Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Review Of Intrusion Detection System Architectures in IoT-WSN Network

Sara Mahdi Abboud

Computer Science Department, College of Computer Science and Information Technology, University of AL- Qadisiyah, Iraq. com21.post6@qu.edu.iq

ARTICLE INFO

Article history:
Received: 23 /01/2026
Rrevised form: 20 /02/2026
Accepted : 22 /02/2026
Available online: 30 /06/2026

Keywords:

Intrusion detection system; anomaly detection; signature-based detection; IoT security; WSN

ABSTRACT

The rapid evolution of the Internet and the increased reliance on computerized services have exacerbated concerns about security, privacy, and confidentiality. Intrusion Detection Systems (IDSs) work with preventive controls by monitoring hosts and network traffic for suspicious activities or policy violations, and reporting alerts to operators or SIEM platforms. This work explores the deployment model (host-based vs. network-based) and the application domain (web applications, cloud environments, Internet of Things, wireless sensor networks, mobile ad hoc networks, and Voice over IP). We review representative research topics (e.g., alert reduction, honeypot-aided detection, botnet command-and-control discovery, SDN/OpenFlow-based IDS, and hybrid cloud-based IDS architecture), and summarize evaluation caveats such as the false positives/false negatives trade-off, data/feature bias, and resource-overhead challenges. 2.p4p3 Recommendations The paper offers some recommendations for aligning IDS design to threat models and deployment realities.

https://doi.org/10.29304/jqcsm.2026.18.22605

∗Corresponding author

Email addresses:

Communicated by ‘sub etitor’

1. Introduction

Network computing enables the sharing of resources at large scale, but it also increases the scope of attacks. Insiders (authorized entities making unethical use of privileges) or outsiders (unauthorized actors) may launch active (altering system resources) or passive attacks, which involve tampering with system resources or capturing information without altering any resource [1][2]. The paper being surveyed also stresses that there is no system that is absolutely secure and that vulnerabilities can be identified in hardware and software [3]. Intrusion detection is defined as the act of detecting activities that seek to "violate the security policy of an information system" by attempting to escape the information system's policies on confidentiality, integrity, or availability [4]. As it happens, IDSes can observe network devices or more complex conglomerations, such as hosted systems and those running in the cloud, reporting alarms to administrators or to centralized SIEMs that match alerts to filter out potentially false positives. IDSs differ from firewalls; firewalls control access between networks to prevent unauthorized users from accessing the network, while IDSs focus on identifying and detecting suspicious activities within observed traffic [5] [6].

Fast proliferation of networked computing and digital services has exposed individuals, businesses, and vital systems to increased risks associated with security, privacy, and confidentiality as adversaries continue to take advantage of active attacks such as tampering, which entail the alteration of resources or passive attacks in the form of eavesdropping, whereby the stored data is captured unobtrusively by attackers [7]. In this context, Intrusion Detection Systems (IDS) are considered as a key component of defense-in-depth strategy; the goal is to detect attempts to breach confidentiality, integrity, and/or availability of assets whereas an IDS is defined as "a device or software application that monitors host or network activities for malicious behavior or policy violations" and can produce alerts [8]. Compared with firewalls, which mainly control inter-network access to prevent intrusion, IDS monitors and detects traffic and system behavior, often combined with Security Information and Event Management (SIEM) to filter alarms and reduce false positives [9]. The research presented in this paper is a successor of survey-based taxonomies that characterize IDS based on detection logic notably anomaly, learning baselines developed from normal data and raise alarms on deviation to expose unknown attacks and misuse (signature), comparing activity with known attack signatures; and by deployment locus grouping host-based, and network based IDS according to where they are placed hence the evidence provided and the operational costs entailed[10][11]. With these underpinnings in mind, this paper discusses IDS design aspects across the different deployment settings identified by the survey—web apps, cloud computing, and so on—at a high level, to understand how threat models and resource limitations shape detection choices and evaluation focus [12][13]. This is because the effectiveness of IDS does not rely solely on its ability to detect, but also on how false alarms and alert density are managed; thus, context-friendly architectures and alarm filtering are necessary for operational survival. We therefore posit that hybrid IDS architectures employing a combination of anomaly-based and signature-based detection, leveraging centralized alert filtering, will produce more operationally useful security results than monolithic single-method IDS, where the goal is to maintain sensitivity to the unknown threat while at the same time preserving precision in recognizing confirmed attack patterns.

NOMENCLATURE

Aradius of

Bposition of

Cfurther nomenclature continues down the page inside the text box

2. Types of IDS by Detection Logic

The restructured survey categorizes IDSs into two basic detection logics: anomaly- and misuse (signature)-based, which differ in their assumptions about normality and the representations used to characterize attacks; as a result, differences in efficiency in detecting unseen threats can be observed.

2.1 Anomaly recognition

Within the system, anomaly-based IDS characterizes "normal" user or system behavior (either manually or automatically) and detects deviations from the profile as potentially hazardous. An important advantage is the ability to identify previously unknown attacks and insider misuse, as anomalies can expose activities that deviate from the established profile or pattern of normalcy [14]. Nevertheless, anomaly-based IDSs may yield high false alarm rates when normal behavior evolves or when profiles are incomplete [15].

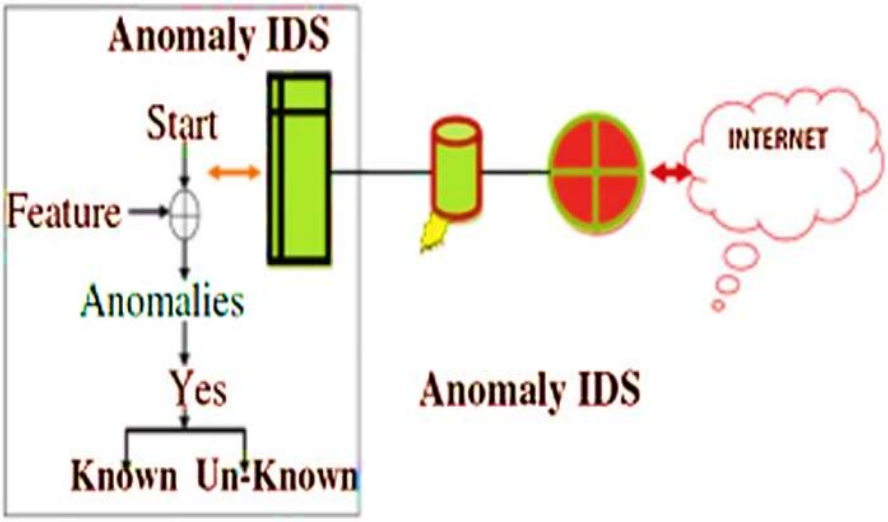

Fig 1 Anomaly Recognition [16].

2.2 Misuse (signature) recognition

Alerts are generated when known attack signatures match observations. For known threats, it is accurate and explainable, as reports are explicitly matched against rules. However, some drawbacks include a lack of protection against new attacks and the need to constantly update signature databases [17] [18].

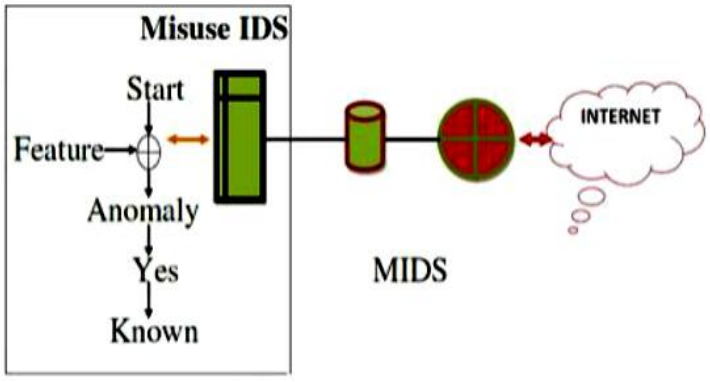

Fig 2 Misuse Recognition [19].

2.3 Specification-based detection

Specification-based IDS identifies intrusions by comparing observed behaviour to a given explicit specification of acceptable behaviour (e.g. protocol state machines, time constraints, and legal command sequences). In contrast to misuse logic, it does not assume that one is aware of certain attacks, and unlike anomaly logic, it does not learn a baseline using data; it simply indicates any violation of formally specified rules. Such reasoning is especially applicable when using an IoT-WSN with predictable node behavior (periodic sensing and reporting) and whose duty cycle and routing constraints can be explicitly defined. Nevertheless, such a level of specification accuracy is a must: a very strict specification can result in false alarms, whereas a very loose specification can fail to detect stealthy attacks.

2.4 Hybrid Detection Logic

Hybrid IDS combines two or more detection logics to compensate for the weaknesses of any single approach. One typical architecture is a two-stage pipeline in which anomaly (or specification) detection flags are sent through signature validation to verify the presence of known attacks; the other architecture performs concurrent detection and combines the results using voting or weighted confidence scores. Despite the increased complexity of design and perhaps the overhead of a hybrid system, they tend to enhance overall detection coverage and minimize fatigue during alert operations by cross-validating the various evidence pieces.

2.5 Design Considerations and Comparison

Deployment-wise, signature-based IDS is more likely to reduce false positives, but only for threats already listed in the catalog, whereas anomaly-based IDS has a broader scope at the expense of a higher false-alarm rate and is sensitive to baseline changes. In well-defined protocol behavior and duty cycles, specification-based IDS can offer a compromise to the IoT-WSN case; however, it necessitates rule engineering and maintenance. Hybrid designs are thus becoming increasingly popular for high-precision signatures and for anomaly or specification detection, providing early warnings and zero-day protection. Resource constraints also dictate this logic choice in the IoT-WSN network: lightweight checks can be run on sensor nodes, whereas more computationally intensive learning and correlation should be offloaded to edge gateways or the cloud.

3. IDS by Deployment Locus

IDS may also be classified by where monitoring occurs: host-based IDS (HIDS) and network-based IDS (NIDS). Placement influences observable evidence, confidence about attack success, and system overhead.

3.1 Host-based IDS (HIDS)

HIDS examine host-level residue, including system calls and log files, allow for detailed diagnosis, and usually provide stronger evidence as to whether an attack was successful [20]. The trade-off is local overhead and potential exposure if a compromised host tampers with monitoring components [21].

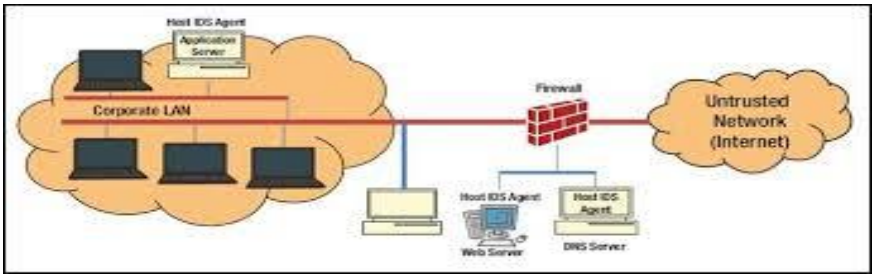

Fig 3 Host-Based IDS [22].

3.2 Network-based IDS (NIDS)

NIDS observe packets or flows traversing a network segment, providing visibility across multiple hosts. They can help identify coordinated attacks, but may struggle to confirm success without endpoint state [23]. High traffic volumes and encryption further motivate scalable, feature-efficient designs [24].

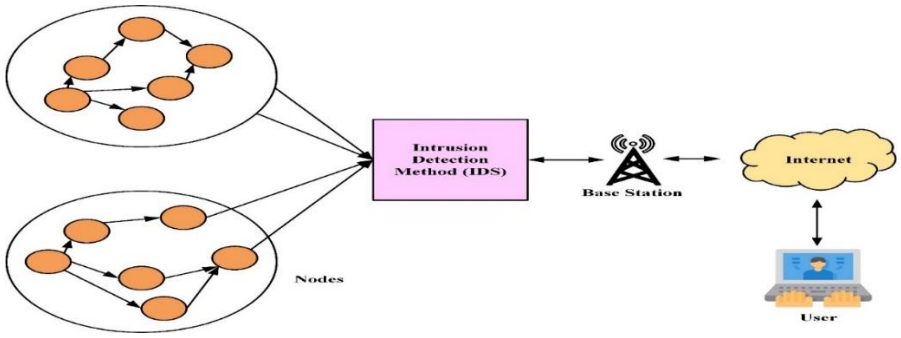

Fig 4 Network-Based IDS [25].

4. Surveyed Application Contexts

A major contribution of the cross-domain view of IDS research in web applications, cloud environments, IoT, WSN, MANET, and VoIP, each with different constraints and threat models.

4.1 Web applications

Web applications are among the most common systems targeted because of their open exposure and the use of protocols like HTTP and HTTPS. In this regard, the threat model is primarily external and includes the following attacks: SQL injection, cross-site scripting (XSS), remote code execution, credential stuffing, and application-layer denial-of-service attacks. Hackers typically use automated tools to scan web endpoints at scale, and more sophisticated attackers might seek to escalate privileges or establish an insider presence. Large traffic volume and the need to encrypt traffic with TLS are two major limitations of the web environment, as they hinder deep packet inspection. Moreover, contemporary web services are dynamic, and therefore, it is difficult to maintain rules that are not dynamic. It demands real-time detection, and hence IDS solutions should be used with minimal latency overhead to avoid disrupting users [26].

The main benefit of IDS implementation in web applications is that a signature-based system can efficiently identify known exploit patterns, particularly when combined with Web Application Firewalls (WAFs). There are additional behavioral and anomaly-based approaches that increase attack detection by modeling normal request patterns and system-call sequences, thereby detecting zero-day attacks. Nevertheless, anomaly-based detection is often vulnerable to high false-positive rates, especially when legitimate traffic patterns evolve too quickly.

Further, encrypted traffic limits visibility into payloads without requiring decryption or side-channel analysis. Current trends in this field include deep learning-based behavioral profiling and hybrid detection schemes that integrate rule-based and machine learning algorithms to achieve a balance between detection accuracy [27].

4.2 Cloud environments

Cloud computing environments present a dynamic, complex threat model that encompasses both external and insider threats. The major attack vectors are hypervisor exploitation, API abuse, and lateral movement between virtual machines, container escape vulnerabilities, and privilege escalation in multi-tenant environments. Due to the sharing of resources among tenants, there is a risk of a massive compromise in the event of an isolation failure caused by virtualization, distributed workloads, and the scale of resources [28]. These properties impose visibility constraints, particularly for encrypted east-west traffic among internal services. In addition, autoscaling behavior generates large numbers of legitimate events, making it difficult to model anomalies and leading to more alert noise. One of the key benefits of IDS implementation in cloud environments is the potential to have centralized monitoring at the hypervisor or orchestration layer. This allows to scale out distributed sensor deployment and be integrated with SIEM or XDR platform. Having hybrid IDS architectures is especially useful in the cloud context in that they provide the power of signature-based accuracy with known attacks and anomaly-based accuracy with new threats. However, their drawbacks are that it is hard to inspect encrypted intra-node traffic, that large amounts of telemetry data are computationally expensive to analyze, and that coordinating events across distributed nodes is challenging. There is a trend in recent research toward explainable techniques in artificial intelligence to enhance trust and interpretability in cloud-based IDS systems [29].

4.3 Internet of Things (IoT)

Connected devices are heterogeneous and have limited resources, thus posing a unique threat model to IoT environments. The attackers often take advantage of weak authentication systems, outdated firmware, and vulnerabilities in communication protocols. IoT ecosystems are vulnerable to botnet recruitment, device impersonation, and distributed denial-of-service attacks. The major limitations of IoT networks are limited processing and memory, as well as limited battery power. Numerous devices are used in wireless settings with limited bandwidth and a variety of communication protocols, such as MQTT and CoAP. The constraints are major limiting factors to the usability of computationally intensive detection models. The benefit of IDS implementation in IoT systems is the potential for lightweight edge-node anomaly detection, enabling local responses with lower latency. Detection mechanisms can be distributed to increase resilience by avoiding central points of weakness. Hybrid models, and in particular those based on optimized machine learning algorithms, have been shown to achieve better detection accuracy and manageable overhead [30].

Nevertheless, the IoT IDS solutions have significant drawbacks. Strong machine learning models require a wide, representative dataset, which is often unavailable. Consumption of energy is still one of the serious trade-offs as constant monitoring can reduce the life of devices. Besides, protocol diversity makes it difficult to develop universal detection frameworks [31]. Recent studies consider federated learning methods to support collaborative device-based detection while maintaining privacy, as well as energy-efficient optimization methods to address IoT limitations.

4.4 Wireless sensor networks (WSN)

The resources available to Wireless Sensor Networks are very limited, and they are often deployed in distributed, even hostile environments. The threat model includes sinkhole attacks, Sybil attacks, selective forwarding, node compromise, and energy-depletion techniques. Hackers usually aim to disrupt routing or inject invalid information into the network. The main limitations of WSNs are limited energy, limited memory, limited bandwidth, and a dynamic network structure [32]. These are critical in the IDS design decisions. The benefits of IDS in the WSN setting include cluster-based solutions that reduce communication load and save energy. Hybrid methods that integrate lightweight signature-based methods with anomaly-based methods achieve better detection while consuming fewer resources. Biologically inspired optimization techniques have also been suggested to improve detection accuracy in constrained conditions. Collaborative detection overheads, on the other hand, can still be very energy-consuming. Distributed coordination increases detection latency, and the limited feature space also limits the complexity of the implemented models. Recent developments are concerned with energy-efficient IDS systems and dynamic, adaptive clustering systems that trade off detection with network duration [33].

4.5 Mobile ad-hoc networks (MANET)

MANETs are decentralized networks with dynamic topologies and mobile nodes. Threat model: Blackhole and greyhole attacks, routing manipulation, replay attacks, and node impersonation are included. The lack of centralized control makes the environment more susceptible to organized, malignant actions. The limitations of MANETs include the high rate of topology change, limited battery power, and peer-to-peer communication. These attributes make IDS mechanisms dynamic and decentralized. Another major benefit of IDS implementation in MANETs is that it can also enable cooperative detection, in which nodes exchange information to enhance situational awareness. Reputation-based and trust-based systems achieve higher resilience by isolating bad players [34]. Decentralized IDS designs scale with network expansion. Nevertheless, distributed consensus systems raise communication costs and can bring delays. Mobility leads to false positives due to temporary routing changes, and the lack of centralized logging makes forensic analysis difficult.

4.6 Voice over IP (VoIP)

Voice over IP (VoIP) systems inherit the overall threat environment of IP-based networks and introduce protocol-specific vulnerabilities in signaling and real-time media transmission. VoIP environments face threats from SIP flooding, registration hijacking, call interception, toll fraud, replay, and volumetric denial-of-service (DoS) attacks. Attackers can use the signaling layer to control session initiation, exploit authentication system vulnerabilities, or cause resource overload to disrupt service availability [35]. VoIP systems have very stringent real-time requirements, with latency, jitter, and packet loss directly affecting service quality. This presents a major limitation to the operation of IDS, as detection systems cannot be implemented with noticeable delay. Also, encryption protocols such as the Secure Real-Time Transport Protocol (SRTP), Transport Layer Security (TLS), and the Secure/Multipurpose Internet Mail Extensions (S/MIME) are typically used to provide signaling and media confidentiality. Although encryption enhances privacy and integrity, deep packet inspection is constrained in traditional signature-based IDS solutions [36]. The advantage of IDS implementation in VoIP networks is that signalling protocols like SIP are structured, so protocol-sensitive detection strategies can be used to detect malformed requests, unusual call or registration rates, or other anomalies. Behavioral profiling can also identify anomalies in the frequency or duration of calls, potentially due to fraud or automated attacks.

Nevertheless, a major weakness is that, even with encryption in place, volumetric DoS attacks remain effective because their goal is not to access or alter message content, but to flood processing and bandwidth-sensitive facilities. Encryption, therefore, is not effective against resource exhaustion attacks [35]. Moreover, VoIP traffic requires high packet rates; therefore, highly optimized, scalable detection mechanisms are needed to prevent impaired Quality of Service (quality of service) [37].

6. Evaluation Considerations and Practical Recommendations

Anoperational evaluation of an IDS should test more than the detection rate. The survey indicates that IDS may generate massive false, repeated, and useless alerts, which encourage alert filtering and correlation [38]. In resource-limited settings (IoT/WSN/MANET), energy, memory, and communication overhead are key; in cloud and web services, throughput, scalability, and multi-tenant isolation are paramount.

(i)Practically, system designers should describe the threat model (insider/outsider, active/passive)

(ii) align detection with anticipated novelty (signature/ vs. anomaly/ vs. Hybrid)

(iii) select deployment site to fit the available evidence (HIDS, NIDS, or combination)

(iv) Enforce manageable alert control by incorporating SIEM-like filtering, triage, and correlation to reduce alert fatigue.

Conclusion

Intrusion detection is a natural complement to preventive security, protecting systems and networks by monitoring them for malicious activity. The IDS solutions are also contextual: web applications, cloud computing, IoT platforms, WSN, MANET, and VoIP impose specific sets of limitations and attack surfaces. In the literature, a key issue is maintaining high detection performance across different OSNs while minimizing false alarms and the computational cost. Advances are expected to arise from enhanced alert management, collaborative and staged detection, and resource-aware solutions that withstand shifting behavior and adversary adaptation.

References

[1] Mogadem, M. M., Li, Y., & Meheretie, D. L. (2022). A survey on internet of energy security: related fields, challenges, threats and emerging technologies. Cluster Computing, 25(4), 2449-2485.

[2] Abd Alsadh, M. H., Abdulateef, A. N., Al-Amshawi, M. Z., Taha, M. A., Najim, A. H., Ahmed, A. A., ... & Yoon, A. W. (2026). Improving Intrusion Detection in IoT Networks with a Hybrid CNN-BiLSTM Deep Learning Model. International Journal of Intelligent Engineering & Systems, 19(1).

[3] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

[4] Hamad, A. R., Baraa Alsabti, S. M., Najim, A. H., & Kadhim, M. N. (2025). A Hybrid Feature Selection and Machine Learning Approach for Parkinson's Disease Detection from Voice Signals in IoT-Enabled 6G Networks. International Journal of Intelligent Engineering & Systems, 18(5).

[5] Jangam, S. K. (2024). Research on Firewalls, Intrusion Detection Systems, and Monitoring Solutions Compatible with QUIC's Encryption and Evolving Protocol Features. International Journal of AI, BigData, Computational and Management Studies, 5(2), 90-101.

[6] Najim, A. H., Rasool, H. A., Ahmed, A. A., & Soliman, N. F. (2025). Intrusion Detection System in IoT 5G Networks Based on LSSVM and Harmony Search Optimization. Concurrency and Computation: Practice and Experience, 37(25-26), e70297.

[7] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.

[8] Hassan, M. Y., Mahdi, A. J., Al-Sharhanee, K. A. M., Ayad, M., Shutnan, W. A., & Najim, A. H. (2023, October). Designing a prototype smart hotel with high security, solar tracking, and IoT lighting control. In 2023 International Conference on Engineering Applied and Nano Sciences (ICEANS) (pp. 38-43). IEEE.

[9] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.

[10] Shutnan, W. A., Hassan, M. Y., Najim, A. H., & Faisal, N. (2023, July). A review: routing challenges in wireless sensor network. In 2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT) (pp. 40-43). IEEE.

[11] Sindhu, N., Gigras, Y., & Mahajan, S. (2024). Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. Journal of Operating Systems Development & Trends, 11(01), 29-44.

[12] Alsabti, S. M. B., Mustafa, A., Mahmood, N. T., Najim, A. H., & Ahmed, A. A. (2025). Bio-inspired Energy-efficient Routing Protocol for Dynamic Clustering in AI-based Wireless Sensor Networks in Smart Cities. International Journal of Intelligent Engineering & Systems, 18(9), 106-123.

[13] Hassan, M. Y., Najim, A. H., Al-sharhanee, K. A. M., Alkhafaji, M. A., Alfoudi, R. M., & Shutnan, W. A. (2023). Enhancing Resource Allocation and Optimization in IoT Networks Using AI-Driven Firefly Optimized Hybrid CNN-BILSTM Model. International Journal of Intelligent Engineering & Systems, 16(6).

[14] Rasool, H. A., Najim, A. H., Abd Alsadh, M. H., & Hariz, H. M. (2025). Recognition of Threats in Hybrid Wireless Sensor Networks by Integrating Harris Hawks with Gradient Boosting Algorithm. International Journal of Intelligent Engineering & Systems, 18(1).

[15] Iyer, K. I. (2021). From Signatures to Behavior: Evolving Strategies for Next-Generation Intrusion Detection. European Journal of Advances in Engineering and Technology, 8(6), 165-171.

[16] Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Yichiet, A., & Almufareh, M. F. (2022). Intrusion detection systems in internet of things and mobile Ad-Hoc networks. Computer Systems Science & Engineering, 40(3).

[17] Delay and Reliability Aware Optimal Communication in Intelligent Vehicular Adhoc Network (VANETs).

[18] Almheiri, S. J., Shah, A. A., Abbas, S., Ahmad, M., & Khan, M. A. (2025). Smart sustainable cyber security: modelling an interpretable and transparent threat detection with explainable artificial intelligence. Discover Sustainability, 6(1), 442.

[19] Wanda, P., & Jie, H. J. (2019). A survey of intrusion detection system. International Journal of Informatics and Computation, 1(1), 1-10.

[20] Najim, A. H. (2023). Collision aware distributed multicast routing protocol for vehicular adhoc networks. Texas Journal of Engineering and Technology, 22, 1-9.

[21] Al-sharhanee, K. A. M., Abdulsattar, N. F., Najim, A. H., Alkhayyat, A. H., & Alsalamy, F. H. (2023, July). Energy Aware Emergency Packets Dissemination and Effective Trusted RSU Distribution in Vehicular Adhoc Networks. In 2023 6th International Conference on Engineering Technology and its Applications (IICETA) (pp. 346-351). IEEE.

[22] Alsajri, A., & Steiti, A. (2024). Intrusion detection system based on machine learning algorithms:(SVM and genetic algorithm). Babylonian Journal of Machine Learning, 2024, 15-29.

[23] Kamil, R. A., Alsabti, S. M. B., Abdulsattar, R. K., Mohammed, A. H., & Elwi, T. A. (2025). On the enhancement anomaly detection for RF bio-sensors by computing artificial networks using machine learning techniques. Infocommunications Journal, 17(2), 89-95.

[24] Hashim Albohayah, Z. H., Abed, S. B., Mahdi, A. J., Kadhim, M. N., & Najim, A. H. (2025). Ch-PSO: A Novel Embedded Method based on PSO and Chebyshev Distance for Enhanced Epileptic Seizure Classification Using EEG Brain Signals. International Journal of Intelligent Engineering & Systems, 18(5).

[25] Abboud, S. M., Dosh, M. H., Ali, A., Najim, A. H., Alomari, M. A., & Yoon, A. W. (2026). Detection of Threats in IoT Systems by Integrating Particle Swarm Optimization with Light Gradient Boosting Algorithm. International Journal of Intelligent Engineering & Systems, 19(1).

[26] Alaoui, R. L., & Nfaoui, E. H. (2022). Deep learning for vulnerability and attack detection on web applications: A systematic literature review. Future Internet, 14(4), 118.

[27] Kailan, S. L., Muhammed, A. A., Mohammed, A. H., Al-Naemi, A. Q., Al-Sabti, S. M. B., & Abdulateef, I. A. (2024, December). Smart Continuous Wearable Real Time Monitoring System for Human Health Care based on IoT. In 2024 8th International Symposium on Innovative Approaches in Smart Technologies (ISAS) (pp. 1-6). IEEE.

[28] Rasool, H. A., Abdul-Sadah, A. M., Taha, M. S., Najim, A. H., & Meor Said, M. A. (2025). Multi-agent Reinforcement Le

[29] Al-Shawwaf, N. M. S., Ibrahim, A. A., & Al-Sabti, S. M. B. (2023, November). Energy Consumption Estimation Using Machine Learning with Data from Smart Meters in a Residential Complex Building in Iraq. In 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS) (pp. 1-7). IEEE.

[30] Ahmed, A. A., Al-sharhanee, K. A. M., Najim, A. H., Alheeti, K. M. A., Satar, N. S. M., & Hashim, A. H. A. (2024, December). Efficient UAV Routing Strategies for Wireless Sensor Network Data Retrieval. In 2024 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 1-5). IEEE.

[31] Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A survey of IoT and blockchain integration: Security perspective. IEEE Access, 9, 156114-156150.

[32] Shutnan, W. A., Mohammed, N. A., Abdulmunem, F. A., Najim, A. H., Hassan, M. Y., Soliman, N. F., & Algarni, A. D. (2024). Modeling and Control of a 3DOF Robot Manipulator Using Artificial Fuzzy-Immune FOPID Controller. IEEE Access.

[33] Gupta, N., Jindal, V., & Bedi, P. (2023). A survey on intrusion detection and prevention systems. SN Computer Science, 4(5), 439.

[34] Khodayer, A. M., Najim, A. H., Alkhazraji, N., Alkhayyat, A. H., & Abbas, F. H. (2023, July). Performance Evaluation of Effective Cluster Head Selection and Maintenance for LTE Based Vehicular Ad-Hoc Networks. In 2023 6th International Conference on Engineering Technology and its Applications (IICETA) (pp. 714-719). IEEE.

[35] BAlsabti, S. M., Al-Gburi, R. M., Mustafa, A., AHMED, S. K., Issa, A. M., Al-Naimi, T. M., ... & Elhenidy, A. M. (2025). Advances in Deep Learning for Multimodal Brain Imaging: A Comprehensive Survey. Neuroscience Informatics, 100252.

[36]Khudhair, K. M., Jabbar, R. H., Hasan, M. H., Muhsen, D. K., Kreah, A. F., & Najim, A. H. (2025, November). Behavioral Biometrics-Based Intrusion Detection in Online Banking Using LSTM Networks. In *2025 International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 1-7). IEEE.

[37] Sadiq, A. T., Muhsen, D. K., Ahmed, A. A., Fadhil, S. A., Ali, S. M., & Najim, A. H. (2025, November). Metaheuristic-Based Secure Forecasting of Cryptocurrency Volatility in Adversarial Environments. In *2025 International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 1-5). IEEE.

[38] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). International journal of information security, 22(5), 1125-1162.