Volume 11, Issue 8, August – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

A Comprehensive Review of Malware Detection Techniques in Wireless Sensor Networks

Aman Sharma[1]; Vishvesh Revoori[2]

[1]Senior Software Engineer at Meta Seattle
[2]Senior Software Development Engineer at Amazon, Austin, Texas, USA

Publication Date: 2026/08/08

Abstract: Over the past few years, Wireless Sensor Networks (WSNs) have been increasingly deployed for numerous sensing and monitoring purposes in environmental monitoring, industrial automation, health monitoring, military surveillance, smart agriculture and disaster management among others. The inherent limitations in terms of processing power, memory, communication bandwidth and energy of sensor nodes make WSNs highly susceptible to malware attacks. A wide variety of malware such as sensor network worms, Trojans, viruses, botnets and ransomware can easily propagate in a network through inter node communication. Such malware can cause serious damage to communication, compromise sensitive data, consume energy of the infected nodes thereby reducing the lifetime of network among others. In the last decade, numerous approaches have been proposed for the detection of malware infecting sensor nodes. These approaches range from traditional signature-based detection and behavior-based detection to more advanced approaches such as machine learning (ML)-based, deep learning (DL) -based, blockchain-based, trust management-based and federated learning-based detection. Most of the existing approaches for malware detection in WSNs have been designed to work on WSNs and have not been tested on real scenarios. Most of the approaches have their own strengths and weaknesses and the most suitable approach for a given application depends on various factors. In this paper, we present a comprehensive review of approaches for the detection of malware infecting sensor nodes in WSNs. We present a taxonomy of reviewed approaches for detection of malware. We also present a discussion on approaches for modeling malware propagation in a WSN as well as review on various categories of malware that have been designed to attack sensor nodes in WSNs along with detection frameworks for different categories of malware. We also present a comparative study of approaches used for the detection of malware in WSNs on the basis of various parameters such as detection accuracy, computational complexity, energy efficiency, scalability, detection latency and deployability. The review and taxonomy presented in this paper will be highly beneficial for researchers and practitioners designing approaches and systems for the detection of malware in WSNs. Various open research challenges in this area have also been discussed in this paper including detection of zero-day malware, designing of intelligent models to be light enough to be deployed on sensor nodes, use of explainable artificial intelligence for detection of malware in WSNs, designing approaches for privacy-preserving collaborative learning in WSNs and designing adaptive security approaches for WSNs.

Keywords: *Wireless Sensor Networks, Malware Detection, Network Security, Machine Learning, Deep Learning, Blockchain, Trust Management, Federated Learning, Cybersecurity.*

How to Cite: Aman Sharma; Vishvesh Revoori (2026) A Comprehensive Review of Malware Detection Techniques in Wireless Sensor Networks. *International Journal of Innovative Science and Research Technology*, 11(8), 45-51. https://doi.org/10.38124/ijisrt/26aug099

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become indispensable for modern intelligent sensing, enabling autonomous data collection and transmission across distributed locations with minimal human intervention [1], [4], [14], [18], [20], [29]. Comprising numerous low-cost, battery-powered nodes equipped with sensing and communication capabilities, WSNs collaboratively monitor environmental conditions and forward data to base stations for analysis [1], [4], [14], [18], [20], [29]. Their self-organizing nature, flexible deployment, and cost-effectiveness have driven widespread adoption in environmental monitoring, industrial automation, healthcare, surveillance, structural health monitoring, smart agriculture, disaster management, transportation, and IoT applications [1], [4], [14], [18], [20], [29]. Integration with cloud computing, edge intelligence, and Industry 4.0 has further expanded their role in next-generation infrastructures [2], [4], [9]. However, same features that make WSNs so attractive also bring a number of security challenges [1], [4], [14], [18], [20].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

Existing survey studies have mainly been centered around a single facet of WSN security; malware detection surveys have only dealt with conventional settings without taking into account the challenges of WSN security, while WSN security survey articles have mostly addressed routing, trust, authentication, and intrusion detection aspects without considering the taxonomy of malware, its propagation, and intelligent detection [6], [8], [23], [1], [4], [5]. With the recent advancements in AI, deep learning, blockchain, and collaborative security, there is a need for an up-to-date and comprehensive review [1], [4], [5], [8], [23]. In this paper, we present a comprehensive overview of malware detection in WSNs by providing an insight into both conventional and intelligent malware detection techniques, proposing a unified taxonomy of malware, identifying the propagation of malware in WSNs, investigating signature-based, heuristic, behavior-based, ML, deep learning, blockchain-based, and trust-aware malware detection methods, comparing different methods from the perspectives of accuracy, complexity, overhead, energy, scalability, and feasibility, recognizing research gaps, and discussing new research trends such as lightweight AI, federated learning, explainable AI, edge intelligence, TinyML, blockchain-based security, adaptive trust management, and autonomous malware detection [4], [5], [9], [14], [15], [16], [17], [18], [20], [29]. This figure 1 provides a hierarchical taxonomy of malware detection approaches in WSNs. The taxonomy classifies existing malware detection methods into five major categories based on their underlying detection strategy. The diagram is suitable for a review paper because it provides a clear overview of how different techniques have evolved from traditional methods to modern AI-driven approaches.

II. RELATED WORK

In recent years, the applications of WSNs have been increased in areas of health monitoring, industrial automation, environmental monitoring, military, precision agriculture and smart cities. Therefore, security of these networks is a great concern because of distributed nature of WSNs, limited capabilities of sensors, restricted energy at sensors, unattended nature of sensors to be deployed. Therefore, traditional methods of security such as encryption, authentication, access control are not sufficient to counter-attack the advanced malwares. Malwares can infect the sensor nodes by exploiting the vulnerabilities of sensor nodes, alter the normal behavior of sensor nodes and can propagate in the network rapidly. Many research efforts have been done to develop the malware detection and security systems for WSNs. Malware detection using various approaches such as blockchain based trust management, malware propagation using epidemic models and intrusion detection using AI and ML have been developed for securing WSNs. The research has been moved from traditional approaches to rule-based systems to intelligent, adaptive, distributed systems for securing the malware attacks in WSNs. However, many challenges exist that need to be addressed for efficient security of WSNs.

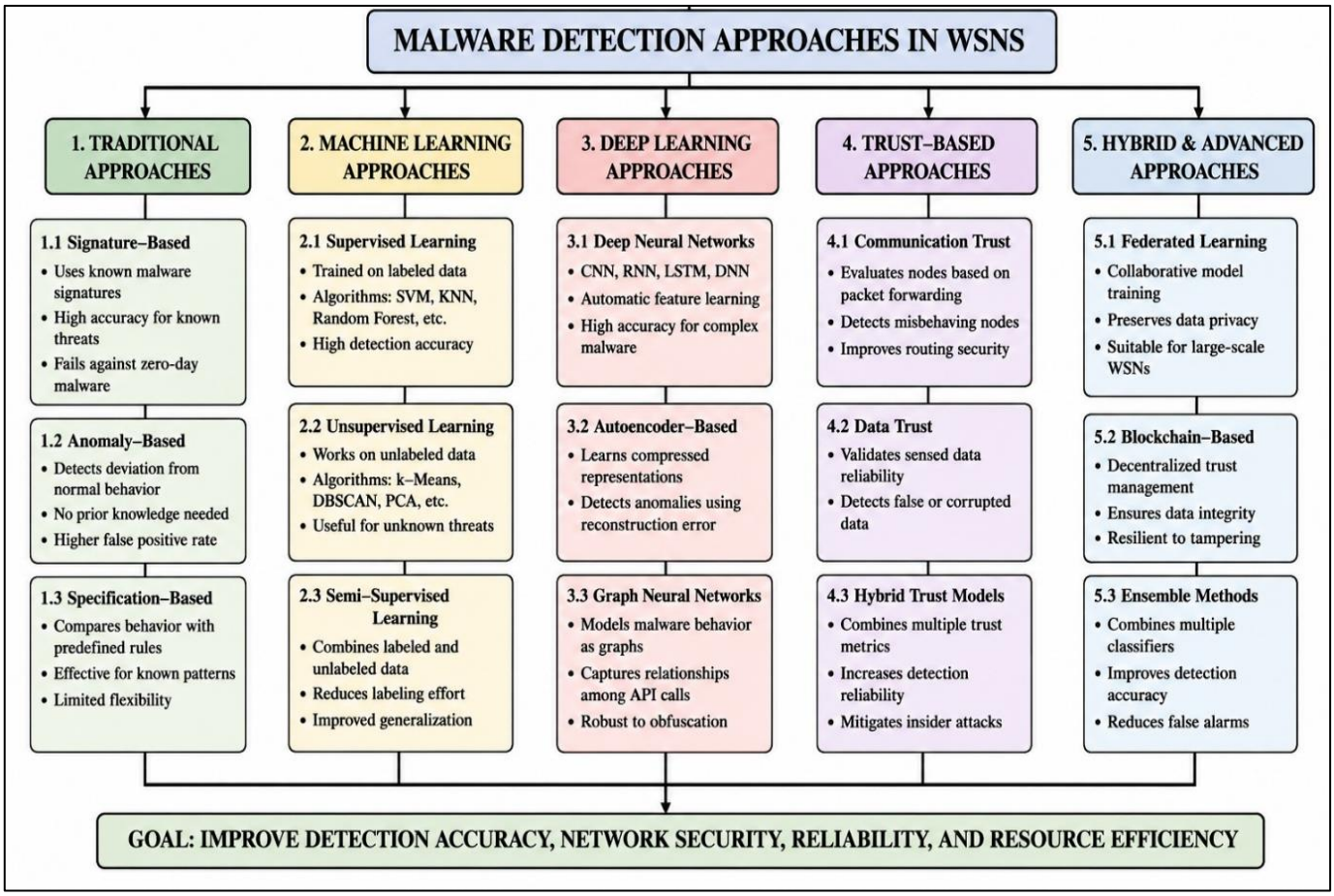

Fig 1: Hierarchical Taxonomy of Malware Detection Approaches in WSNs.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

The enhancement of trust and transparency in WSNs through Distributed Ledger Technology (DLT) or Blockchain is one of the major issues. The trust management in WSNs can be enabled by various mechanisms and blockchain is one of the emerging technologies which enables data integrity, traceability and avoids single point of failure. Even though the use of blockchain in WSNs is in its infancy, various applications have emerged that enable the use of WSNs in various fields. In this paper, we present a survey on distributed ledger technology in WSNs. The various architectures, consensus, smart contracts, authentication, privacy preserving and data aggregation in WSNs that enables malicious node detection and secure communication are presented. The uses of blockchain in WSNs enable various advantages to the users and also can be used in various applications. However, there are various challenges that affect the use of blockchain in WSNs. Some of the major challenges include high computational overhead, increased communication overhead, large storage requirements, scalability and high energy consumption. These challenges restrict the usage of various blockchain protocols in WSNs and hence, there is a need to propose various lightweight consensus algorithms and also energy efficient blockchain architectures for WSNs.

Table 1. Comparative Analysis of Existing Malware Detection and Security Approaches in WSNs

Ref.	Method / Technique	Application / Focus	Key Advantages	Major Limitations	Research Gap
[1]	Blockchain-enabled WSN security	Malicious node detection	Decentralized trust, immutable storage, secure data sharing	High computation, storage, communication overhead	Lightweight blockchain for resource-constrained WSNs
[2]	SE_1E_2IR epidemic model	Malware propagation analysis	Models multi-malware spread and infection dynamics	No practical malware detection mechanism	Integration with intelligent real-time detection
[3]	Fractional-order SE_1E_2VIQR model	Multi-malware propagation	Considers memory effects, vaccination and quarantine	Purely analytical model	Practical AI-enabled malware detection framework
[4]	ML survey	WSN security	Comprehensive review of ML techniques for network security	Not malware-specific	Dedicated malware detection taxonomy
[5]	CNN-based Intrusion Detection System	Wi-Fi WSN intrusion detection	High detection accuracy (~97%), low false alarms	Detects intrusions rather than malware	Malware-oriented deep learning framework
[6]	Static malware analysis	IoT malware detection	Low computational complexity, cross-platform applicability	Ineffective against obfuscated and polymorphic malware	Hybrid static-dynamic analysis
[7]	Game theory + epidemic model	Malware propagation	Models attacker–defender interaction	No adaptive malware detection	Intelligent adaptive defense mechanisms
[8]	Comprehensive malware detection survey	Malware detection techniques	Categorizes signature, heuristic, ML and DL approaches	General survey, not WSN-specific	WSN-oriented malware detection review
[9]	ML with SDN	Attack detection	Intelligent network management and attack mitigation	Focuses on DDoS rather than malware	Malware detection in WSNs
[10]	CNN + Malware visualization	Windows malware detection	Automatic feature extraction with high accuracy	High computational complexity	Lightweight edge-based deep learning
[11]	Comparative ML classifiers	Dynamic malware detection	Excellent classification accuracy using behavioral features	Evaluated on general datasets	Validation in resource-constrained WSNs
[12]	Graph Convolutional Network (GCN)	Malware detection	Learns graph relationships and improves robustness	Computationally expensive	Lightweight graph learning
[13]	Autoencoder + CNN	Android malware detection	Automatic feature learning with high accuracy	Android-specific and computationally intensive	Real-time WSN malware detection

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

[14]	Secure and Dependable Trust Assessment Scheme (SDTS)	Trust-based malicious node detection	Low false positives and improved trust evaluation	Does not directly detect malware	AI-assisted trust-based malware detection
[15]	CATER	Secure routing	Congestion-aware trust and energy-efficient routing	Focuses on routing security	Integration with malware detection
[16]	Universal Trust Model (UTM)	Forest fire monitoring	Reliable trust-based data validation	Application-specific	Generalized malware detection framework
[17]	ICMA	Congestion control	Improves throughput and bandwidth utilization	Not designed for malware detection	Congestion-aware malware mitigation
[18]	Multi Trust-Based Secure Trust Model	Trust management	Detects malicious nodes with low overhead	Trust evaluation only	AI-integrated malware detection
[19]	Coati Optimization Algorithm	Node localization	High localization accuracy	Not related to malware analysis	Security-aware localization
[20]	Lightweight Trust Estimation Scheme (LTS)	Clustered WSN security	Efficient trust computation and routing reliability	No malware classification	Hybrid trust + AI framework
[21]	SE-TEM	Trust evaluation	Lightweight secure communication	No malware detection	Intelligent malware-aware trust evaluation
[22]	Deep Generative Model	Obfuscated malware detection	Effective against code obfuscation	High computational cost	Lightweight deployment for WSNs
[23]	AI-driven cybersecurity survey	Malware & intrusion detection	Reviews ML, DL, FL, XAI, RL	Identifies open challenges only	Practical WSN malware framework
[24]	PCA + SVD + DNN	Cyberattack detection	High accuracy with feature reduction	General cyberattacks, not malware	Malware-specific classification
[25]	Federated Learning	IoT malware detection	Privacy-preserving collaborative learning	Communication overhead and synchronization	Efficient FL for WSNs
[26]	Time-aware ML	Android malware detection	Robust against evolving malware	Android-specific	Adaptation for WSN malware
[27]	Early ransomware detection	Crypto-ransomware	Detects attacks before encryption	Limited to ransomware	General malware detection
[28]	Recurrent Neural Network (RNN)	IoT malware detection	Captures temporal malware behavior	High computational requirements	Lightweight recurrent models
[29]	ML-oriented Trust Decision Framework	Malicious node detection	Combines ML with trust evaluation	Limited malware analysis	Dedicated malware classification
[30]	Resource-aware Secure Trust Model	Trust management	Low communication and computational overhead	No AI-based malware detection	Hybrid AI-trust malware detection

III. TAXONOMY OF MALWARE DETECTION APPROACHES IN WSNS

The rapid growth of WSNs has changed the way we collect, process, and analyze data. However, this growth has also made it easier for cybercriminals to attack these systems, making malware detection a crucial part of network security. The main challenge in defending WSNs is that they have limited resources, such as processing power, memory, and battery life. This means that traditional security mechanisms, which are often computationally intensive, cannot be used. Malware detection for WSNs is becoming a huge problem as WSNs are increasingly being used in industrial control systems, healthcare monitoring systems, and even in transportation systems. In this work, we survey a number of different approaches for malware detection in WSNs. The first approach for malware detection in WSNs is the use of signature-based detection, where files or network traffic are compared to the signatures of known malicious software. This approach has a number of advantages, including ease of use and good performance for known malicious software.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

IV. COMPARATIVE ANALYSIS, RESEARCH CHALLENGES, AND FUTURE RESEARCH DIRECTIONS

So far, a large number of approaches have been proposed to detect malware in WSNs. However, many of the current approaches have several limitations, such as low accuracy, high computational complexity, and bad scalability, etc. Thus, these approaches can not be applied to the detection of malware in WSNs directly. As for the three traditional approaches for malicious software detection, namely, signature-based detection, specification-based detection and anomaly-based detection, the first one has a low detection rate for unknown malware, since a complete virus and malware database is difficult to establish due to the fast growth of virus and malware in recent years. Although the false detection rate of specification-based detection approaches can be decreased significantly by using deep knowledge of network behavior, the approaches are difficult to maintain, since network policies often change with time. In addition, the detection performance of anomaly-based approaches greatly depends on the learning data, and it is often difficult to obtain high detection accuracy using a small amount of training data. Recently, many approaches based on ML have been proposed to improve the detection performance. The approaches can be divided into three categories, namely, supervised learning, unsupervised learning and semi-supervised learning. Many supervised learning-based approaches have been proposed to use various learning models such as Support Vector Machines, Random Forests, Decision Trees and k-Nearest Neighbors, and so on, for the detection of malware in WSNs, since they can obtain high detection accuracy when a large amount of labeled data is provided.

V. CONCLUSION AND FUTURE WORK

Detecting malware on WSNs has recently gained a lot of attention and a large number of techniques have been proposed in order to face this challenging task. Most of these techniques are not able to satisfy all of the required constraints at the same time and thus, new rule-based methods have to be replaced by AI-based methods that are able to learn from data and to adapt to new and unknown malware behavior within very limited resources [4], [5], [8], [9], [23]. A first category of methods is based on the signature of malware, i.e., they search in a database for known malware. However, this category of methods fails in case of unknown or polymorphic malware [8], [22], [23]. A second category of methods is based on the anomaly detection in the behavior of sensor nodes. Anomaly-based detection methods are able to detect unknown malware but they often produce a large number of false positives since many legal behaviors in a network deviate from the normal behavior [8], [23]. In order to reduce false positives, a third category of methods uses the specification of the behavior that a sensor node is allowed to perform. Specification-based methods reduce false positives since they verify the behavior of a sensor node against a set of predefined policies [4], [8]. However, the specification of the allowed behavior has to be created by an expert and has to be updated often since the network architecture is changing over time. Hence, specification-based methods are not widely used. ML methods have been widely used for detecting malware in WSNs. They use supervised learning techniques such as Support Vector Machines, Random Forests, Decision Trees, and k-Nearest Neighbors to create models that can classify network traffic as malicious or not. Most of these methods are able to achieve high accuracy if a sufficient amount of labeled data is available. However, they are sensitive to a number of issues including class imbalance between classes, dataset bias, and concept drift over time as malware evolves [4], [5], [9], [11], [24]. Unsupervised and semi-supervised learning have also been used for detecting malware in WSNs. These methods are able to alleviate some of the requirements for supervised learning methods by not requiring labeled data for training. However, their accuracy for classification is generally lower than that of supervised learning methods [4], [9], [11]. Recent years have also seen the emergence and use of Deep Learning (DL) techniques for malware detection in WSNs. DL methods are able to automatically discover hierarchical features from input data such as malware binaries, API calls, and execution traces without requiring manual feature engineering. These methods include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTM), Autoencoders, and Graph Neural Networks (GNNs). DL-based methods have recently achieved state-of-the-art performance for detecting polymorphic malware. However, their high detection accuracy comes with the cost of increased computational requirements, higher energy consumption, and larger memory needs, which make their direct implementation on sensor nodes infeasible. To address these challenges, many approaches have been proposed, including edge-based detection, cloud-based detection, hybrid approaches that first detect malware on the sensor node and then verify the result on the cloud, and federated learning approaches that enable privacy-preserving collaborative learning between sensors without requiring to transfer their data to a central server [10], [12], [13], [22], [26], [28]. In addition to AI-based methods for detecting malware, a number of other approaches have been recently proposed, including trust-based methods, blockchain-based methods, and Federated Learning methods. Trust management methods have recently been used for detecting malware in WSNs since they are able to detect behavior that deviates from a threshold of normal behavior and to isolate malicious sensors before they are able to cause significant damage to the network. However, these methods are not able to distinguish between stealthy malware that behaves normally and malicious behavior that has been intentionally introduced to the network by an attacker [14], [15], [16], [18], [20], [21], [29], [30]. Blockchain has also been used for securing data in WSNs since it is able to provide a distributed data structure that is used to record all changes in a network in a secure, tamper-proof, and decentralized way. However, the use of blockchain in sensor networks is still in its infancy since it requires a lot of storage and a lot of computational power at each sensor node, which are not available on most sensor devices. Thus, most approaches that use blockchain for securing data in WSNs use it on the cloud or on a gateway instead of on the sensor nodes themselves [1]. Federated Learning has also been used for detecting

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

malware in WSNs since it enables a sensor node to contribute to a ML model without having to transfer its data to another node. However, Federated Learning has a number of challenges, including high communication overhead, non-independent data distributions, client heterogeneity, and vulnerability to poisoning attacks. Thus, Federated Learning has recently started to be used for WSNs in conjunction with other techniques in order to address these challenges [25]. Recently, a number of hybrid approaches have been proposed that combine multiple techniques in order to take advantage of their complementary strengths. For example, some approaches use AI-based methods for detecting unknown behaviors and rely on trust management or specification-based methods for classifying the detected behavior as malicious or not, while other approaches use blockchain for securing the results of AI-based methods and store them in a distributed dataset instead of storing them on a single server. These hybrid approaches have the potential to achieve better detection accuracy, higher reliability, and better energy efficiency than any single technique. Thus, they represent an important direction for future research on malware detection in WSNs [21], [23], [25], [29].

- Conflicts of Interest: The authors declare that they have no competing interests.
- Acknowledgement: Not applicable.
- Consent to Publish declaration: Not applicable.
- Consent to Participate declaration: Not applicable.
- Ethics declaration: Not applicable.

REFERENCES

[1]. Ramasamy, Lakshmana Kumar, Firoz Khan KP, Agbotiname Lucky Imoize, Joshua O. Ogbebor, Seifedine Kadry, and Seungmin Rho. "Blockchain-based wireless sensor networks for malicious node detection: A survey." *IEEE Access* 9 (2021): 128765-128785.

[2]. Awasthi, Shashank, Pramod Kumar Srivastava, Naresh Kumar, Rudra Pratap Ojha, Purnendu Shekhar Pandey, Rajesh Singh, Anita Gehlot, Neeraj Priyadarshi, Rituraj Jain, and Yohannes Bekuma Bakare. "An epidemic model for the investigation of multi-malware attack in wireless sensor network." *IET Communications* 17, no. 11 (2023): 1274-1287.

[3]. Mishra, Jyoti, Pramod Kumar Srivastava, and Vineet Srivastava. "Securing Wireless Sensor Network Against Multi-Malware Threats: A Comprehensive Modeling and Analysis Approach." *SN Computer Science* 6, no. 3 (2025): 236.

[4]. Ghadi, Yazeed Yasin, Tehseen Mazhar, Tamara Al Shloul, Tariq Shahzad, Umair Ahmad Salaria, Arfan Ahmed, and Habib Hamam. "Machine learning solutions for the security of wireless sensor networks: A review." *Ieee Access* 12 (2024): 12699-12719.

[5]. Sadia, Halima, Saima Farhan, Yasin Ul Haq, Rabia Sana, Tariq Mahmood, Saeed Ali Omer Bahaj, and Amjad Rehman Khan. "Intrusion detection system for wireless sensor networks: A machine learning based approach." *IEEE Access* 12 (2024): 52565-52582.

[6]. Ngo, Quoc-Dung, Huy-Trung Nguyen, Van-Hoang Le, and Doan-Hieu Nguyen. "A survey of IoT malware and detection methods based on static features." *ICT express* 6, no. 4 (2020): 280-286.

[7]. Zhou, Haiping, Shigen Shen, and Jianhua Liu. "Malware propagation model in wireless sensor networks under attack–defense confrontation." *Computer Communications* 162 (2020): 51-58.

[8]. Aslan, Ömer Aslan, and Refik Samet. "A comprehensive review on malware detection approaches." *IEEE access* 8 (2020): 6249-6271.

[9]. Kumar, Parmod, Anupam Baliyan, K. Ramalingeswara Prasad, N. Sreekanth, Parag Jawarkar, Vandana Roy, and Enoch Tetteh Amoatey. "Machine learning enabled techniques for protecting wireless sensor networks by estimating attack prevalence and device deployment strategy for 5G networks." *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 5713092.

[10]. Huang, Xiang, Li Ma, Wenyin Yang, and Yong Zhong. "A method for windows malware detection based on deep learning." *Journal of Signal Processing Systems* 93, no. 2 (2021): 265-273.

[11]. Akhtar, Muhammad Shoaib, and Tao Feng. "Evaluation of machine learning algorithms for malware detection." *Sensors* 23, no. 2 (2023): 946.

[12]. Li, Shanxi, Qingguo Zhou, Rui Zhou, and Qingquan Lv. "Intelligent malware detection based on graph convolutional network." *The Journal of Supercomputing* 78, no. 3 (2022): 4182-4198.

[13]. Xing, Xiaofei, Xiang Jin, Haroon Elahi, Hai Jiang, and Guojun Wang. "A malware detection approach using autoencoder in deep learning." *Ieee Access* 10 (2022): 25696-25706.

[14]. Khan, Tayyab, Karan Singh, Khaleel Ahmad, and Khairol Amali Bin Ahmad. "A secure and dependable trust assessment (SDTS) scheme for industrial communication networks." Scientific Reports 13, no. 1 (2023): 1910.

[15]. Jangir, Mahendra Kumar, Karan Singh, Tayyab Khan, and Ali Ahmadian. "CATER: Congestion Aware Trust-Enabled Routing for Energy-Constrained Wireless Sensor Networks." *Computer Networks* (2026): 112030.

[16]. Khan, Tayyab, Karan Singh, Bhoopesh Singh Bhati, Khaleel Ahmad, Amal Al-Rasheed, Masresha Getahun, and Ben Othman Soufiene. "Trust-driven approach to enhance early forest fire detection using machine learning." *Scientific Reports* 15, no. 1 (2025): 14480.

[17]. Khan, Tayyab, Karan Singh, and Kamlesh C. Purohit. "ICMA: An efficient integrated congestion control approach." Recent Patents on Engineering 14, no. 3 (2020): 294-309.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug099

[18]. Khan, Tayyab, Karan Singh, Sakshi Gupta, and Manisha Manjul. "Multi Trust-based Secure Trust Model for WSNs." *Journal of Information Technology Management* 14, no. Special Issue: Security and Resource Management challenges for Internet of Things (2022): 147-158.

[19]. Dohare, Indu, Karan Singh, Tayyab Khan, Yogendra Mohan, and Intyaz Alam. "Coati optimization algorithm for node localization in sensor enabled-IoT." *Cluster Computing* 28, no. 4 (2025): 221.

[20]. Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks." *Ieee Access* 7 (2019): 58221-58240.

[21]. Khan, Tayyab, and Karan Singh. "SE-TEM: Simple and Efficient Trust Evaluation Model for WSNs." *The Smart Cyber Ecosystem for Sustainable Development* (2021): 111-130.

[22]. Kim, Jin-Young, and Sung-Bae Cho. "Obfuscated malware detection using deep generative model based on global/local features." *Computers & Security* 112 (2022): 102501.

[23]. Salem, Aya H., Safaa M. Azzam, Omar E. Emam, and Amr A. Abohany. "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques." *Journal of Big Data* 11, no. 1 (2024): 105.

[24]. Behiry, Mohamed H., and Mohammed Aly. "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods." *Journal of Big Data* 11, no. 1 (2024): 16.

[25]. Rey, Valerian, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, and Gérôme Bovet. "Federated learning for malware detection in IoT devices." *Computer networks* 204 (2022): 108693.

[26]. AlSobeh, Anas MR, Khalid Gaber, Mahmoud M. Hammad, Maryam Nuser, and Amani Shatnawi. "Android malware detection using time-aware machine learning approach." *Cluster Computing* 27, no. 9 (2024): 12627-12648.

[27]. Kok, S. H., Azween Abdullah, and N. Z. Jhanjhi. "Early detection of crypto-ransomware using pre-encryption detection algorithm." *Journal of King Saud University-Computer and Information Sciences* 34, no. 5 (2022): 1984-1999.

[28]. Woźniak, Marcin, Jakub Siłka, Michał Wieczorek, and Mubarak Alrashoud. "Recurrent neural network model for IoT and networking malware threat detection." *IEEE Transactions on Industrial Informatics* 17, no. 8 (2020): 5583-5594.

[29]. Khan, Tayyab, Karan Singh, Mohd Shariq, Khaleel Ahmad, K. S. Savita, Ali Ahmadian, Soheil Salahshour, and Mauro Conti. "An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach." *Computer Communications* 209 (2023): 217-229.

[30]. Khan, Tayyab, and Karan Singh. "Resource management based secure trust model for WSN." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 8 (2019): 1453-1462.