Security Threats, Vulnerabilities, Intrusion Detection and Communication Protocols for Securing IoT Ecosystems

[1]Dr. Pardeep Singh, [2]Dr. Taruna Gulati

[1]Dean (Academics) & HOD(CSE), Guru Tegh Bahadur 4th Centenary Engineering College,

G-8 Area, Rajouri Garden, New Delhi, India.

[2]Assistant Professor, Maharaja Agrasen Institute of Technology, Sector 22, Rohini, Delhi, India. singh.pardeep@gmail.com, tarunagulati07@gmail.com

Abstract: Currently, the IoT has found its way in the present technology environment through the seamless fusion and vistas of heterogeneous devices, applications, and services in a veritable manner. However, the rising size and complexity of IoT ecosystems have raised substantial security challenges, such as cyber-attacks, device vulnerabilities, unauthorized access and data leakage, and communication-based risks. However, many IoT devices are resource-limited, and heterogeneous designs (e.g., different communication protocols) make it difficult to design and deploy efficient security solutions. In this work, we address IoT security risks and attacks, existing intrusion detection systems (IDSs), and security communication protocols. It discusses key attack types against IoT architectures, identifies vulnerabilities at different layers, and surveys existing intrusion detection methodologies (i.e., signature-based, anomaly-based, specification-based, and machine learning-based). It also covers common IoT messaging protocols, their potential vulnerabilities, and security features. The paper also provides detailed comparisons of current detection algorithms based on their merits, demerits, and appropriateness for resource-constrained IoT contexts. Key research issues linked with overheads, scalability, accuracy, privacy, interoperability, and real-time detection are also reported. Finally, we discuss emerging research paths toward establishing a framework for the establishment of safe, trustworthy, and resilient IoT ecosystems. With this purpose, we hope that this survey will offer a systematic view of the IoT security landscape to academics and practitioners and to expose perspectives for developing effective and powerful security solutions.

Keywords: Internet of Things (IoT), IoT Security, Cyberattacks, Security Vulnerabilities, Intrusion Detection Systems, Machine Learning, Communication Protocols, Network Security.

Introduction: Billions of smart gadgets are being connected to the internet through the Internet of Things (IoT). Data collection and sharing are made easier by the integrated software, sensors, and communication technologies in these devices. Healthcare, agriculture, home automation, manufacturing, the military, and transportation are just a few of the sectors that IoT solutions may help[1]. According to [2], automated home appliances, remote monitoring, smart locks in home automation, smart water management, smart transportation in smart cities, soil management, crop management, smart irrigation systems in agriculture, energy and water management, and many other scenarios, these solutions can be applied. IoT devices are vulnerable to a variety of security attacks due to their inherent resource constraints, the diversity of communication protocols, the vast number of connected devices, and the abundance of data generation [3]. The Internet of Things (IoT) is one of the most important revolutions of the high-tech era that allows communication between objects with specific physical properties, devices, sensors, and computer systems over the Internet. It has enabled seamless communication, data transfer, and remote monitoring across various application domains, such as smart homes, healthcare, industrial automation, intelligent transportation, smart cities, agriculture, and energy management [4]. The advances in sensing, wireless technology, cloud computing, and artificial intelligence have further improved the IoT systems by enabling automated reasoning and intelligent service provision. The growing density of connected devices is further complicated by the heterogeneity and interconnectivity of IoT systems[5]. However, alongside such tremendous advances afforded by adoption of IoT on incremental scale, one should take into account serious security and reliability challenges caused by pervasive use of this new technology[6]. Unlike conventional computing systems, the IoT ecosystem encompasses a diverse range of devices with varying hardware capabilities, operating systems, communication technologies, and security needs (and, thus, responses). Due to limited processing, memory, and energy

capabilities, conventional security mechanisms cannot be applied to many IoT devices. Furthermore, weak authentication, absence of access-control mechanism, insecure firmware, misconfiguration of the devices, and poor encryption can make IoT infrastructures vulnerable to certain types of cyberattacks. Such vulnerabilities allow attackers to compromise devices, alter transmitted data, disrupt services, and gain unauthorized access to sensitive data[7].IoT security threats are attacks on devices, communication channels, network infrastructure, and application services. These range from DDoS attacks, botnet attack, spoofing, eavesdropping, MITM attacks, replay attacks, routing attacks, to malware infections[8]. Such threats may impact the confidentiality, integrity, and availability of IoT resources. More importantly, for critical application domains such as healthcare, industrial control, and intelligent transportation, successful attacks may result in serious operational, safety, and reliability ramifications in addition to information security issues. Therefore, we need a deep understanding of IoT ecosystems vulnerabilities and security threats at different architectural layers to protect them[9].Intrusion detection systems (IDS) play a vital role in detecting malicious activities and safeguarding IoT networks against evolving cyber assaults. Traditional intrusion detection approaches are mostly signature-based and pattern-based, which are effective in detecting known threats but are largely blind to unknown or emerging attacks[10]. Anomaly-based detection methods address limitations of the above approaches to a certain degree by detecting any deviation from normal network or device behavior. Especially deep learning and machine learning based IoT intrusion detection approaches have attracted much attention in the last few years, given their ability to deal with large amounts of network traffic, capture complex behavioral patterns, and recognize unknown malicious activity. However, these approaches also face challenges in terms of computational overhead, training overhead, false-positive rate, scalability, and deployment on resource-constrained devices[11].Protocols are also important in IoT security as they govern communication between devices over heterogeneous networks. Protocols such as MQTT, CoAP, HTTP, AMQP, Zigbee, BLE, and LoRaWAN facilitate communication in different IoT applications and deployments[12]. While these protocols differ in features such as efficiency, scalability, and resource usage, the security features also vary greatly among the protocols. Weak authentication, poor encryption, insecure session management, and protocol misconfiguration can make communication channels susceptible to interception, tampering, and unauthorized access. Therefore, suitable security mechanisms must be selected to help ensure the confidentiality, integrity, and availability of IoT communications[13].

The remaining parts of the paper are organized as follows. Section II describes background and architectural foundations of IoT ecosystems. Section III discusses major attack types and security threat categories. Section IV presents vulnerabilities across various IoT layers. Section V discusses the state-of-the-art intrusion detection techniques and a performance comparison. Section VI discusses future direction for research, and concludes the paper.

II. **Background and Architectural Foundations of IoT Ecosystems.**

IoT can be defined as an internetworking of physical things that can sense, actuate, compute, and communicate to collect, exchange, and process information. These devices communicate with their environment and other devices in the network to provide intelligent services with minimal human intervention[14]. Advances in wireless communications, embedded systems, cloud and edge computing, and artificial intelligence have made IoT applicable to many domains. However, the heterogeneity of connected devices, communication technologies, and deployment environments makes the architecture complex and poses greater security requirements [15]. First, we must identify the current security threats in the IoT architecture and design a security solution to protect it. There are many iterations of IoT, but the general three-layer model (as shown in Fig. 1) is widely accepted: the perception layer, the network layer, and the application layer [16].

A. IoT Architecture

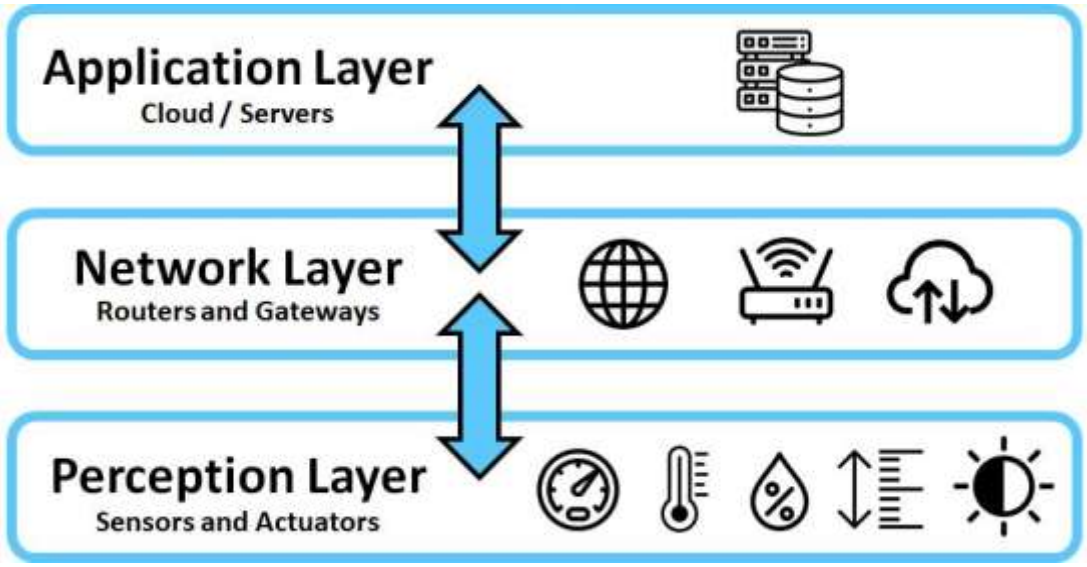


Fig. 1. IoT Architecture.

1. Perception Layer.

The perception layer is the physical foundation of an IoT ecosystem. It comprises sensors, actuators, RFID tags, embedded controllers, cameras, and other sensing devices that gather data from the environment. Sensing devices measure physical parameters like temperature, humidity, pressure, motion, and location, while actuators perform actions based on commands. Because these devices typically have limited processing power, memory, and battery life, it is challenging to deploy strong security mechanisms. Attacks on this layer typically bound to physical tampering, device access, insecure firmware, impersonating the device/sensors, and tampering with the sensors [17].

2. Network Layer.

It enables data collected to be shared between IoT devices, gateways, edge nodes, and clouds. It uses wired/wireless communication technologies like Wi-Fi, Bluetooth low energy (BLE), Zigbee, cellular networks, and LPWAN (low-power-wide-area-networks). The interconnected devices communicate data through communication protocols such as MQTT, CoAP, and HTTP. Security threats for this layer include eavesdropping, spoofing, replay attacks, man-in-the-middle attacks, routing attacks, and denial-of-service attacks. Thus, secure communication, authentication and encryption, and access control are critical to securing transmitted information [18].

3. Application Layer.

The application layer provides services and interfaces for users and organizations that interact with the IoT system. It comprises application software, cloud platforms, data analytics services, monitoring systems, and intelligent decision-making applications. Application Areas: Intelligent Health Delivery, Industrial Monitoring, Smart Houses, Agriculture, Transportation, and Smart City Infrastructure. Security threats in this layer include unauthorized access, data leakage, insecure APIs, privacy violations, and malicious software activity. Compromise at this layer can affect sensitive data and critical Internet of Things (IoT) services [19].

D. Security Challenges in Heterogeneous IoT Environments.

The "messiness" of IoT ecosystems makes it difficult to enforce uniform security policies. Devices from different manufacturers may use different hardware, operating systems, communication protocols, and authentication mechanisms. This makes it difficult to ensure interoperability while abiding by consistent security standards. Moreover, resource-limited devices may not be able to support complex encryption protocols or sophisticated intrusion

detection techniques. The growing number of connected devices increases the attack surface and demand for ongoing surveillance and vulnerability management. Moreover, the distributed nature of cloud, fog, and edge computing environments complicates efforts to secure stored data, manage identities, provide secure communication channels, and coordinate threat detection.
Considering these architectural and operational challenges, IoT security cannot be realized through a single protection mechanism. Instead, a comprehensive security architecture should include device security, secure communication protocols, strict access control, vulnerability assessment, and intelligent intrusion detection [20].

III. Security Threats and Attack Classification in IoT Ecosystems

Growing deployment of Internet-of-Things (IoT) devices has increased the attack surface of networked systems to various cyber assaults. The use of diverse devices, weak device resources, weak security of vendors/devices, and a wide variety of communication technologies provide niches for cyberthreats to compromise the system. Such attacks can target individual devices, communication channels, network infrastructure, or application services, compromising the confidentiality, integrity, availability, and reliability of operations [21].

A. Major IoT Security Attacks

IoT ecosystems are exposed to different cyberattacks on devices, communication channels, and network services. Common threats include Distributed Denial-of-Service (DDoS) attacks that overwhelm services and botnet attacks that mobilize compromised devices to perform malicious actions. Communication attacks such as man-in-the-middle (MitM), spoofing, replay, and eavesdropping allow attackers to intercept communication, alter data in transit, or pose as legitimate entities. Malware and ransomware also pose a challenge, disrupting device functionality, revealing confidential information, or preventing access to system resources. Routing attacks such as sinkhole, wormhole, and selective forwarding are more dangerous to reliable data transmission because they interfere with network communication. These attacks collectively jeopardize the confidentiality, integrity, and availability of the Internet of Things systems [22].

B. Classification of Attacks Across IoT Layers

IoT attacks can also be classified according to the architectural layer they target, as shown in Table 1.

Table 1. Classification of Attacks.

IoT Layer	Common Attacks
Perception Layer	Physical tampering, sensor manipulation, device impersonation
Network Layer	DDoS, MitM, spoofing, replay, eavesdropping, routing attacks
Application Layer	Malware, ransomware, unauthorized access, data breaches

C. Impact of Security Attacks on IoT Ecosystems.

Security attacks can have a significant impact on IoT infrastructure. Successful attacks may lead to sensitive data leakage, manipulation of sensor data, critical services disruption, monetary loss, and device disruption. Moreover, these attacks may affect the physical safety and reliability of safety-critical domains such as healthcare, industrial automation, and intelligent transportation.

Therefore, the growing sophistication of cyberattacks cannot be handled by traditional security measures alone. Thus, IoT security needs to be continuously evaluated for vulnerabilities, secure communication, and smart intrusion detection techniques for differentiating known and unknown threats [24].

IV. Vulnerabilities in IoT Ecosystems

IoT vulnerabilities are the weaknesses of the hardware, software, communication protocols, and network settings of the devices that can be exploited by malicious actors. Vulnerabilities include IoT architecture and connected devices, limited processing power, and corrupt settings and configurations. Awareness of such vulnerabilities is important in understanding potential attack pathways and pre-empting the attacks by implementing suitable protection mechanisms [25].

A. Device-Level Vulnerabilities

IoT devices often have limited processing power, memory, and energy, which limits the implementation of sophisticated security mechanisms. Weak passwords, inadequate authentication, unpatched firmware, insecure software updates, and physical exposure may leave individual devices vulnerable to compromise. Such vulnerabilities can enable unauthorized control of device operations and their malicious alteration [26].

B. Network and Communication Vulnerabilities

IoT devices typically employ wireless communication and lightweight protocols. However, insecure networks, weak encryption, and poor authentication and key management can allow information to be intercepted and altered. In addition, environments lacking protection against spoofing, replay, and routing attacks can compromise communication reliability and network security [27].

C. Software and Application Vulnerabilities.

Software vulnerabilities are big problems resulting from, for example, insecure software provided by IoT applications, cloud platforms, and their APIs and can expose data, functionality, and the system to attackers. Common vulnerabilities include insecure interfaces, insufficient access control, missing input validation, insecure data storage, and outdated software components. Exploiting these vulnerabilities can lead to service disruption, unauthorized access, and data leakage [28].

D. Privacy and Data Security Vulnerabilities.

IoT devices continuously collect and exchange information about users, environments, and operational activities. Inadequate data protection, excessive information collection, weak access restrictions, and insecure storage mechanisms can expose sensitive personal and organizational information. These vulnerabilities raise significant privacy concerns, particularly in healthcare, smart homes, and other environments involving confidential data [29].

E. Challenges in Vulnerability Management

Managing vulnerabilities across large-scale IoT ecosystems remains challenging because devices differ in their hardware capabilities, software configurations, manufacturers, and update mechanisms. The absence of regular security updates, limited monitoring capabilities, and inconsistent security standards can leave devices exposed to known weaknesses. Therefore, effective vulnerability management requires regular security assessments, secure firmware updates, strong authentication, encryption, and continuous monitoring [30].

V. Intrusion Detection Strategies in IoT Environments

Intrusion Detection Systems (IDS) are essential for identifying malicious activities and protecting IoT networks from cyber-attacks. They monitor network traffic, system behavior, and reactions to abnormal/suspicious activities to identify possible security breaches. IDS approaches are classified according to detection mechanisms as follows:

A. Signature-Based Detection

Signature-based IDS identifies attacks by comparing network activities against databases of known attack patterns. It effectively detects previously identified threats but has limited capability to recognize unknown attacks [31].

B. Anomaly-Based Detection

Anomaly-based IDS establishes a baseline of normal system or network behavior and identifies deviations that may indicate malicious activities. Although it can detect previously unknown attacks, it may generate false positives [32].

C. Specification-Based Detection

This approach detects intrusions by comparing system activities against predefined specifications of legitimate device and network behavior. It can identify deviations without depending entirely on known attack signatures [33].

D. Machine Learning-Based Detection

Machine learning techniques analyze network traffic and behavioral patterns to identify malicious activities. Algorithms such as Random Forest, Support Vector Machine, Decision Tree, and Naive Bayes are commonly investigated for IoT intrusion detection [34].

E. Deep Learning-Based Detection

Deep learning approaches, including Artificial Neural Networks, Convolutional Neural Networks, and Long Short-Term Memory networks, can learn complex patterns from network traffic. However, their computational requirements may limit deployment on resource-constrained IoT devices [35].

F. Comparative Analysis

In general, it is impossible to eliminate all IoT security threats with a single intrusion detection technique. In a hybrid approach, efficient detection, lightweight processing, continuous monitoring, and secure communication can improve the security of overall IoT ecosystems [36].

Table II. Comparative Analysis of Intrusion Detection Approaches in IoT Environments

Detection Approach	Major Advantage	Major Limitation
Signature-Based	Accurate for known attacks	Cannot easily detect unknown attacks
Anomaly-Based	Detects previously unseen threats	Higher false-positive possibility
Specification-Based	Uses defined legitimate behaviour	Requires accurate specifications
Machine Learning	Learns attack patterns	Depends on training data
Deep Learning	Learns complex features	High computational requirements

Table II compares IoT intrusion detection methods. Signature-based detection efficiently identifies known attacks but is limited in detecting unknown threats. Anomaly-based detection can detect unknown attacks by identifying deviations from normal behavior but may generate false positives. Specification-based detection relies on pre-defined rules of normal behaviour, and machine learning techniques allow malicious pattern detection over the data. Deep learning approaches can detect complex attack patterns but require more computational resources. In conclusion, the comparison

implies that the choice of intrusion detection approach depends on the IoT environment's security requirements, resources, and limitations [37].

VI. Future Research Directions and Conclusion.

Emerging Internet of Things technologies present challenges related to attacks, privacy, vulnerabilities, and security limitations. Future work will seek lightweight and intelligent intrusion detection methodologies using machine learning, deep learning, and federated learning. Edge computing, blockchain, lightweight encryption, and improved authentication can also improve security, scalability, and reliability. This paper provides an extensive survey of IoT security threats, vulnerabilities, and intrusion detection methods. It discusses key attack techniques, IoT system vulnerabilities, and existing detection systems. It highlights the need for adaptive, efficient, and scalable security solutions to address new threats and resource-limited devices. In summary, smart intrusion detection for connected devices and continuous monitoring are necessary for secure IoT ecosystems.

References

[1] Singh, U., Sood, M. & Bhadoria, R.S. IoT reliability, safety and trust under threat: a comprehensive survey of attacks, vulnerabilities, intrusion detection strategies and enabling protocols. *Life Cycle Reliab Saf Eng* (2026). https://doi.org/10.1007/s41872-026-00475-1

[2] Moucharraf, M., Ridouani, M., Salahdine, F., & Kaabouch, N. (2026). IoT Security: A Comprehensive Review of Architectures, Threat Models, Detection Methods, and Countermeasures. *Future Internet*, *18*(5), 266.

[3] Komal, A., & Li, S. (2026). Intrusion Detection in the Internet of Things: A Comprehensive Review of Techniques, Architectures, Datasets, and Emerging Trends. *Sensors*, *26*(11), 3405.

[4] Sallam, S., El Barachi, M., & Li, N. (2026). Intrusion Detection on the Internet of Things: A Comprehensive Review and Gap Analysis Toward Real-Time, Lightweight, Adaptive, and Autonomous Security. *Internet of Things (IoT)*, *7*(1), 16.

[5] Anand, N., Singh, K.J. (2024). A Comprehensive Study of DDoS Attack on Internet of Things Network. In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore. https://doi.org/10.1007/978-981-99-4713-3_56

[6] Anand, N., Singh, K.J. (2023). An Overview on Security and Privacy Concerns in IoT-Based Smart Environments. In: Rao, U.P., Alazab, M., Gohil, B.N., Chelliah, P.R. (eds) Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol 1049. Springer, Singapore. https://doi.org/10.1007/978-981-99-3569-7_21

[7] Kumar, S. S., & Jerlin, M. A. (2026). Intelligent defense at the edge: a comprehensive survey of federated learning, TinyML and explainable AI for intrusion detection in IoT and IIoT ecosystems. *Frontiers in Artificial Intelligence*, *9*, 1900815.

[8] Baccari, S., Hadded, M., Khalil, O. K., & Laouiti, A. (2026). Cybersecurity challenges in the internet of energy: a survey of attack taxonomies, defense mechanisms, and open issues. *Journal of King Saud University Computer and Information Sciences*.

[9] Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors*, *21*(11), 3654. https://doi.org/10.3390/s21113654

[10] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEe Access*, *9*, 59353-59377.https://doi.org/10.1109/ACCESS.2021.3073408

[11]Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent security trends in internet of things: A comprehensive survey. *IEEE Access*, *9*, 113292-113314. https://doi.org/10.1109/ACCESS.2021.3103725

[12]Singh, P., Sharma, V., Anand, N., Kundu, R. (2027). A Systematic Analysis of Learning Methods for Privacy Preservation in IoT Environments. In: Roy, N.R., Panda, B., Halgamuge, M.N. (eds) Proceedings of International Conference on Artificial Intelligence and Cyber Security. ICAICS 2025. Lecture Notes in Networks and Systems, vol 2024. Springer, Cham. https://doi.org/10.1007/978-3-032-28379-5_28

[13] Kumar, N., Asmita, Kaushik, S., Soni, R.S., Verma, R., Anand, N. (2026). Experimental Results Region-Based Convolutional Neural Network Algorithm for Deep Face Detection. In: Udgata, S.K., Mohapatra, D., Sethi, S., Rana, M.E. (eds) Intelligent Systems. ICMIB 2025. Lecture Notes in Networks and Systems, vol 1624. Springer, Cham. https://doi.org/10.1007/978-3-032-05117-2_26

[14] Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst 73, 3–25 (2020). https://doi.org/10.1007/s11235-019-00599-z

[15] R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1019-1024, https://doi.org/10.1109/ICOEI.2019.8862720

[16]Nayak, D. *et al.* (2026). A Metaheuristic-Tuned Hybrid IDS for Detecting DDoS Attacks in IoT Networks. In: Swaroop, A., Virdee, B., Correia, S.D., Valicek, J. (eds) Data Processing and Networking. ICDPN 2025. Lecture Notes in Networks and Systems, vol 2005. Springer, Cham. https://doi.org/10.1007/978-3-032-27691-9_11

[17] Kumar, M., Lal, I.B., Ranjan, R., Kumar, N., Kumar, N., Anand, N. (2025). Optimizing Modulation Schemes for 5G Efficiency Networks. In: Ghonge, M.M., Liu, H., Khan, M., Tran, T.A. (eds) Advances in Emerging Technologies and Computing Innovations. ICETCI 2025. Sustainable Artificial Intelligence-Powered Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-92854-3_39

[18] Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, *9*(2), 44. https://doi.org/10.3390/computers9020044

[19] Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. *Applied Sciences*, *16*(3), 1511. https://doi.org/10.3390/app16031511

[20] Agarwal, S., Singh, A. P., & Anand, N. (2013, July). Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for non-linear mathematical optimization functions. In *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)* (pp. 1-8). IEEE.https://doi.org/10.1109/ICCCNT.2013.6726474

[21] Anand, N., & Kumar, M. (2013, July). Modeling and optimization of extraction-transformation-loading (ETL) processes in data warehouse: An overview. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICCCNT.2013.6726592

[22] Anand, N., Raj, P., Shivam, S., & Sharma, V. (2025, August). A Layer based Aspect of the Security Issues in Internet of Things: An Analytical Survey. In *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)* (pp. 34-40). IEEE. https://doi.org/10.1109/CISES66934.2025.11265603

[23] Hamroun, C., Fladenmuller, A., Pariente, M., & Pujolle, G. (2025). Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges, and perspectives. IEEE Access, 13, 40950-40976. https://doi.org/10.1109/ACCESS.2025.3546338

[24] Concejal-Muñoz, D., Del Corte-Valiente, A., & Pastor-Vargas, R. (2026). A Quantitative Comparative Analysis of Centrality Metrics for an Efficient and Effective Intrusion Detection System in IoT Networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2026.3752775

[25] Verma, R., Kumar, V., Sharma, A., Anand, N., Raj, K., & Kumar, N. (2025, December). Artificial Intelligence Based Image Classification and Compression Technique. In *2025 IEEE International Conference on Electrical,*

Electronics, Communication and Computers (ELEXCOM) (pp. 1-5). IEEE. https://doi.org/10.1109/ELEXCOM67950.2025.11451667

[26] Nayak, D., Anand, N., Prusty, T., & Das, S. Transfer learning for corn leaf disease detection: experimental comparison of MobileNetV2 and EfficientNetBO. In Connecting Intelligence (pp. 408-412). CRC Press. https://doi.org/10.1201/9781003773504-69

[27] Sharma, V., Kumari, P., Das, S., Anand, N., & Kundu, R. Energy efficient IoT enabled smart irrigation system leveraging LoRa technology. In Connecting Intelligence (pp. 413-418). CRC Press. https://doi.org/10.1201/9781003773504-70

[28] Anand, P. S. N. (2014). Framework for The Integrated And Validated Model of Data Warehouse. *American Journal of Engineering Research (AJER), e-ISSN*, 2320-0847.

[29] Anand, N. (2014). The Conceptual Modeling of ETL Processes. *Journal of Global Research in Computer Science*, *5*(1), 16-18.

[30] Anand, N. (2012). Application of ETL tools in business intelligence. *International Journal of Scientific and Research Publications*, *2*(11), 1-4.

[31] Kumar, N., Sharma, P., Anand, N., & Dash, J. (2025, April). Frame Encoding Technique by Different Stuffing Approaches. In *Proc. Int. Conf. Advances in Computing, Communication & Networks (ICACCN), Bhubaneswar, India*.

[32] Anand, N., & Sharma, P. (2014). Data Warehouse Security through Conceptual Models.

[33] Nitin Anand, Vatsala Sharma, Pardeep Singh (2025); ETL and Data Warehousing: Architecture, Vulnerabilities, and Security Mechanisms; International Journal of Scientific and Research Publications (IJSRP) 15(10) (ISSN: 2250-3153), DOI: http://dx.doi.org/10.29322/IJSRP.15.10.2025.p16612

[34] Anand, N., & Kumar, N. Jnyanaranjan Dash. Dipa Patra: Using ETL for Optimizing Business Intelligence Success in Multiple Investment Combinations, published in International Journal of Applied Engineering Research ISSN, 0973-4562.

[35] Kumari, A., Kumar, P., Nath, T., Mondal, B., Hazra, K., Anand, N., & Kumar, N. (2026). Evaluating a Novel Hybrid Deep Learning Model for Brain Tumor Diagnosis. *Available at SSRN 6062834*. https://dx.doi.org/10.2139/ssrn.6062834

[36] Ahmed, A. H., Fida, M. R., & Arsalaan, A. S. (2026). In-Network Security Framework for Detecting and Classifying DDoS Attacks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2026.3745922

[37] Kumar, P., & Kumar, B. (2025, April). Enhanced Security with Deep Learning-Based Intrusion Detection. In *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)* (Vol. 3, pp. 1484-1488). IEEE. https://doi.org/10.1109/ICCSAI64074.2025.11063977