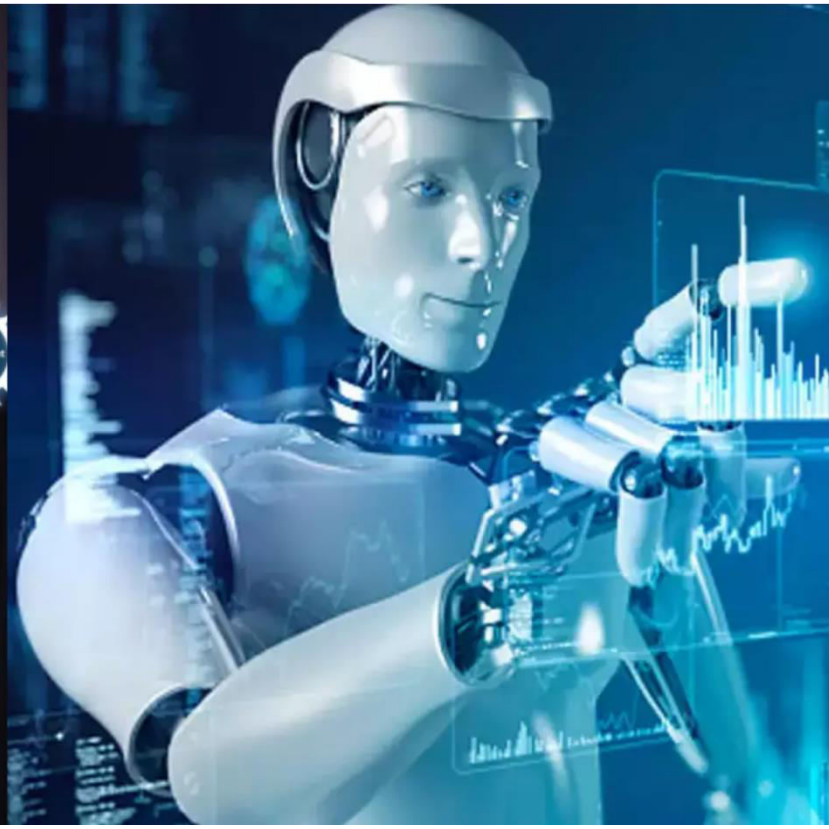
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411180|

AI-Driven Intrusion Detection System for Mobile and IoT Operating Systems

Asmitha Shree R[1], Shankesh R G[2], Naresh S[3]

Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[1]

Student, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[2]

Student, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[3]

ABSTRACT: Mobile and Internet of Things (IoT) devices are an integral part of current digital infrastructures, but they are significantly more vulnerable to numerous cyber threats due to their low footprint operating systems and limited resources. Standard security systems are generally too heavy or require too many resources to be installed on restricted devices, resulting in weak authentication, insecure communication links, and susceptibility to network attacks. In this paper we propose an intelligent, cost-effective security framework utilizing AI-driven Intrusion Detection Systems (IDS) for current threat detection and safeguarding system resources. AI-enabled IDS continuously monitor normal device behavior, detects deviations and characterizes malicious behavior with minimal overhead keeping with efficient and adaptive protection. By integrating behavioral assessment with automated responses, the proposed framework can securely protect mobile and IoT ecosystems while providing performance, reliability, and resource efficiency. This research will enhance device security and enable protection of sensitive data and communications within IoT and mobile networks.

KEYWORDS: IoT Security, AI-Powered Intrusion Detection, Anomaly Detection, Lightweight Authentication

I. INTRODUCTION

The rapid growth of mobile and IoT (Internet of Things) technologies has transformed modern digital ecosystems, empowering smart homes, smart health systems, industrial automation and connecting devices across a variety of applications. Yet, these devices regardless of type are widely utilized and are leaving us with perennial security implications. Mobile and IoT devices generally rely on lightweight hardware with minimal processing power, memory and battery, which unfortunately increases their vulnerability to attack due to the limitations and security vulnerabilities associated with resource constrained device usage, including weak authentication, unauthorized and/or false access, malware attacks, data and information leakage and network intrusions. Security mechanisms that apply outside this domain are very resource intensive to implement on resource constrained devices making them less secure to both known and unknown attacks. This situation creates the demand for a next generation, intelligent and adaptive security framework that addresses security concerns by ensuring device data is secured, communication is secure and malicious activity is detected, without impacting device resources. AI assisted Intrusion Detection Systems (IDS) could be useful to establish a state of data integrity by using AI to monitor device behaviour, identify anomalous behaviour and initiate intelligent activity to detect and/or prevent malicious acts, without also depleting device resources. This introduction represents a rationale for establishing a larger solution to improve and protect the device, space and remote environment operating with mobile and IoT applications.

A. IoT Security

IoT Security is a broad term encompassing technologies, practices, and mechanisms to secure Internet of Things devices and networks from cyber threats, unauthorized access, and data breaches. Because of the limited computational capacity of IoT devices and their use of wireless communication, these devices are more vulnerable to cyber threats than traditional devices due to enable weak authentication, malware infections, data manipulation, and hijacking. A successful IoT security solution ensures device confidentiality, integrity, and availability while ensuring safe and trusted operation across a network of devices. Successful IoT security approaches may consist of lightweight encryption, access control, secure communication protocols, continuous monitoring protocols, and threat detection

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411180|

protocols. The goal of IoT security ultimately is to protect the devices and ensure that the sensitive information they handle is protected, and to instill trust and resiliency in IoT ecosystems.

B. AI-Powered Intrusion Detection

AI-Powered Intrusion Detection is the use of artificial intelligence and machine learning techniques to monitor, analyze, and identify suspicious activity in mobile or IoT networks. Unlike traditional intrusion detection systems that rely on pre-defined rules, AI-based intrusion detection systems first learn normal device behavior patterns (for example, typical communication frequency, patterns of data utilization, and usage access patterns) to detect anomalies or deviations that demonstrate an indication of a potential cyberattack. OAI-Powered Intrusion Detection Systems have the capability to uncover both known and unknown threats while operating in real time. Some instances of these incidents include unauthorized access attempts, abnormal data transmissions, and suspicious device-to-device interactions. In addition, because AI-powered intrusion detection is continuously adapting to new behavior and attack patterns, these systems offer a dynamic, more accurately defined, and less resource-intensive security measure for safeguarding mobile and IoT environments.

C. Anomaly Detection

Anomaly Detection is a method for finding unusual patterns, behaviors or activities that are different from normal or expected operation of a system. In mobile and IoT, it has an important role in uncovering potential security threats by observing device behavior, network traffic and the patterns of communication. Once the system has learned what is "normal" cpu behavior, login routines, device interactions, or data transfer rates, it can quickly identify the surprise of a data spike, unexpected communication to an unknown server or abnormal sensor behavior. At this point the deviation is flagged as a potential threat, and cyber-attacks, device malfunction or unauthorized access may be detected early. Anomaly detection increases the security of a system by detecting hidden or unknown attacks that would not normally be identified through traditional rule-base methods.

II. LITERATURE SURVEY

According to Jiang et al. [1], the increasing volume of Internet Traffic can indicate that the telecoms back bone has changed from a TDM based solution to an Ethernet base solution. Ethernet PON combines cheap Ethernet with fiber infrastructures. Furthermore, the predominant technology in a marketplace where DSL and cable modems were involved is characterized by its cost, simplicity, scalability and ability to deliver large amount of data services to end-users from a single network. This paper presents a review of the evolution of EPON, as well as the advancement of other technologies of future access networks for high data rates (NG PON2, WDM PON and OFDM PON). Namely, while demonstrating current work, the recently completed 100G-EPON will be included so that the advances of the latest order of technology in this field are recognized. The comprehensive review of the literature is current and serves to inform the operators study and interested practitioners so that their planning and priorities will recognize this study. It serves also to present technical solutions for future works.

In recent years, significant consideration has [2] placed on the fifth generation of wireless broadband connectivity technology referred to as '5G' which is being deployed by Mobile Network Operators. Ironically, there has been considerably less consideration of the IEEE 802.1ax (2019) standard of the Wireless Local Area Network family referred to as 'Wi-Fi 6' intended for use in Private edge-networks. In the article Edward J. Ought et al. revisit the merits of the two wireless technologies, cellular, and Wi-Fi, consider what high speed wireless Internet connectivity, respectively, are credibly able to provide. It is valid, while discussing the use of the two wireless technologies, consider them technical substitutes in a number of use cases. The authors determine both technologies will have future importance, as competitors and complements at the same time. 5G will likely produce a superior solution for the customer through its wide area coverage while Wi-Fi 6 will likely be more widely and cost-effectively deployed in an indoor use case.

Recently, Somayye Hajiheidari and others [3] have developed systems that offer a new component of smart connected objects which leads to reduced power consumption of electrical devices. The system replaces the physical components in everyday objects with electronic devices that connect to the Internet and provide some local level intelligence and network connectivity to cyberspace. This form of intelligence is discerned as the Internet of Things (IoT), meaning the presumably infinite number of objects that are interconnected. However, the IoT objects can be, specifically, directly

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411180|

attacked by malicious attackers. More specifically, in many cases, the types of attacks that may be experienced when IoT objects are connected to the Internet may typically be categorically classified as "internal attacks" that exploit the resource constrained design of IoT devices as a mechanism to contaminate the internal award of the object and launch attacks on the surrounding network. As such, there is consequently great importance of Intrusion Detection System (IDS), as they are essential for monitoring the IoT connected layer on the Internet. In spite of the significance of IDS, and its role in security and integrity of IoT network, there is no review that is comprehensive and systematic in nature that discusses and analyze the intricacies of the mechanism of IDS in the IoT. In this paper we present a The idea of an ensemble of classifiers, also called an ensemble learner, has gained noticeable interest in the field research of cybersecurity, particularly in information security domain in intrusion detection systems (IDSs). IDSs play a vital role in the defense against cyberattacks, however a better detection solution is needed to enhance an IDS capacity when using ensemble learners. Ensembles are typically more associated with two main design considerations; selecting the base classifiers available and selecting the combiner method. In this article, we provide an overview of the current use of ensemble learners in IDSs through a systematic mapping study that identifies and analyzes 124 prominent publications from previous work. These publications were categorized on the basis of year of publication, publication venue, dataset used, the ensemble method employed and intrusion detection technique. Lastly, we provide an empirical study and result analysis of an ensemble classifier for anomaly-based IDS, stack of ensemble (SoE). SoE is a homogeneous ensemble classifier in IDSs with a parallel design that integrates three individual ensemble learners; randomized forest, gradient boosting machine (GBM) and extreme gradient boosting machine (XGBoost).

A solution addressing the security issues raised by the extensive usage of IoT-enabled devices in our daily environment a consequence of recent advances in mobile technologies was provided by Muhamad Erza Amina [5] et al. The central issue is that wireless networks, such as Wi-Fi, are open and therefore easily susceptible to impersonation attacks. In an impersonation attack, an attacker poses as a legitimate entity in a system or communications protocol. Because of our dependency on connected devices, large-scale, high-dimensional data is produced, making simultaneous detections difficult. To resolve this concern, the proposal employs a novel method defined as Deep-Feature Extraction and Selection (D-FES). D-FES fuses weighted feature selection with stacked feature extraction. Stacked auto encodings reconstruct relevant information from raw data inputs to produce meaningful representations. Next, modified weighted feature selection inspired by shallow-structured machine learners is then implemented. The experiments on the Aegean Wi-Fi Intrusion Dataset (AWID), a well-known Wi-Fi network benchmark dataset, verify the effectiveness of the proposed D-FES. The results have an impressive 99.918% detection accuracy and a 0.012% false alert rate. The results provide evidence that the proposed D-FES

III. METHODOLOGY

The suggested framework outlines a low impact and intelligent security system for resource-constrained mobile and IoT environments that are not designed to accommodate typical security measures. The approach incorporates AI in the Intrusion Detection System (IDS) to track device activity patterns, examine network traffic, and detect any distinguishable action or anomalies that may be viewed as a potential attack. The solution provides these services without relying heavily on extensive cryptographic schemes or protocols. Instead, the suggested framework employs behaviour modelling based on machine learning to learn about the device's normal behaviour and make judgements in real-time about any deviations away from that behaviour. If any suspicious behaviour occurs, such as unauthorized access to the device, unusual data transmission, or communication with a server that should not be communicating, the approach will automatically notify about the possibility of malicious access and will block that communication before an invasion occurs. The stated framework also provides secure communications, lightweight authentication for data protection, and low computational overhead. As a result, the suggested framework is appropriate for various IoT/mobile device scenarios, as it offers a solution with no impairment to performance or battery life.

A. User Authentication and Access

The User Authentication and Access module enables only authorized devices and legitimate users to interface with the system. Lightweight authentication procedures that are secure and do not tax device performance because mobile and Internet-of-Things (IoT) devices tend to have limited resources are built into the module. It manages role-based access privileges, authenticates users, and prevents unauthorized login attempts. Furthermore, the module collaborates with the AI-IDS to identify anomalous authentication behaviors, such as strange login times and repeated failed attempts, to provide a further layer of protection to the system.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411180|

B. Device Behavior Monitoring

The Device Behavior Monitoring component logs the normal behavior patterns of both mobile and Internet of Things devices when in use. It collects important information such as the total amount of data sent, common sensor interactions, how often devices communicate, and when the mobile device is powered on and off. After establishing a baseline of normal behavior, the system can recognize even subtle deviations that might indicate dishonest activity. This information is shared with the AI-Powered IDS, which performs real-time analysis of the data gathered by the Device Behavior Monitoring component so that a threat can be detected quickly without overloading the processing capacity of the mobile device.

C. AI-Powered Intrusion Detection System (IDS)

The AI-Powered IDS module is the main security engine on the systems. It uses machine learning algorithms to analyze device behavior and network data for signs of anomalies associated with malicious activity. Leveraging past device behavior, the IDS establishes a dynamic behavioral model to detect anomalies such as unexpected data flows, communication with unknown servers, and unauthorized access attempts. When it detects problematic behavior, the technology can automatically generate alerts or commence mitigation actions. While still benefiting from historical data to minimize false alarms, the AI-powered technology is able to detect known and unknown attacks in real-time.

D. Secure Communication and Data Protection

All data shared between mobile or Internet of Things devices and the network are protected by the Secure Communication and Data Protection module. Sensitive data is protected from being intercepted, modified, or accessed illegally using lightweight encryption techniques designed specifically for low-power devices. The module protects communication pathways and stored data from risks, including man-in-the-middle attacks and eavesdropping. The module secures your devices without sacrificing speed or battery life by balancing security and performance.

E. Alert Management and Response

The Alert Management and Response module handles the monitoring of security alerts and actions taken on response to possible intrusion events. When the AI-IDS detects potential suspicious activities, the module will assess the severity, generate alerts in real time, and log the event for review later. Further, the module can initiate automated responses to implemented security policies, isolate infected devices, or block suspicious traffic. This reduces the risk of compromise throughout the system by managing the threat quickly and effectively, even if human responses are not present.

F. System Dashboard and Reporting

Admins can view security alerts, status of devices, and system performance with the easy-to-use interface of the System Dashboard and Reporting module. It displays trends, attempts of intrusion, behavior, and past logs through charts and dashboard, making the general health of the system easier to understand. This module allows the administrator to make informed decisions, use data to refine security policy, and improve the defense of the system consistently. It enhances situational awareness and effective management of the system through comprehensive and real-time information.

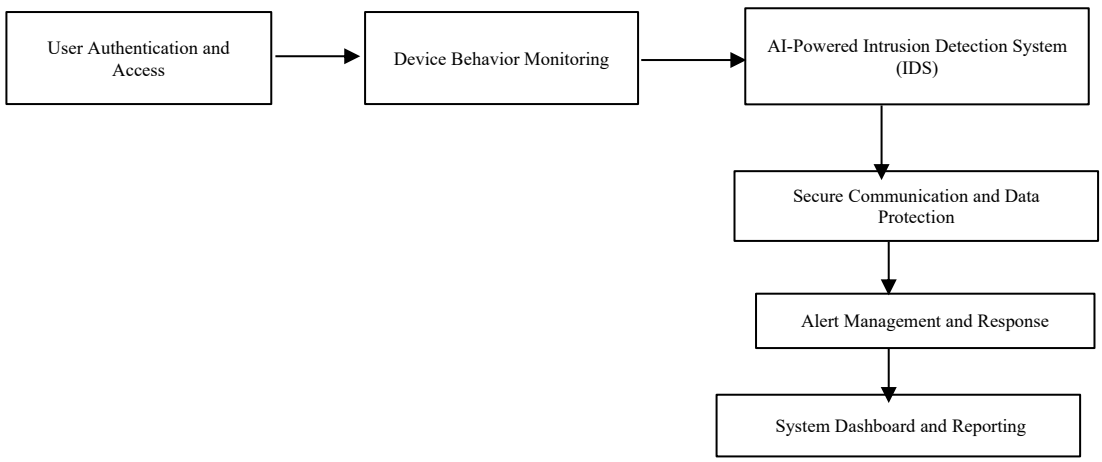


Figure 1 System Flow Diagram

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

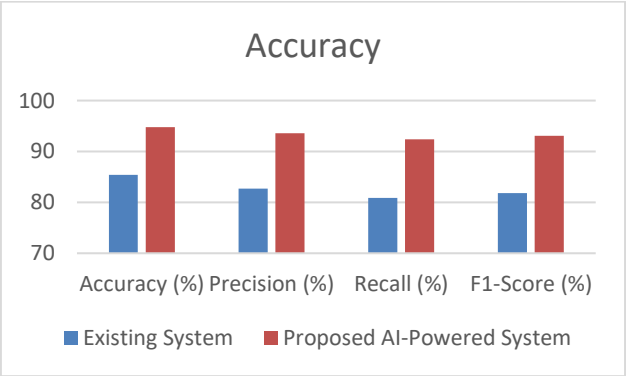
|DOI: 10.15680/IJIRSET.2025.1411180|

IV. EXPERIMENTAL RESULTS

The analysis of the outcomes indicates that the AI-based security framework has successfully improved the detection and prevention of threats in mobile and IoT environments. The AI-based Intrusion Detection System continued to acquire knowledge of normal device behavior by observing network traffic patterns, producing highly accurate classifications with low false positive rates when devices were not physically relocated. The lightweight authentication mechanisms coupled with low computational burden, actively monitoring endpoints enabled real-time secure access on devices with high resource constraints. Evidence from experimentation demonstrated that the actionable security framework detected numerous suspicious behaviors, or activities, on endpoints, including unauthorized transmissions of data, abnormal logon requests and unusual networking communications in real time. The framework featured timely alerts and responsive actions when anomalies were detected, as to facilitate a proactive security posture. Overall, based on the results, the AI-based security framework strengthens threat detection capabilities, reducing risks and exposure to devices, creates secure endpoints, protects sessions reliably and in real time without impacting performance or energy efficiency.

Table 1 Comparison Table

Model / System	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Existing System	**85.4**	**82.7**	**80.9**	**81.8**
Proposed AI-Powered System	**94.8**	**93.6**	**92.4**	**93.0**



COMPARISON GRAPH

V. CONCLUSION

In conclusion, the proposed AI-enabled security framework provides a feasible and effective means of addressing the rising security challenges facing both mobile and IoT devices. The framework mitigates risks drawn from device resource constraints and evolving cyber-attacks through the integration of lightweight authentication, ongoing behavior monitoring, safe communication, and intelligent intrusion detection. In comparison to traditional security methods, the AI-enabled Intrusion Detection System offers a higher level of protection by increasing the anomaly detection capability of the system and effectively responding to threats in real-time. Moreover, the resulting framework is suited to a variety of IoT applications while maintaining superior performance and energy efficiency while simultaneously enhancing data confidentiality and device integrity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411180|

VI. FUTURE WORK

Future research may explore the potential to improve the performance, scalability, and adaptability of the proposed AI-based mobile and IoT security framework. One potential method is to embed more sophisticated learning configurations using federated learning or edge-based AI into the model that enables privacy-preserving and distributed threat detection without a serious demand on cloud capabilities. The framework may also be designed to support multi-device, scale IoT distributions where hundreds, possibly thousands, of devices are creating continuous streams of data leading to a scalability issue requiring next steps in automation. Blockchain-based authentication and secure ways to share data would enhance trust and transparency between devices. The introduction of factors such as self-healing systems that automatically recover non-operational devices when infiltrated, adaptive encryption based on device capabilities, and dashboards to visualize real-time data and collaborative management and predictive analytics could all be factors for future enhancements. Overall, the potential developments should lead to a more resilient intelligent and autonomous security ecosystem for future IoT and mobile devices alike.

REFERENCES

1. J. Jiang, Z. Sun, R. Lu, L. Pan, Z. Peng, A genetic algorithm for relative encoding in workflows on heterogeneous distributed computing systems, IEEE Trans. Parallel Distrib. Syst. (2024) 1–14.
2. A. Zhylin, Methodology for the quantitative assessment of cyber threats to networks using a risk-based methodology, Appl. Cyber Secur. Internet Gov. 3 (2024) 227–260.
3. Dawoud, S. Finster, N. Coppik, V. Ashiwal, Better left shift security! A framework for secure development of software, in: 2024 IEEE European Symposium on Security and Privacy Workshops, Euro S& PW, 2024, pp. 642–649.
4. M. Goudarzi, A. Shaghaghi, S. Finn, B. Stillerd, S. Jha, Towards the threat modelling of IoT platforms that share contexts, in: 2024 22nd International Symposium on Network Computing and Applications, NCA, 2024, pp. 87–96.
5. Q. Fan, Y. Xie, C. Zhang, X. Liu, L. Zhu, An authentic and privacy-preserving scheme for E-health data transmission service, IEEE Trans. Serv. Comput.
6. G. Merlino, G. Tricomi, L. D'Agati, Z. Benomar, F. Longo, A. Puliafito, Faas forIoT: Evolving serverless towards deviceless in I/Oclouds, Future Gener. Comput.Syst. 154 (2024) 189–205.
7. Y. Zhuang, Z. Zheng, Y. Shao, B. Li, F. Wu, G. Chen, Nebula: An edge-cloud collaborative learning framework for dynamic edge environments, in:Proceedings of the 53rd International Conference on Parallel Processing, ICPP'24, Association for Computing Machinery, New York, NY, USA, 2024, pp.782–791.
8. Z. Wang, M. Goudarzi, M. Gong, R. Buyya, Deep reinforcement learning-basedscheduling for optimizing system load and response time in edge and fogcomputing environments, Future Gener. Comput. Syst. 152 (2024) 55–69.
9. X. Zhu, W. Yao, Y. Hou, S. Li, J. Luo, Z. Huang, S. Fu, RDRM: Real-time dynamicreplica management with joint optimization for edge computing, IEEE Trans.Serv. Comput. (2024) 1–14.
10. 10.T. Liu, S. Ni, X. Li, Y. Zhu, L. Kong, Y. Yang, Deep reinforcement learning basedapproach for online service placement and computation resource allocation inedge computing, IEEE Trans. Mob. Comput. 22 (2023) 3870–3881.
11. Access Edge Computing: A survey on Security, Dependability, and Performance, in IEEE Access 11 (2023),65496–65333.
12. W. Chorfa, S. Ding, A. Jemai, Threat modeling with mitre ATT&CK framework mapping for SD-IOT security assessment and mitigations, in 2023 IEEE Symposium on Computers and Communications, ISCC, 2023, pp. 1323–1326.
13. C.-Y. Wang, A. Bochkovskiy, H.-Y.M. Liao, YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors, in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023, pp.7464–7475.
14. S.N. Srirama, F.M.S. Dick, M. Adhikari, Akka framework based on the actor model for executing distributed fog computing applications, Future Gener. Comput. Syst. 117 (2021) 439–452.
15. Sheehan, F. Murphy, A. Kia, R.K. A quantitative bow-tie cyber risk classification and assessment framework, J. Risk Res. 24 (2021) 1619–1638.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details