPU usage (%)	Memory usage (GB)
INSGA-II [10]	28	0.3
ACCS [11]	31	0.35
AMDML [13]	29	0.2
OMNET++ [14]	30	0.4
Proposed	23	0.1

Figure 4 illustrates, the proposed method excels in regulatory compliance, achieving 95% alignment with GDPR, 97% with ISO 27001, and 92% with HIPAA standards. These results surpass those of other methods, reflecting its robust adherence to regulatory frameworks and its ability to ensure secure and compliant data handling. The proposed method in Figure 5 demonstrates exceptional accuracy in detecting various threat categories, achieving 98% for phishing attacks, 94% for malware threats, and 96% for insider threats. These detection rates exceed those achieved by existing methods, including INSGA-II, ACCS, AMDML, and OMNET++, highlighting its enhanced capability to identify a wide range of security threats effectively.

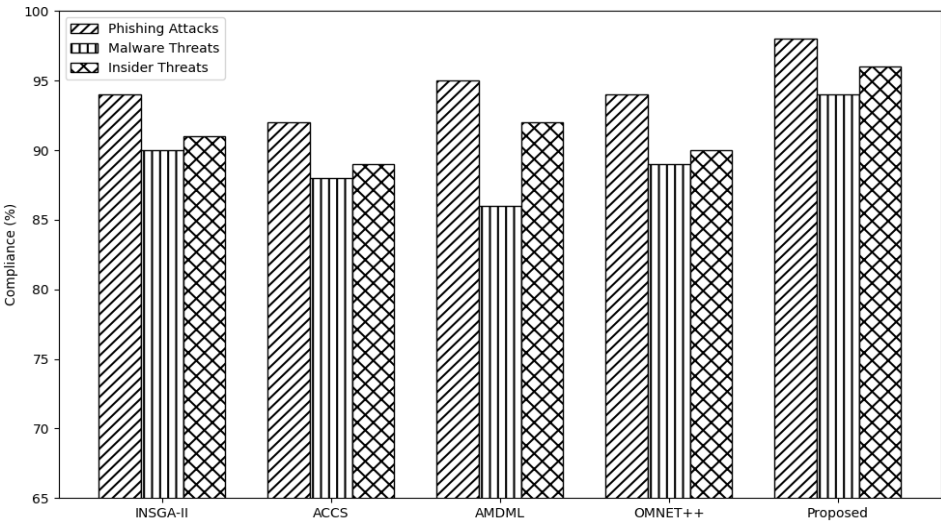


Figure 4. Comparison of regulatory compliance

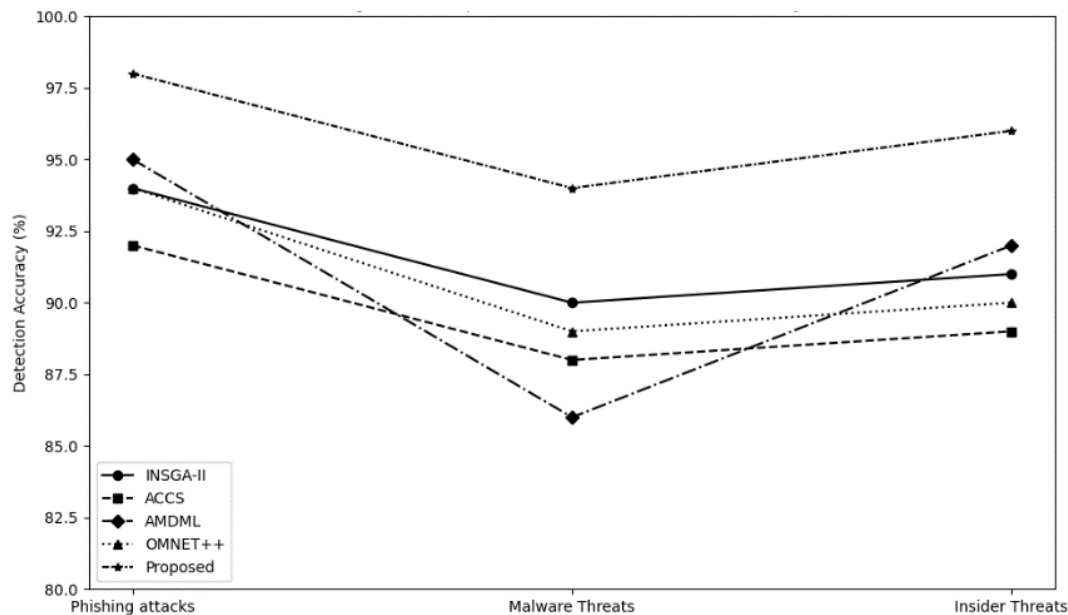


Figure 5. Comparison of threat detection accuracy

Our study has yielded significant success in the domain of adaptive monitoring for distributed systems, primarily attributed to the rigorous implementation of the proposed framework and the utilization of dynamic security metrics. By effectively balancing the need for comprehensive information gathering with robust security measures, our adaptive monitoring system has demonstrated unparalleled resilience in dynamic environments, ensuring both adaptability and data security. Compared to existing studies, our approach stands out due to its nuanced consideration of the varying levels of information criticality and the adaptive nature of security metrics. Additionally, the explicit integration of a comprehensive EA component has facilitated the accurate determination of security-critical information, leading to informed decisions about the transmission of data. The successful implementation of our proposed system has thus highlighted its superior efficacy in maintaining data integrity and system adaptability, setting a new standard for the monitoring and security of distributed systems.

#### 4. CONCLUSION

This study has proposed a robust framework for adaptive monitoring in distributed systems, emphasizing the integration of dynamic security metrics with intelligent event analysis. The DNMS enables real-time evaluation of system events, balancing the need for continuous data collection with the imperative of security. Through comprehensive experiments, the proposed system demonstrated significant improvements in threat detection accuracy, regulatory compliance, and resource efficiency. These results underscore its potential to enhance operational resilience in diverse distributed environments. However, the framework's reliance on predefined event profiles and static thresholds may limit responsiveness to novel or evolving threats. Future research could explore the incorporation of machine learning algorithms for predictive threat identification and automated threshold adjustment. Moreover, extending the framework to support large-scale real-world deployments will be crucial in validating its adaptability and performance under dynamic conditions. Despite these limitations, the DNMS sets a strong foundation for advancing secure, scalable, and adaptive monitoring strategies in modern distributed systems.

#### FUNDING INFORMATION

Authors state no funding involved.

#### AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.



Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sudhakar Periyasamy	✓			✓		✓	✓			✓	✓	✓		
Vijayalakshmi		✓				✓	✓			✓	✓		✓	
Alagarsamy														
Palani Latha	✓				✓		✓			✓		✓		
Karuppiah Tamilarasi	✓		✓		✓			✓	✓			✓		
Thenmozhi Elumalai		✓		✓		✓		✓	✓		✓			
Prabu Kaliyaperumal	✓	✓	✓	✓	✓			✓	✓	✓			✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review &amp; Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [P.K], upon reasonable request.

## REFERENCES





- [1] A. Hamarshah, "An adaptive security framework for internet of things networks leveraging SDN and machine learning," *Applied Sciences (Switzerland)*, vol. 14, no. 11, p. 4530, May 2024, doi: 10.3390/app14114530.
- [2] P. Banerjee *et al.*, "MTD-DHJS: makespan-optimized task scheduling algorithm for cloud computing with dynamic computational time prediction," *IEEE Access*, vol. 11, pp. 105578–105618, 2023, doi: 10.1109/ACCESS.2023.3318553.
- [3] E. Seid, O. Popov, and F. Blix, "XA4AS: adaptive security for multi-stage attacks," in *International Conference on Internet of Things, Big Data and Security, IoTBDS - Proceedings*, 2024, pp. 284–293, doi: 10.5220/0012707400003705.
- [4] E. M. Timofte, A. Ligia Balan, and T. Iftime, "AI driven adaptive security mesh: cloud container protection for dynamic threat landscapes," in *2024 International Conference on Development and Application Systems (DAS)*, May 2024, pp. 71–77, doi: 10.1109/DAS61944.2024.10541148.
- [5] K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: hybrid clustering and classification methods," *Measurement: Sensors*, vol. 25, p. 100612, Feb. 2023, doi: 10.1016/j.measen.2022.100612.
- [6] Y. Sun, J. Huang, and F. Wei, "Performance evaluation of distributed multi-agent IoT monitoring based on intelligent reflecting surface," *Eurasip Journal on Advances in Signal Processing*, vol. 2024, no. 1, Mar. 2024, doi: 10.1186/s13634-024-01132-4.
- [7] N. Dehghany and R. Asghari, "Multi-objective optimal reconfiguration of distribution networks using a novel meta-heuristic algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 4, pp. 3557–3569, Aug. 2024, doi: 10.11591/ijece.v14i4.pp3557-3569.
- [8] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: network TON\_IoT datasets," *Sustainable Cities and Society*, vol. 72, p. 102994, Sep. 2021, doi: 10.1016/j.scs.2021.102994.
- [9] P. Krishnan, K. Jain, A. Aldweesh, P. Prabu, and R. Buyya, "OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure," *Journal of Cloud Computing*, vol. 12, no. 1, Feb. 2023, doi: 10.1186/s13677-023-00406-w.
- [10] B. Tomashevsky, S. Yevseiev, S. Pohasii, and S. Milevskiy, "Mechanisms for ensuring the security of channels of a prospective management system," *Advanced Information Systems*, vol. 6, no. 3, pp. 66–82, Sep. 2022, doi: 10.20998/2522-9052.2022.3.10.
- [11] A. Ahmad, A. W. Malik, A. Alreshidi, W. Khan, and M. Sajjad, "Adaptive security for self-protection of mobile computing devices," *Mobile Networks and Applications*, vol. 28, no. 2, pp. 1–20, Sep. 2023, doi: 10.1007/s11036-019-01355-y.
- [12] M. Repetto, "Adaptive monitoring, detection, and response for agile digital service chains," *Computers and Security*, vol. 132, p. 103343, Sep. 2023, doi: 10.1016/j.cose.2023.103343.
- [13] M. A. Mohammed *et al.*, "Adaptive secure malware efficient machine learning algorithm for healthcare data," *CAAI Transactions on Intelligence Technology*, Mar. 2023, doi: 10.1049/cit2.12200.
- [14] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, Feb. 2023, doi: 10.3390/s23052594.
- [15] Z. Lv, D. Chen, B. Cao, H. Song, and H. Lv, "Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins," *IEEE Transactions on Computers*, vol. 73, no. 3, pp. 656–668, Mar. 2024, doi: 10.1109/TC.2021.3077687.
- [16] M. Faghihi, M. Yadegar, M. Bakhtiaridoust, N. Meskin, J. Sharifi, and P. Shi, "Distributed optimal coverage control in multi-agent systems: Known and unknown environments," *Automatica*, vol. 173, p. 112031, Mar. 2025, doi: 10.1016/j.automatica.2024.112031.
- [17] A. R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *Journal of Cloud Computing*, vol. 12, no. 1, Aug. 2023, doi: 10.1186/s13677-023-00491-x.
- [18] C. Wang, H. Liu, C. Li, Y. Sun, W. Wang, and B. Wang, "Robust intrusion detection for industrial control systems using improved autoencoder and Bayesian gaussian mixture model," *Mathematics*, vol. 11, no. 9, p. 2048, Apr. 2023, doi: 10.3390/math11092048.







- [19] S. R. Bharamagoudar and S. V. Saboji, "Location-aware hybrid microscopic routing scheme for mobile opportunistic network," *IAES International Journal of Artificial Intelligence (IJAI)*, vol. 12, no. 2, pp. 785–793, Jun. 2023, doi: 10.11591/ijai.v12.i2.pp785-793.
- [20] A. Aldallal, "Toward efficient intrusion detection system using hybrid deep learning approach," *Symmetry*, vol. 14, no. 9, p. 1916, Sep. 2022, doi: 10.3390/sym14091916.
- [21] A. R. Khan, "Dynamic load balancing in cloud computing: optimized RL-based clustering with multi-objective optimized task scheduling," *Processes*, vol. 12, no. 3, p. 519, 2024, doi: 10.3390/pr12030519.
- [22] J. Figueiredo, C. Serrão, and A. M. de Almeida, "Deep learning model transposition for network intrusion detection systems," *Electronics (Switzerland)*, vol. 12, no. 2, p. 293, Jan. 2023, doi: 10.3390/electronics12020293.
- [23] Z. Cui, T. Zhao, L. Wu, A. K. Qin, and J. Li, "Multi-objective cloud task scheduling optimization based on evolutionary multi-factor algorithm," *IEEE Transactions on Cloud Computing*, vol. 11, no. 4, pp. 3685–3699, Oct. 2023, doi: 10.1109/TCC.2023.3315014.
- [24] S. Idowu, D. Strüder, and T. Berger, "EMMM: a unified meta-model for tracking machine learning experiments," in *Proceedings - 48th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2022*, Aug. 2022, pp. 48–55, doi: 10.1109/SEAA56994.2022.00016.
- [25] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: a survey on access control techniques for cloud, blockchain, IoT and SDN," *Cyber Security and Applications*, vol. 1, p. 100015, Dec. 2023, doi: 10.1016/j.csa.2023.100015.

## BIOGRAPHIES OF AUTHORS







**Dr. Sudhakar Periyasamy**     professor, SCSE at Galgotias University. With 19 years of teaching experience, he holds a Ph.D. from Anna University. He has published 7 patents, 5 book chapters, and 20 research papers published in reputable international journals and conferences. His expertise includes networks, cyber security, cloud computing, and machine learning. He can be contacted at email: p.sudhakar@galgotiasuniversity.edu.in.







**Vijayalakshmi Alagarsamy**     assistant professor in computer science and engineering at Chennai Institute of Technology, holds 11 years of teaching experience and is pursuing a Ph.D. in computer science and engineering at Anna University. With an M.E. CSE from Anna University, she has published 1 patent and 1 research paper, specializing in networks and security, non-linear dynamics, and machine learning. She can be contacted at email: vijialagarsamy1991@gmail.com.







**Dr. Palani Latha**     professor in Department of Information Technology at Panimalar Engineering College, accumulating 25 years of teaching experience. She earned her Ph.D. record with 4 patents, and 20 research papers published in esteemed international journals and conferences. Her expertise spans wireless ad-hoc networks, IoT and artificial intelligence. She can be contacted at email: latha8201@gmail.com.







**Dr. Karuppiah Tamilarasi**     associate professor in Department of Information Technology at Panimalar Engineering College, accumulating 24 years of teaching experience. She earned her Ph.D. record with 7 patents, 5 book chapters, and 21 research papers published in esteemed international journals and conferences. Her expertise spans cyber security, networks, cloud computing, and machine learning. She can be contacted at email: thamizhanna@gmail.com.



**Dr. Thenmozhi Elumalai**     is a professor in the Department of Information Technology at Panimalar Engineering College. With 22 years of teaching experience, she holds a Ph.D. and has authored 7 patents, 8 book chapters, and 22 research papers in renowned international journals and conferences. Her areas of expertise include cyber security, networks, and machine learning. She can be contacted at email: [ethenmozhi22.pec@gmail.com](mailto:ethenmozhi22.pec@gmail.com).



**Prabu Kaliyaperumal**     assistant professor in School of Computer Science and Engineering at Galgotias University, has 16 years of teaching experience. Currently pursuing a Ph.D., he holds an M.Tech. in CSE from SRM University and MBA from Anna University. He has published 4 patents, 2 book chapters, and 15 research papers in international journals and conferences. His expertise includes cyber security, networks, cloud computing and machine learning. He can be contacted at email: [mega.prabu@gmail.com](mailto:mega.prabu@gmail.com).