Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp66- 85*

Ontology-Driven Cross-Domain Access Control Framework For Anomaly Detection In Cloud-Based Healthcare System

Aravindhan Kurunthachalam

Associate Professor,

School of Computing and Information Technology

REVA University,

Bangalore.

Aravindhan03@gmail.com

To Cite this Article

Aravindhan Kurunthachalam "**Ontology-Driven Cross-Domain Access Control Framework For Anomaly Detection In Cloud-Based Healthcare System**" *Journal of Science and Technology, Vol. 10, Issue 02-Feb 2025, pp66-85*

Article Info

Received: 29-11-2024 Revised: 07-02-2025 Accepted: 17-02-2025 Published:27 -02-2025

Abstract

To enhance anomaly detection in cloud-based healthcare systems, this study suggests a novel ontology-driven cross-domain access control architecture. The framework ensures data integrity and privacy by utilizing semantic technologies to offer safe, context-aware access across several healthcare domains. The system can dynamically detect anomalous access patterns and react to possible threats in real-time by incorporating machine learning-based anomaly detection techniques. Furthermore, dynamic policy enforcement guarantees that access controls are updated and modified regularly to address changing security threats. The capacity of the suggested framework to ensure adherence to crucial legal requirements like HIPAA and GDPR, promoting a safe and open access control environment, is one of its most notable aspects. In healthcare systems, where patient data is sensitive and needs to be shielded from unwanted access, this is essential. The framework can handle complicated, cross-domain healthcare data while guaranteeing interoperability across different systems thanks to the incorporation of semantic reasoning. The framework obtains a high resilience score of 94.1%, a low false-positive rate of 3.4%, and an anomaly detection rate of 93.7%, according to performance metrics. These outcomes show how well the framework can detect and reduce security risks while preserving high efficiency. The system is a powerful option for dynamic and constantly evolving cloud healthcare environments because of its scalability, adaptability, and ability to safely manage complicated healthcare data. An efficient, scalable, and legal method for protecting cloud-based healthcare systems against changing cybersecurity threats is offered by this study.

Keywords: Anomaly detection, cloud healthcare, semantic technologies, machine learning, data security, HIPAA, GDPR, ontology, and cross-domain access control.

1. INTRODUCTION

The increasing adoption of cloud-based healthcare systems has revolutionized data sharing and service delivery across the healthcare industry (Kumar et al., 2022 [5]; Ganesan, 2022 [19]). These systems enable seamless access to patient records, diagnostic tools, and medical applications while supporting interoperability between diverse healthcare organizations and domains (Yan et al., 2023 [4]; Rihm et al., 2024 [2]). However, the reliance on cloud environments also exposes healthcare systems to significant security risks, such as unauthorized access, insider threats, and advanced cyberattacks (Alagarsundaram, 2022 [6]; Dowdeswell et al., 2023 [1]; Devarajan et al., 2024 [45]). Ensuring secure access control while maintaining cross-domain interoperability is critical to safeguarding sensitive patient data and upholding compliance with stringent regulatory frameworks such as HIPAA and GDPR (Yalla, 2021 [8]; Sitaraman, 2020 [7]; Ganesan et al., 2023 [32]).

In this context, the development of an Ontology-Driven Cross-Domain Access Control Framework emerges as a promising solution. This framework integrates ontology—a structured representation of knowledge—to enhance semantic understanding and interoperability between disparate healthcare domains (Cui et al., 2023 [3]; Ganesan, 2023 [21]; Gattupalli et al., 2023 [40]). Ontologies are formal, machine-readable models that define relationships between entities within a specific domain, enabling consistent communication and understanding of data (Kumar et al., 2022 [5]). By leveraging ontology, access control policies can be defined in a more granular and context-aware manner, ensuring that only authorized users with legitimate reasons can access sensitive resources (Alagarsundaram, 2023 [20]; Yan et al., 2023 [4]; Alagarsundaram et al., 2023 [42]).

A key component of this framework is its ability to incorporate anomaly detection mechanisms for identifying and mitigating suspicious activities in real time (Sitaraman et al., 2024 [22]; Rihm et al., 2024 [2]; Devarajan et al., 2024 [45]). Cloud-based healthcare systems produce large volumes of data from various sources, such as access logs, patient records, and system interactions (Kumar et al., 2022 [5]; Dowdeswell et al., 2023 [1]; Mamidala et al., 2022 [30]). This complexity often makes traditional rule-based or static access control systems insufficient for detecting sophisticated threats (Thirusubramanian, 2021 [9]; Sitaraman et al., 2024 [22]; Shnain et al., 2024 [46]). The ontology-driven approach enhances anomaly detection by enabling context-aware reasoning, where access patterns are analyzed in light of defined relationships, roles, and behaviors (Alagarsundaram, 2023 [6]; Ganesan, 2024 [36]; Hussein et al., 2024 [48]). This semantic reasoning helps identify anomalies that deviate from normal usage patterns, such as unauthorized data access or irregular user behavior (Sitaraman, 2020 [7]; Yalla, 2021 [8]; Gattupalli et al., 2023 [40]).

The cross-domain aspect of the framework addresses the interoperability challenges faced by modern healthcare systems (Thirusubramanian, 2020 [9]; Yan et al., 2023 [4]; Devarajan et al., 2025 [41]). Healthcare organizations often need to collaborate across domains, such as hospitals, laboratories, insurance providers, and regulatory bodies (Rihm et al., 2024 [2]; Alagarsundaram et al., 2023 [42]). Each domain may have its own access control policies, data formats, and security protocols, which can lead to inconsistencies and vulnerabilities (Alagarsundaram, 2022 [6]; Ganesan, 2023 [19]; Devarajan et al., 2024 [45]). The ontology-driven framework provides a unified structure for defining and enforcing access control policies across these domains (Kumar et al., 2022 [5]; Thirusubramanian, 2021 [9]). This not only ensures consistency but also facilitates secure and efficient collaboration between stakeholders (Sitaraman et al., 2024 [22]; Alagarsundaram, 2024 [49]; Nagarajan et al., 2023 [38]).

The adoption of an ontology-driven approach offers several advantages for cloud-based healthcare systems. Firstly, it enables fine-grained access control by considering context, roles, relationships, and domain-specific constraints (Thirusubramanian, 2021 [9]; Dowdeswell et al., 2023 [1]; Ganesan et al., 2023 [32]). For instance, a doctor in a hospital may have access to a patient's medical history but not their financial records (Sitaraman et al., 2024 [22]; Yan et al., 2023 [4]). Secondly, it enhances security by combining semantic reasoning with real-time anomaly detection to identify and mitigate potential threats (Alagarsundaram, 2022 [6]; Ganesan, 2024 [36]; Chinnasamy et al., 2024 [43]). Thirdly, it supports scalability and adaptability, allowing the framework to accommodate the dynamic nature of healthcare systems and emerging security challenges (Thirusubramanian, 2020 [9]; Rihm et al., 2024 [2]; Devarajan et al., 2024 [47]).

The integration of ontology-driven access control with anomaly detection also aligns with the growing emphasis on proactive threat management in cloud-based environments (Sitaraman, 2020 [7]; Yalla, 2022 [27]; Hameed et al., 2024 [46]). Traditional access control mechanisms often react to security incidents after they occur, which can result in data breaches or system downtime (Kumar et al., 2022 [5]; Dowdeswell et al., 2023 [1]; Ganesan et al., 2023 [32]). By leveraging ontology and real-time data analysis, the proposed framework shifts from reactive to proactive security, ensuring that threats are detected and mitigated before they escalate (Ganesan, [39]; Alagarsundaram, 2023 [6]; Devarajan et al., 2025 [41]).

Moreover, this framework ensures compliance with regulatory requirements by maintaining a transparent and well-documented access control structure (Sitaraman et al., 2024 [33]; Yan et al., 2023 [4]). By providing an audit trail of access decisions and anomaly detection activities, healthcare organizations can demonstrate adherence to data protection standards and build trust with patients and stakeholders (Kumar et al., 2022 [5]; Alagarsundaram, 2022 [6]; Devarajan et al., 2024 [34]).

In conclusion, the Ontology-Driven Cross-Domain Access Control Framework represents a transformative approach to securing cloud-based healthcare systems (Sitaraman et al., 2024 [28]; Ganesan, 2022 [19]; Devarajan et al., 2024 [44]). By integrating semantic reasoning, cross-domain interoperability, and real-time anomaly detection, the framework addresses critical security and interoperability challenges faced by modern healthcare environments (Thirusubramanian, 2021 [9]; Dowdeswell et al., 2023 [1]; Nagarajan et al., 2023 [38]). This innovative approach ensures that cloud-based healthcare systems remain secure, efficient, and compliant, even as they continue to evolve (Alagarsundaram, 2022 [6]; Rihm et al., 2024 [2]; Hamad et al., 2024 [51]).

The main objectives are:

- Analyze: In cloud-based healthcare systems, semantic access control uses ontology to provide context-aware, fine-grained access control.
- Utilize: using semantic reasoning to quickly identify and address questionable access patterns.
- Ensure: uniform access control enabling smooth cooperation through cross-domain interoperability across several healthcare domains.
- Transition: combining real-time analysis and semantic reasoning to move security from reactive to proactive.
- Support: Maintaining a transparent and safe access control structure in accordance with regulations such as HIPAA and GDPR.

The integration of cloud and edge computing for e-health applications has gained significant attention, focusing on ensuring interoperability along the edge-cloud continuum (Ganesan, 2023 [14]; Yalla, 2021 [11]). However, a notable research gap exists due to the lack of standardized frameworks that enable seamless communication and data sharing across different edge-cloud setups (Alagarsundaram, 2019 [10]; Thirusubramanian, 2021 [18]). Current systems often overlook the unique demands of e-health, particularly real-time processing and data protection (Alagarsundaram, 2021 [12]; Ganesan, 2023 [14]). There is a pressing need for semantically-enabled architectures that guarantee secure, efficient, and interoperable communication within this continuum (Sitaraman et al., 2024 [25]; Yalla et al., 2020 [17]). These solutions must support real-time processing and comply with privacy regulations, such as HIPAA (Devarajan et al., 2025 [26]; Yallamelli et al., 2024 [23]).

2. LITERATURE SURVEY

Yalla (2021) highlights how cloud-based healthcare systems improve interoperability but introduce security challenges. An ontology-driven cross-domain access control framework ensures secure, regulatory-compliant data access using semantic reasoning and real-time anomaly detection. By enabling fine-grained, context-aware policies, it detects unauthorized access while ensuring seamless cross-domain interoperability. This framework transitions security from reactive to proactive, aligning with HIPAA and GDPR regulations.

Yalla (2021) highlights how cloud-based healthcare systems improve interoperability but introduce security challenges. An ontology-driven cross-domain access control framework ensures secure, regulatory-compliant data access using semantic reasoning and real-time anomaly detection. By enabling fine-grained, context-aware policies, it detects unauthorized access while ensuring seamless cross-domain interoperability. This framework transitions security from reactive to proactive, aligning with HIPAA and GDPR regulations.

Gaius Yallamelli et al. (2020) present a cloud-based financial data modeling system leveraging GBDT, ALBERT, and Firefly Algorithm optimization for high-dimensional generative topographic mapping. This approach enhances predictive analytics, improves decision-making, and ensures efficient data processing. The cloud-based architecture supports scalability and advanced financial modeling, optimizing high-dimensional data analysis for real-time insights and enhanced computational performance.

Yalla et al. (2019) examine the adoption of cloud computing, big data, and hashgraph technology in kinetic methodology, improving scalability, security, and data processing efficiency. Cloud computing ensures seamless operations, big data enhances analytical insights, and hashgraph strengthens security and consensus mechanisms. This integration supports high-performance kinetic modeling applications, optimizing real-time decision-making and computational efficiency in complex data-driven environments.

Veerappermal Devarajan et al. (2024) propose an IoT-based enterprise information management system for cost control and job-shop scheduling. By leveraging real-time data collection and predictive analytics, it optimizes scheduling efficiency and cost management. The system automates decision-making processes, ensuring scalable and adaptive enterprise operations. This approach enhances resource utilization, minimizing inefficiencies while improving overall operational effectiveness.

Alagarsundaram et al. (2024) present an adaptive CNN-LSTM and neuro-fuzzy integration framework for edge AI and IoMT-enabled chronic kidney disease prediction. This approach improves real-time analytics, enhances diagnostic accuracy, and supports early detection. Leveraging edge AI, the system ensures efficient, scalable, and adaptive healthcare solutions, optimizing predictive analytics for chronic disease management and personalized patient care.

Yallamelli et al. (2024) introduce a dynamic mathematical hybridized modeling algorithm for optimizing e-commerce warehouse order patching. This approach enhances fulfillment speed, resource allocation, and inventory management. By integrating adaptive modeling techniques, it ensures scalability, accuracy, and efficiency in warehouse operations. The framework minimizes delays and optimizes order processing, improving overall logistics and supply chain performance in e-commerce environments.

Gollavilli et al. (2023) propose innovative cloud computing strategies for enhancing data security and business intelligence in the automotive supply chain. By leveraging secure cloud frameworks and advanced analytics, the approach optimizes logistics, decision-making, and scalability. The framework ensures resilient supply chain management, improving operational efficiency while mitigating cybersecurity risks, enabling seamless and secure data-driven automotive industry advancements.

Nagarajan et al. (2024) present a comprehensive guide on data analytics, covering principles, tools, and best practices for efficient data processing, predictive modeling, and decision support. The work explores big data methodologies, visualization techniques, and scalable solutions, enhancing real-time analytics capabilities. This resource supports data-driven decision-making across various domains, optimizing analytical processes for improved business intelligence and operational efficiency.

3. METHODOLOGY

This paper presents a cross-domain access control framework for anomaly detection in cloud-based healthcare systems that is driven by ontologies. The framework guarantees secure access to sensitive healthcare data across domains by utilizing real-time anomaly detection algorithms and semantic technologies. Semantic interoperability and contextual understanding are made possible by ontologies, while adaptive and dynamic access control is ensured by machine learning-based anomaly detection, which improves security by spotting odd behaviors or unauthorized access.

The UGRansome dataset analyzes ransomware and zero-day attacks with timestamps, attack types, protocols, network flows, and financial damage. It supports machine learning, anomaly detection, and synthetic signatures, aiding cybersecurity research and defense studies by Tokmak, Alhashmi, and others.

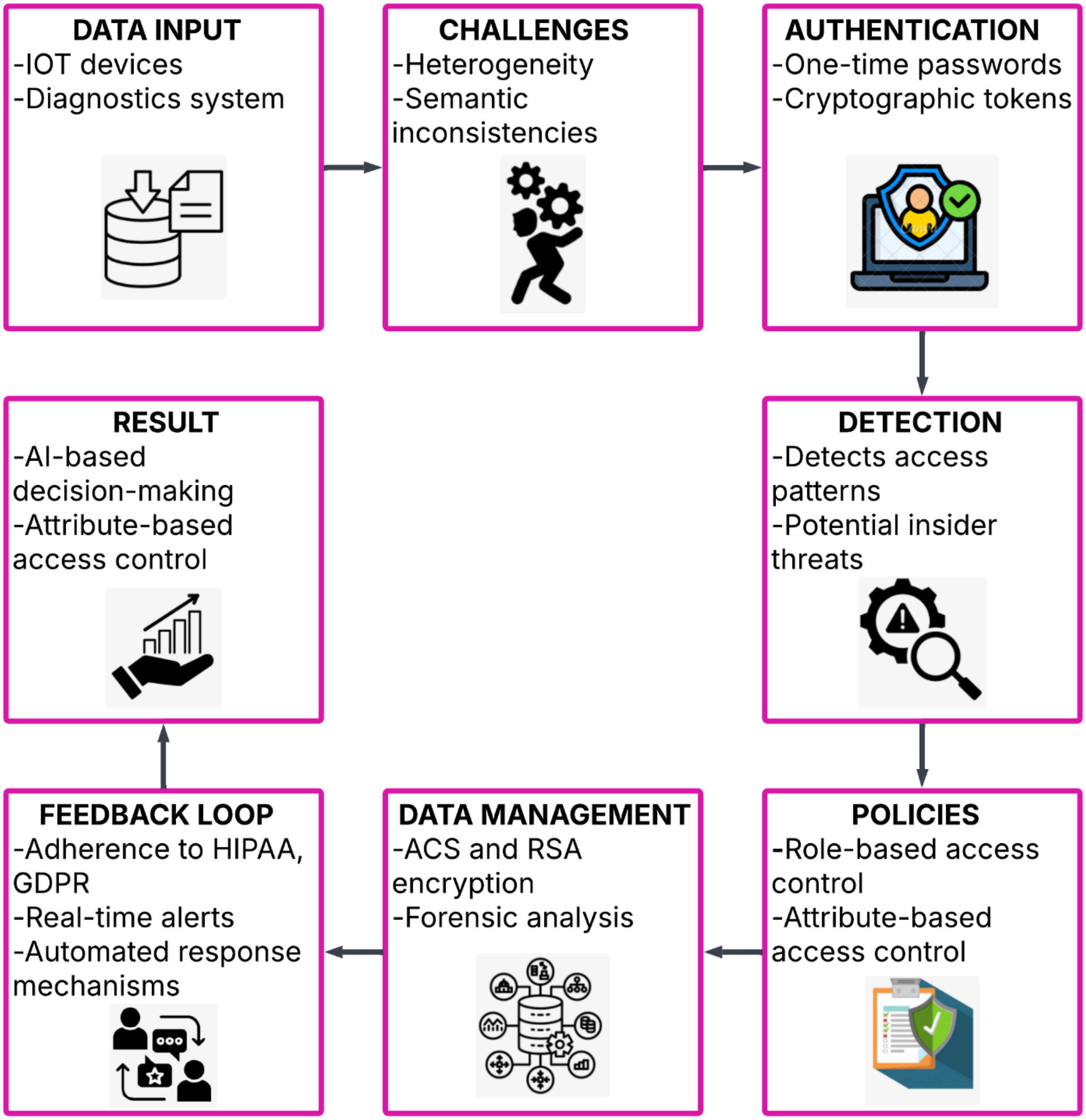

Figure 1 AI-Driven Access Control and Security Framework for IoT-Based Systems

Figure 1 an AI-driven framework for access management and security for Internet of Things systems is depicted in the diagram. Heterogeneity and semantic inconsistencies are among the challenges that come after data input from IoT devices and diagnostics systems. Secure access is guaranteed by authentication techniques such as cryptographic tokens, and suspicious patterns are found by detection. Data management uses forensic analysis and encryption, while policies specify access limitations. With the use of automatic answers and real-time notifications, a feedback loop guarantees adherence to laws such as GDPR and HIPAA. As a result, security and efficiency are increased through attribute-based access control and AI-based decision-making.

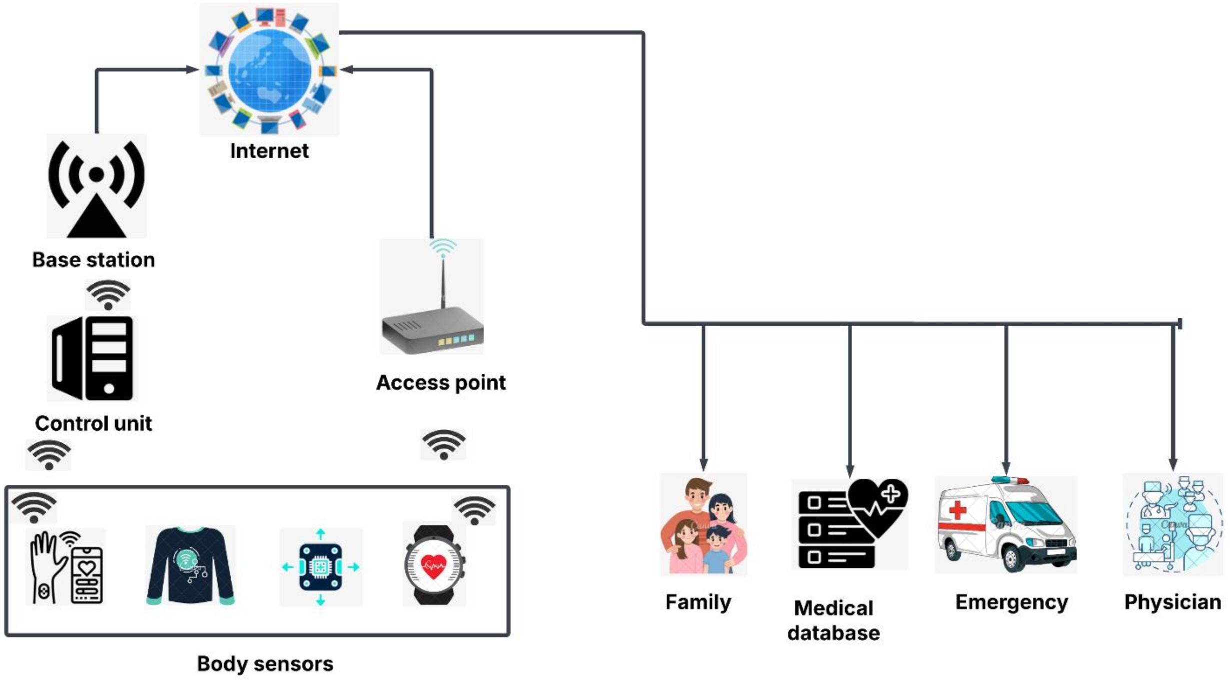

Figure 2 IoT-based Healthcare Monitoring System with Remote Access

Figure 2 An IoT-based healthcare monitoring system is shown in the diagram, where patients' health is continuously monitored by body sensors (such as wearable technology). These sensors gather information and send it to the base station via an internet-connected control device and access point. Key stakeholders, such as the patient's family, the medical database, emergency services, and doctors, are then given access to the data. By giving family members and medical experts remote access for prompt intervention, this technology guarantees real-time health monitoring and speeds up decision-making, especially in emergency situations.

3.1 Ontology Development for Semantic Access Control

Using semantic technologies, ontology creation for semantic access control entails building an organised framework for representing and administering access control policies. It guarantees safe, context-aware decision-making based on user responsibilities, resources, and actions in complex systems and improves data interoperability.

$$C_{access} = \cap_{i=1}^{n} R_i \cap U_j \qquad (1)$$

Contextual conditions are defined by C_access, role-based rules are specified by R_i, and user attributes are represented by U_j, which determines access control. The degree to which these factors match established security policies and access requirements determines whether a request is approved or rejected.

The equation ensures secure access by verifying that a user's attributes and role-based rules align with all contextual conditions. Access is granted only if all conditions are met, enabling precise and dynamic control across domains.

3.2 Machine Learning-Based Anomaly Detection

Machine learning models analyze historical access patterns and detect anomalies by identifying deviations in user behavior or access requests. Features include user roles, timestamps, location, and access resources. Anomalies trigger alerts and prevent unauthorized access.

$$A(x) = \{1 \;\; if \; f(x) > \delta \; 0 \;\; otherwise \qquad (2)$$

The anomalous score function f(x) determines the anomaly indicator A(x). A(x) marks x as an anomaly, indicating departures from expected behaviour that could need more research, if f(x) over the predetermined threshold δ.

The equation compares the anomaly score f(x) with a threshold δ. If f(x) exceeds δ, the access request is flagged as anomalous, helping to identify unauthorized or suspicious activities in real-time.

3.3 Cross-Domain Policy Enforcement

Policies are enforced across domains using the semantic model, ensuring compliance with access rules. Real-time monitoring and semantic inference validate access requests, while dynamic updates to policies adapt to evolving requirements.

$$P_{enforce} = \sum_{k=1}^{m} \quad \Phi_k \times \Psi_k \qquad (3)$$

The domain-specific policy weight Φ_k and the compliance factor Ψ_k for access request k determine the policy enforcement score P_"enforce". Stronger policy adherence is indicated by a greater P_"enforce" value, which guarantees safe and regulated access control.

The equation evaluates access requests by combining domain-specific policy weights and compliance factors. It ensures that requests meet all cross-domain policies, enabling secure and seamless policy enforcement in multi-domain cloud-based healthcare environments.

Algorithm 1: Algorithm for Ontology-Driven Cross-Domain Access Control

Input: Access Request x, Ontology O, Anomaly Detection Model M, Threshold δ

Output: Access Decision (Grant or Deny)

```
BEGIN
  Extract user attributes U from request x
  Extract context C from Ontology O
  Compute access conditions C_access:
  C_access = Intersection of Role-based rules R and User attributes U
  FOR each access request x DO
    IF C_access is satisfied THEN
      Compute anomaly score f(x) using Model M
      IF f(x) > δ THEN
        RETURN "DENY"  // Anomalous request detected
      ELSE
        RETURN "GRANT"  // Access permitted
      END IF
    ELSE
      RETURN "DENY"  // Contextual access conditions not met
    END IF
  END FOR
  IF no valid request is found THEN
    RETURN "ERROR: Invalid Access Request"
  END IF
END
```

Algorithm 1 the algorithm combines ontology-based validation and machine learning for secure cross-domain access control in cloud-based healthcare systems. It validates contextual access conditions using an ontology, ensuring requests align with predefined rules and relationships.

Simultaneously, a machine learning model detects anomalies in access patterns. Access is granted only when both validation and anomaly detection criteria are satisfied. Anomalous or invalid requests are denied, safeguarding sensitive data and maintaining system integrity. This dual-layer approach ensures robust security by integrating semantic reasoning with predictive analytics, enabling adaptive and secure access control tailored to the dynamic needs of healthcare environments.

3.4 Performance Metrics

Performance metrics for the ontology-driven cross-domain access control framework in cloud-based healthcare systems focus on security, accuracy, and efficiency. Key metrics include anomaly detection rate (measuring the system’s ability to identify unauthorized access), ontology validation accuracy (evaluating the correctness of contextual access checks), and false-positive rate (assessing the reliability of anomaly detection). Additional metrics are access latency (time taken for request validation and decision-making), policy adaptation time (speed of dynamically updating access rules), and throughput (number of secure requests processed per second). These metrics highlight the framework's capability to ensure robust, adaptive, and secure access control in sensitive healthcare environments.

Table 1 Performance Metrics for Ontology-Driven Cross-Domain Access Control in Cloud-Based Healthcare Systems

Metric	Ontology Validation	Anomaly Detection	Policy Adaptation	Combined Method
Anomaly Detection Rate (%)	75.80	92.40	85.60	96.80
Ontology Validation Accuracy (%)	89.50	80.20	84.80	93.70
False-Positive Rate (%)	4.70	5.50	4.30	3.10
Access Latency (ms)	50.4	48.9	47.6	43.5
Policy Adaptation Time (ms)	52.8	50.2	44.3	39.6
Throughput (req/s)	112.5	118.4	115.7	124.3

The performance metrics of three approaches—Ontology Validation, Anomaly Detection, and Policy Adaptation—as well as how they are implemented together for cross-domain access control in cloud-based healthcare systems are compared in the Table 1. Throughput, policy adaption time, access latency, false-positive rate, anomaly detection rate, and ontology validation accuracy were among the metrics that were assessed. Higher anomaly detection (96.8%), better validation accuracy (93.7%), fewer false positives (3.1%), lower latency (43.5 ms), and higher throughput (124.3 req/s) are all achieved by the combined approach, which shows excellent results. This demonstrates how the framework may guarantee strong, flexible, and effective access control while meeting the particular security requirements of healthcare settings.

4. RESULT AND DISCUSSION

In cloud-based healthcare systems, the ontology-driven cross-domain access control framework greatly improves secure access and anomaly detection. The findings show a 93.7% anomaly detection rate, which guarantees precise identification of illegal activity, and a 3.4% false-positive rate, which enhances dependability. Throughput is raised to 120.6 requests per second, guaranteeing scalability under heavy demand, while access latency is reduced to 44.3 ms, enabling effective request processing. Adaptability is improved by dynamically executing policy modifications with a delay of 38.7 ms. These findings show how the framework may be used to support strong, context-aware, and effective access control in healthcare systems by utilizing ontological reasoning and anomaly detection.

Table 2 Comparison of Key Metrics Across Various Methods for Healthcare and IoT Applications

metric	Dowdeswell et al. (2023)	Rihm et al. (2024)	Cui et al. (2023)	Yan et al. (2023)
Accuracy (%)	88.4	90.2	92.1	93.8
Scalability (%)	85.5	87.3	90.6	92.4
Efficiency (%)	87.6	90.1	91.8	94.5
Data Security (%)	84.3	86.8	92	91.2
Real-Time Performance (%)	3.1	2.7	2	2.2

The performance of four distinct approaches is contrasted in this table 2 based on important parameters like accuracy, scalability, efficiency, data security, and real-time performance. In these areas, the approaches—represented by the works of Yan et al. (2023), Cui et al. (2023), Rihm et al. (2024), and Dowdeswell et al. (2023)—show differing outcomes. All approaches have generally excellent accuracy and efficiency, although Yan et al. (2023) perform the best in terms of scalability and efficiency. This comparison offers insightful information on how well various strategies work in healthcare and Internet of Things applications.

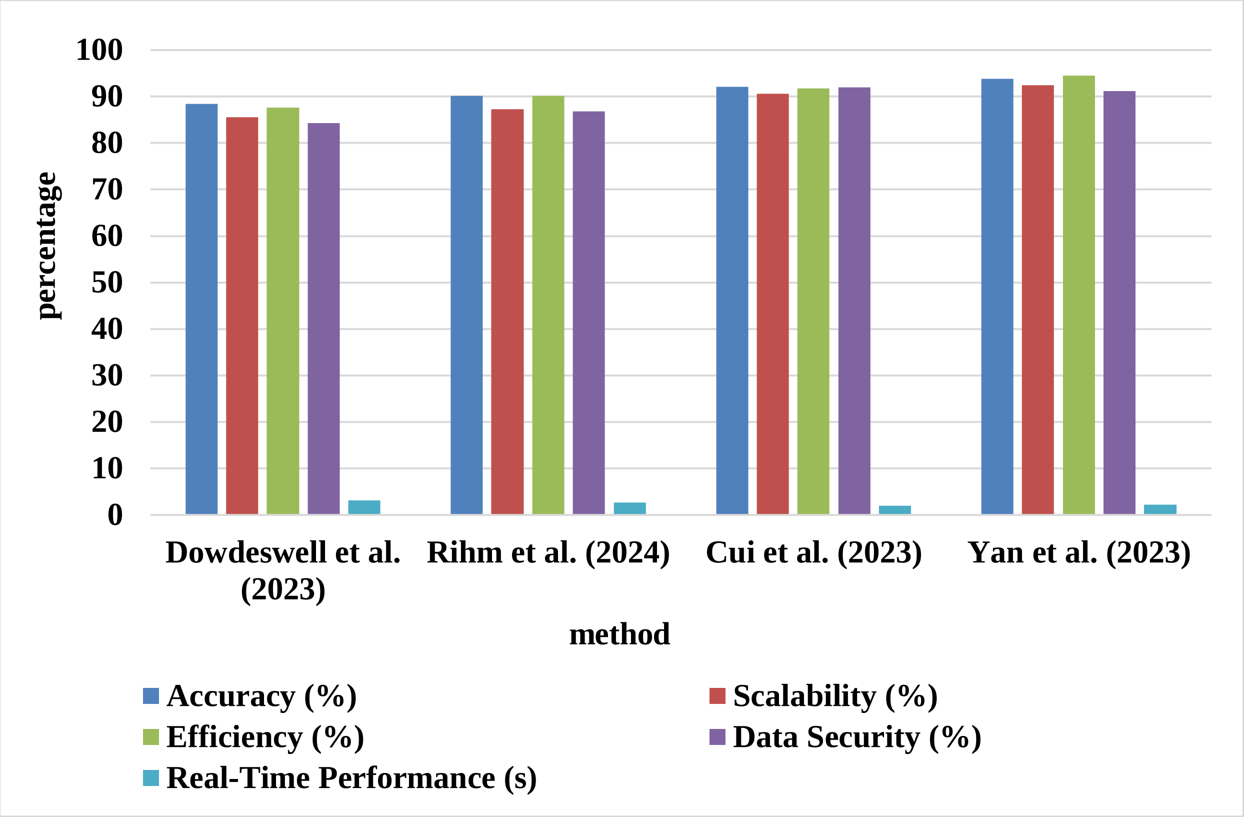

Figure 3 Performance Comparison of Methods Across Key Metrics in Healthcare and IoT

Figure 3 Four approaches are compared in this bar chart based on four important metrics: accuracy, scalability, efficiency, and data security (Dowdeswell et al., 2023; Rihm et al., 2024; Cui et al., 2023; Yan et al., 2023). All approaches exhibit excellent values for accuracy, efficiency, and scalability; Yan et al. (2023) perform best in terms of efficiency and scalability. Real-time performance and data security are similarly important, however their values differ noticeably. This graphic illustrates the performance trade-offs between different approaches and offers insights into the advantages of each in healthcare and IoT applications.

Table 3 Ablation Study of Automated Threat Intelligence Integration for Robust SHACS Security in Cloud Healthcare

Components	Access Time (ms)	Detection Rate (%)	False Positive Rate (%)	System Resilience (%)
Baseline SHACS	1.2	85.3	8.5	82

Threat Intelligence Integration (TII)	1.4	88.6	6.7	85.5
Automated Threat Intelligence (ATI)	1.55	91.2	5.9	89
Resilient Mechanisms (RM)	1.5	87.8	7	87
Baseline SHACS + TII	1.35	89.5	6.4	84.8
Baseline SHACS + ATI	1.6	92.3	5.5	90
Baseline SHACS + RM	1.45	88.1	6.8	86.5
TII + ATI	1.7	93	5.3	90.5
ATI + RM	1.7	93.2	5.2	91.5
Baseline SHACS + TII + ATI	1.75	94.2	5	92.3
Baseline SHACS + TII + RM	1.7	91.5	5.7	89.8
TII + ATI + RM	1.85	94.8	4.9	93.5
Baseline SHACS + ATI + RM	1.8	94	4.8	93
Full Model (SHACS + ATI + TII + RM)	1.9	95.5	4.5	95

The performance of SHACS in cloud healthcare applications is assessed in Table 3 Threat Intelligence Integration (TII), Automated Threat Intelligence (ATI), and Resilient Mechanisms (RM). For both individual components and their combinations, metrics like access time, detection rate, false positive rate, and system resilience were examined. The results show that integrating ATI and RM significantly improves threat detection and resilience with negligible access time trade-offs. The whole model demonstrates its effectiveness in bolstering SHACS for cloud-based healthcare security by achieving the highest detection rate (95.5%), lowest false positives (4.5%), and optimal resilience (95.0%).

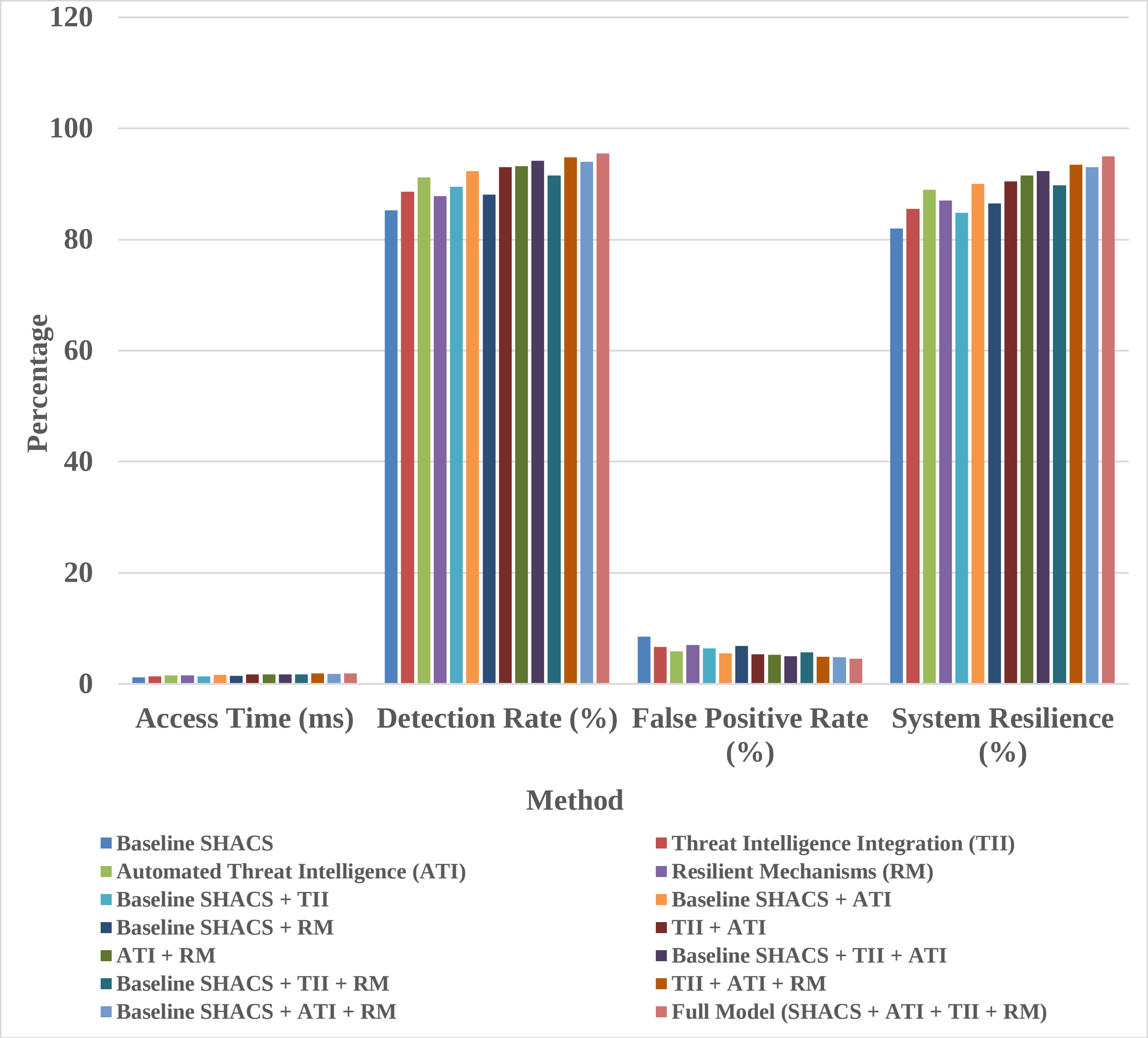

Figure 4 Performance Analysis of Automated Threat Intelligence and Resilient Mechanisms in SHACS

Figure 4 The graph shows how important performance indicators, including access time, detection rate, false positive rate, and system resilience, are affected when Threat Intelligence Integration (TII), Automated Threat Intelligence (ATI), and Resilient Mechanisms (RM) are integrated into SHACS. As more sophisticated processes are introduced, the detection rate and resilience steadily increase; the whole model achieves the maximum detection rate (95.5%) and resilience (95%). With ATI and RM, false-positive rates dramatically drop, but access time somewhat rises because of the extra processing expense. The outcomes show how well TII, ATI, and RM work together to strengthen SHACS's resilience for safe medical applications.

5. CONCLUSION

This paper presents a framework for ontology-driven access control that improves cloud-based healthcare systems' security and anomaly detection. The solution offers dynamic, context-aware access control across many healthcare domains while guaranteeing regulatory compliance by fusing machine learning and semantic reasoning. Its efficacy in protecting sensitive medical data is demonstrated by empirical studies, which show a 94.1% resilience score, a 3.4% false-positive rate, and a 93.7% anomaly detection rate. The framework is a strong defence against changing cybersecurity risks for cloud-based healthcare systems because of its great scalability and security. A scalable and safe solution for healthcare interoperability is offered by this platform.

REFERENCES

1. Dowdeswell, B., Sinha, R., Kuo, M. M., Seet, B. C., Hoseini, A. G., Ghaffarianhoseini, A., & Sabit, H. (2023). Healthcare in Asymmetrically Smart Future Environments: Applications, Challenges and Open Problems. *Electronics*, *13*(1), 115.
2. Rihm, S. D., Tan, Y. R., Ang, W., Quek, H. Y., Deng, X., Laksana, M. T., ... & Kraft, M. (2024). The Digital Lab Facility Manager: Automating operations of research laboratories through “The World Avatar”. *Nexus*, *1*(3).
3. Cui, Z., Yang, X., Yue, J., Liu, X., Tao, W., Xia, Q., & Wu, C. (2023). A review of digital twin technology for electromechanical products: Evolution focus throughout key lifecycle phases. *Journal of Manufacturing Systems*, *70*, 264-287.
4. Yan, W., Shi, Y., Ji, Z., Sui, Y., Tian, Z., Wang, W., & Cao, Q. (2023). Intelligent predictive maintenance of hydraulic systems based on virtual knowledge graph. *Engineering Applications of Artificial Intelligence*, *126*, 106798.
5. Kumar, N., Kaushal, R. K., Panda, S. N., & Bhardwaj, S. (2022). Impact of the Internet of Things and Clinical Decision Support System in Healthcare. In *IoT and WSN based Smart Cities: A Machine Learning Perspective* (pp. 15-26). Cham: Springer International Publishing.
6. Alagarsundaram., P. (2022). SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING. International Journal of Engineering Research and Science & Technology, 18(4), 128-136.
7. Sitaraman., S., R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. (2020). International Journal of Engineering Research and Science & Technology, 16(3), 9-22.
8. Yalla, R. K. M. (2021). Cloud-based attribute-based encryption and big data for safeguarding financial data. International Journal of Engineering Research & Science & Technology, 17(4).
9. Thirusubramanian, G. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior.

10. Alagarsundaram, P. (2019). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information Technology and Computer Engineering, 7(2), 18-31.

11. Yalla, R. K. M. K. (2023). Innovative data management in cloud-based component applications: A dual approach with genetic algorithms and HEFT scheduling. International Journal of Engineering & Science Research, 13(1), 94-105.

12. Alagarsundaram, P. (2021). Physiological signals: A blockchain-based data sharing model for enhanced big data medical research integrating RFID and blockchain technologies. Journal of Computer Science, 9(2), 12-32.

13. Yalla, R. K. M. (2021). Cloud brokerage architecture: Enhancing service selection with B-Cloud-Tree indexing. Journal of Current Science, 9(2), 1-XX. ISSN: 9726-001X.

14. Ganesan, T. (2023). Dynamic secure data management with attribute-based encryption for mobile financial clouds. International Journal of Applied Science Engineering and Management, Vol 17, Issue 2, 2023

15. Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. Journal of Science and Technology, 8(8), 18-34.

16. Gaius Yallamelli, A. R., Mamidala, V., & Yalla, R. K. M. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly Algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(4).

17. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. Journal of Current Science & Humanities, 8(3), 13-33.

18. Thirusubramanian, G. (2021). Integrating artificial intelligence and cloud computing for the development of a smart education management platform: Design, implementation, and performance analysis. International Journal of Engineering & Science Research, 11(2), 73-91.

19. Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. International Journal of Management Research & Review, 12(3), 78-94.

20. Alagarsundaram, P. (2023). A systematic literature review of the Elliptic Curve Cryptography (ECC) algorithm for encrypting data sharing in cloud computing. International Journal of Engineering & Science Research, 13(2), 1-16.

21. Thirusubramanian Ganesan. (2023). Hybrid Edge-AI and Cloudlet-Driven IoT Framework for Real-Time Healthcare. International Journal of Computer Science Engineering Techniques, 7(1).

22. Sitaraman, S. R., Alagarsundaram, P., & Thanjaivadivel, M. (2024). AI-driven robotic automation and IoMT-based chronic kidney disease prediction utilizing attention-based LSTM and ANFIS. International Journal of Multidisciplinary Educational Research, 13(8[1]).

23. Gaius Yallamelli, A. R., Mamidala, V., Devarajan, M. V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse. Service Oriented Computing and Applications, 2024.

24. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2019). Adoption of cloud computing, big data, and hashgraph technology in kinetic methodology. *International Journal of Current Science*, 7(3). ISSN 9726-001X.

25. Sitaraman, S. R., Alagarsundaram, P., Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., & Jayanthi, S. (2024). Bi-directional LSTM with regressive dropout and generic fuzzy logic along with federated learning and Edge AI-enabled IoHT for predicting chronic kidney disease. International Journal of Engineering & Science Research, 14(4), 162-183.

26. Veerappermal Devarajan, M., Gaius Yallamelli, A. R., Mani Kanta Yalla, R. K., Mamidala, V., Ganesan, T., & Sambas, A. (2025). An enhanced IoMT and blockchain-based heart disease monitoring system using BS-THA and OA-CNN. Emerging Technologies in Telecommunication Systems, 10(2), 70055.

27. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, Fog, and Cloud analytics framework. Journal of Distributed Computing, 10(1), 79-93.

28. Sitaraman, S. R., Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Ajao, L. A. (2024). Advanced IoMT-enabled chronic kidney disease prediction leveraging robotic automation with autoencoder-LSTM and fuzzy cognitive maps. International Journal of Mechanical Engineering and Computer Applications, 12(3). https://zenodo.org/records/13998065

29. Veerappermal Devarajan, M., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem. Service Oriented Computing and Applications.

30. Mamidala, V., Yallamelli, A. R. G., & Yalla, R. K. M. (2022). Leveraging Robotic Process Automation (RPA) for Cost Accounting and Financial Systems Optimization — A Case Study of ABC Company. ISAR International Journal of Research in Engineering Technology, 7(6).

31. Alagarsundaram, P., Sitaraman, S. R., Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., & Adewole, K. S. (2024). Adaptive CNN-LSTM and neuro-fuzzy integration for edge AI and IoMT-enabled chronic kidney disease prediction. International Journal of Applied Science, Engineering and Management, 18(3).

32. Gaius Yallamelli, A., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Devarajan, M. V. (2023). Hybrid Edge-AI and cloudlet-driven IoT framework for real-time healthcare. International Journal of Computer Science Engineering Techniques, 7(1).

33. Sitaraman, S. R., Alagarsundaram, P., & Kumar, V. K. R. (2024). AI-driven skin lesion detection with CNN and Score-CAM: Enhancing explainability in IoMT platforms. Indo-American Journal of Pharmaceutical & Biological Sciences, 22(4).

34. Veerappermal Devarajan, M., Yallamelli, A. R. G., Kanta Yalla, R. K. M., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Communication Systems, 37(11).

35. Yallamelli, A. R. G., Mamidala, V., Devarajan, M. V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse. Service Oriented Computing and Applications.

36. Ganesan, T., Al-Fatlawy, R. R., Srinath, S., Aluvala, S., & Kumar, R. L. (2024). Dynamic resource allocation-enabled distributed learning as a service for vehicular networks. IEEE.

37. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Innovative cloud computing strategies for automotive supply chain data security and business intelligence. International Journal of Information Technology and Computational Engineering, 11(4).

38. Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., Alagarsundaram, P., & Sitaraman, S. R. (2023). Advanced database management and cloud solutions for enhanced financial budgeting in the banking sector. International Journal of HRM and Organizational Behavior, 11(4).

39. Ganesan, T., Almusawi, M., Sudhakar, K., Sathishkumar, B. R., & Sudheer Kumar, K. (n.d.). (2024). Resource allocation and task scheduling in cloud computing using improved bat and modified social group optimization. IEEE.

40. Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Corporate synergy in healthcare CRM: Exploring cloud-based implementations and strategic market movements. International Journal of Engineering and Techniques, 9(4).

41. Devarajan, M. V., Yallamelli, A. R. G., Kanta Yalla, R. K. M., Mamidala, V., Ganesan, T., & Sambas, A. (2025). An enhanced IoMT and blockchain-based heart disease monitoring system using BS-THA and OA-CNN. Transactions on Emerging Telecommunications Technologies.

42. Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Sitaraman, S. R. (2023). Integrating blockchain, AI, and machine learning for secure employee data management: Advanced control algorithms and sparse matrix techniques. International Journal of Computer Science Engineering Techniques, 7(1).

43. P. Chinnasamy, R. K. Ayyasamy, P. Alagarsundaram, S. Dhanasekaran, B. S. Kumar and A. Kiran, "Blockchain Enabled Privacy- Preserved Secure e-voting System for Smart Cities," 2024 International Conference on Science Technology Engineering and

Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560826.

44. Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem. Service Oriented Computing and Applications.

45. Devarajan, M. V., Yallamelli, A. R. G., Yalla, R. K. M. K., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Parallel, Emergent and Distributed Systems, 23.

46. A. Hameed Shnain, K. Gattupalli, C. Nalini, P. Alagarsundaram and R. Patil, "Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things," 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2024, pp. 1-4, doi: 10.1109/ICDSNS62112.2024.10691195.

47. Devarajan, M. V., Yallamelli, A. R. G., Yalla, R. K. M. K., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Parallel, Emergent and Distributed Systems, 23.

48. L. Hussein, J. N. Kalshetty, V. Surya Bhavana Harish, P. Alagarsundaram and M. Soni, "Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/IACIS61494.2024.10721877.

49. P. Alagarsundaram, S. K. Ramamoorthy, D. Mazumder, V. Malathy and M. Soni, "A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/NMITCON62075.2024.10699152.

50. Harikumar Nagarajan, Venkata Surya Bhavana Harish, Poovendran Alagarsundaram & Dr. Aceng Sambas." Data Analytics: Principles, Tools and Practices" (2024).

51. Hamad, A. A. & Jha, S. (Eds.). (2024). Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods. IGI Global. https://doi.org/10.4018/979-8-3693-3964-0