International Journal of AI, Big Data, Computational and Management Studies
Noble Scholar Research Group | Volume 3, Issue 1, PP. 140-149, 2022
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I1P116

Towards Secure and Reliable IoT: A Review on Anomaly Detection and Predictive Analytics in Sensor Networks

Srikanth Reddy Keshireddy[1], Venkata Teja Nagumotu[2], Harsha Vardhan Reddy Kavuluri[3], Akhil Kumar Pathani[4], Ajay Dasari[5], Venkata Kishore Chilakapati[6]
[1]Senior Software Engineer, Keen Info Tek Inc.
[2]Sr Network Engineer,Techno-bytes Inc.
[3]Lead database administrator,Wissen infotech.
[4]Network Engineer,Ebay.
[5]Senior Support Engineer,Microsoft.
[6]Technical Advisor,Microsoft.

Abstract: As IoT sensor networks spread into new domains like smart cities, healthcare, industry, transportation infrastructure, and environmental monitoring, predictive analytics and anomaly detection have taken centre stage in improving the security, reliability, and continuity of these networks. The raises in data volumes, distributed designs, non-homogenous sensing instruments, and real time decision needs augment the hazards of sensor faults, cyberattacks, spoofing, data drift, noisy of interfering data, and miscalibration. Smart analytical processes are thus important in detecting abnormal patterns and predicting failures and trusted sensing environments. In this review, the traditional statistical methods, ML methods, and the latest DL and hybrid models are examined in terms of accuracy, scalability, computing footprint, and the ability to be deployed at an edge, fog, and cloud layer. The latest developments such as federated learning, adaptive contextual models, transfer learning, edge intelligence, and automated thresholding are discussed as opportunities to decrease false alarms and increase detection accuracy. This paper also identifies the issues associated with the lack of data sets, the problem of inconsistency of benchmarking, streaming data processing, and measurement scales. The general synthesis shows that combining anomaly detection and predictive analytics can be used to build proactive maintenance, risk mitigation and resilient IoT performance in more dynamic and interconnected environments.

Keywords: Internet Of Things (IoT), Anomaly Detection, Predictive Analytics, Sensor Networks, Cybersecurity, Machine Learning.

1. Introduction

With the advancement of IoT technologies, a diverse spectrum of intelligent and small wireless sensing devices will be employed in a number of application scenarios. Having the nature of the sensor devices [1], as the backbone of IoT ecosystems, this type of sensor devices is necessarily constrained in terms of the energy resources it can utilize, processing and storage capacities, and the radio range and reliability of communication. In spite of these drawbacks, the IoT applications usually require real-time functionality and little or no human intervention. In order to guarantee the adequate operation and sustainability of such devices e.g. monitoring sensor performance or issuing remote commands, it is essential to develop efficient and reliable communication protocols that take control of sensor nodes without creating high resource overheads [2].

The main vision of IoT is to make everything, people, devices, and smart systems connected efficiently wherever and when needed regardless of the network. The implication of this vision is the continually growing variety of IoT applications that continue to saturate the entire scope of human life. Nevertheless, the current trend of integrating wireless sensor networks (WSNs) into IoT ecosystems presents a major security and reliability risk to the mission-critical applications. There are several types of attacks prone to the WSN, and they may be classified as data tampering, node compromise, DoS attacks, and network eavesdropping that are significant threats to the integrity, confidentiality, and availability of IoT services [3].

To overcome such issues, contemporary IoT architectures are more dependent on the tools of ML and DL [4]. ML algorithms can optimise network performance, identify abnormalities, and anticipate potential problems by finding patterns in both historical and real-time sensor data. DL models, which possess the ability to automatically extract features and the ability to process high-dimensional data, are superior in complex pattern recognition, intrusion detection and fault prediction in massive sensor networks. Combined, ML and DL can provide greater reliability, resilience, and security to the IoT system and allow managing it proactively instead of reactively.

Predictive analytics and anomaly detection is therefore part and parcel of secure and reliable IoT implementations. The anomaly detection methods can detect abnormal or suspicious activities within the network traffic and sensor data, thereby enabling the detection of the attacks or system failures early [5]. Predictive analytics relies heavily on looking at historical

sensor data to make predictions about machine failures, boost maintenance efficiency, and guarantee a constant flow of IoT services. These methods, combined with ML and DL, will make it possible to conduct intelligent, automated, and energy-efficient decisions in sensor networks. After summarizing the advantages of ML- and DL-based approaches, this review will examine the recently emerging trends that include edge intelligence, federated learning, and energy-efficient predictive models.

1.1. Structure of the Paper

The paper will be organized as the following: Section II will address the issues of security and reliability and concepts of IoT and sensors. Section III describes what anomaly is and what kind of anomaly is and why it is relevant. Section IV provides the survey of statistical, machine, deep and hybrid learning methods and their application in various industries. In section V, there is a literature synthesis and research gaps. Section VI is a conclusion and indicates the directions in the future.

2. Security and Reliability Challenges in IoT Sensor Networks

IoT networks are vulnerable to hardware, software, protocol, and network threats, whereas reliability is problematic due to correlated, random, and human-induced failures. These vulnerabilities and how to create secure, resilient architectures, such as physical, network, and application layers, are important to ensure continuity of operations, lessening of disruptions, and reliability, long-term functionality of distributed compositions of IoT sensors.

2.1. IoT and Sensor Networks: Concepts and Architecture

IoT refers to the trillions of real-life objects that are interconnected with the Internet and global storage and data transfer. Anything between a pill and an aircraft can now be converted into a component of the IoT By connecting and attaching sensors to all of these various things, the AI used on otherwise dumb devices can share real-time information without a human required. The IoT architecture serves as a gateway to other hardware applications, enabling the expansion of IoT services at every door. Various networking protocols are adhered to like Bluetooth, Wi-Fi, RFID, narrow and broadband, ZigBee, LPWAN to pass and obtain information/data across the various layers of the Io architecture. The most common IoT architecture is a result of three layers, namely, physical, network, and application layers that visualized in Figure 1 and describes following:

- Sensor/Physical Layer: The properties of this layer are sensing, and the knowledge of the world where intelligent objects are present is obtained and accumulated.
- Network Layer: This layer functionalities provide the opportunity to transmit and process the data with the utilization of the internet access of the various devices.
- Perception Layer: This layer has an important role in offering the user a specific application service. It manages convenient applications, including mobile applications and Web portals, and offers information processing, analytics services, and interaction with users, e.g. switching a light on using a smartphone.

Figure 1: The Architecture of IoT Layers[6]

A sensor is an electrical device that can detect and produce an electric signal in response to external physical events or stimuli. The small sensors that comprise a WSN are equipped with memory, processors, and the ability to communicate wirelessly across short distances. The sensor nodes coordinate their activities to collect and compile information on the observed phenomena [7]. The typical layout of a WSN is shown in Figure 2. It mainly consists of three kinds of nodes: sensors, sinks, and gateways. Sensors collect data directly from the environment, whereas sinks aggregate that data and relay it to applications via the gateway. This last one acts as a go-between for the WSN and the outside world by converting and mapping protocols; it has two network interfaces. Common names for the co-located sink and gateway are "sink" and "gateway," respectively. Figure 2 shows WSNs in great detail.

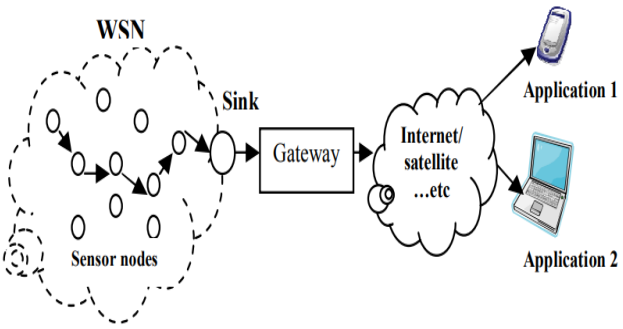

Figure 2: Wireless Sensor Network[8]

2.2. Security Threats in IoT

IoT links the digital and physical realms, which poses new security concerns to established methods. Attack vectors shift from data manipulation to command and control (the physical world becoming more intertwined with the digital) because of this, which has far-reaching consequences for safety.

2.2.1. Hardware Threats

The architecture allows for the interconnection of heterogeneous IoT devices. The attacker may potentially compromise the devices based on their features. These gadgets may be used with two different schemes

- Low Configured Device Attack: Low-end configuration devices are defined as those with lower memory storage, energy, and computational capacity [9]. These improperly configured devices are used by the attacker together with other IoT devices.
- High-End Device Attack: A high-quality gadget is an indication of a powerful and entirely practical instrument. The goal of an attacker targeting high-end devices (e.g., PCs and laptops) might be to cause widespread damage to other networks and devices, leading to a significant financial loss.

2.2.2. Software Threats

Some of the most vulnerable parts exploited in the IoT environment include software vulnerabilities. There are two widespread forms of software-based attacks, which are:

- Botnets: Hackers can exploit IoT gadgets and form a network of nodes with viruses, which are also referred to as bots. They are commonly employed to institute massive DDoS assaults, seize services or transmit malware to other connected systems.
- Man-in-the-Middle (MITM): The attackers in this attack intercept and compromise communication between the IoT device and the servers. In the process, they are able to compromise confidentiality and integrity of the IoT network as shown in the Figure 3.

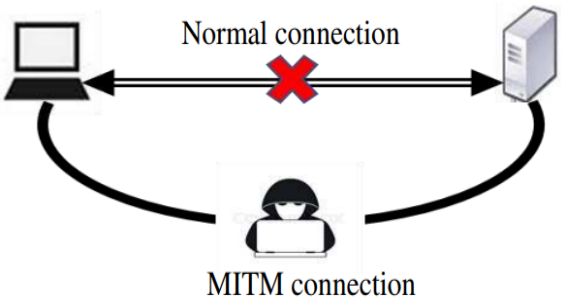

Figure 3: MITM Attack Scenario[10]

2.2.3. Protocols Attacks

Additionally, malicious actors may disrupt the different IoT devices via protocol assaults.

- Protocol Abnormality: An adversary joins in on important conversations or uses programmable protocols to become an insider and report many bots.
- Protocol Distraction: An adversary might potentially disrupt many protocols involving key management, data collecting, or synchronisation from either internal or external devices.

2.2.4. Networks Threats

DoS and spoofing are only two examples of the many network assaults that might affect an IoT system.

- Denial-of-Service/Distributed (DoS) attack: This might render the provider inaccessible to its operators and prevent them from using the device, network, or software. This may also take many other forms [11]. A large amount of network traffic and its spread might be used to launch the assault.
- Spoofing: The practice of posing as a trusted source in order to deceive an unsuspecting network is known as spoofing. Emails, telecall phone calls, and websites are all susceptible to spoofing, as are technical aspects of computers, such as IP addresses, Address Resolution Protocol (ARP), and DomainName System (DNS) servers.

IoT systems have various threats in gadgets, programmes, protocols and networks. These vulnerabilities should be addressed to guarantee secure and reliable operation before thinking of larger issues of reliability.

2.3. Reliability Issues in IoT

An essential but so far underappreciated feature of IoT systems is reliability. The most significant threats to the dependability of IoT systems fall into four categories.

- Handling correlated failures: This is a type of failure that occurs in devices and across time. Spatial correlation occurs when a lot of devices experience similar conditions such as wireless congestions or temperature variations. The temporal correlation is when the effect propagates and affects devices sequentially, e.g. when moisture increases or crowds cause event bursts [12].
- Handling unpredictable failures: Most failures of IoT systems are unpredictable since energy may run out unexpectedly, small load surges may cause instability in the device because of low safety factors, and their failure modes are less familiar than those of server-scale systems.
- Debugging failures: Failure in IoT systems should be enabled to be debugged automatically, and the final emphasis should be on automation since the system is composed of many heterogeneous devices, which would impose a heavy burden on human cognition to debug [13].
- Human considerations: The presence of humans in many of these IoT devices creates a problem with dependability. This might have varying implications depending on the application and even the deployment of that application.

3. Anomaly Detection in Iot Sensor Networks

The anomaly detection in the IoT data will be vital in detecting the faults, cyberattacks, or suspicious trends. These anomalies can be global, contextual, and collective, and are made more difficult by high dimensional, unbalanced, and dynamic data streams. Monitoring facilitates high security, data integrity and reliability because it promotes proactive control and credible IoT network operations.

3.1. Importance of Anomaly Detection

In any modelled system, an anomaly is a non-predictive datum. Anomalies are rare instances or observations that do not conform to typical behaviour or patterns in one particular instance of data, in a particular situation, or in the whole data [14]. The goal of a detection algorithm is to pinpoint the exact location of an anomaly and classify or infer its source; in an ideal world, these abnormalities would have external origins, such as a malfunctioning sensor or an external attack.

An anomaly is any part of the data that deviates from the norm or does not exhibit the anticipated pattern or traits. Since anomalous occurrences contain important information and interests, anomaly identification is really crucial. Anomaly detection is also crucial for delivering other IoT services, such as security, data privacy, and sensor data compression [15]. Additionally, it is essential to strictly maintain QoS throughout the connection to ensure the quality of data, which might be biological images or signals, for real-time remote monitoring. One example is the need to suitably obscure an individual's energy consumption data in response to a privacy warning that is triggered when their smart meter data unexpectedly displays high energy use during the middle of the night.

3.2. Categories of Anomalies

The three main categories of anomalies are as follows:

3.2.1. Global/point anomaly

A global anomaly is a data point that differs greatly from the rest of the points in a certain collection. Therefore, in order to distinguish between typical points and outliers, an appropriate divergence evaluation is required. Since this class of anomalies is the most prevalent and simplest to spot, it is where most anomaly detection algorithms put their emphasis [16]. Global anomaly detection has several uses, including auditing systems for trade activities and intrusion detection.

3.2.2. Contextual anomaly

A contextual outlier is any data point in a dataset that drastically differs from the anticipated behaviour within the given context. Another name for anomalies that change depending on the circumstances is conditional anomalies. Consequently, the context has to be stated as part of the issue specification in order to discover contextual abnormalities. Data objects' properties are grouped into two groups in contextual anomaly detection:

- Contextual attributes: The object's context is defined by these qualities. Time and place are two examples of context.
- Behavioural attributes: This data point is evaluated for abnormality in its context using these attributes, which represent the object's properties.

3.2.3. Collective anomaly

A group anomaly occurs when a subgroup of data items in a given set deviates significantly from the set as a whole. No outliers may be present in the specific data items [17]. Collective anomaly detection requires us to consider the behaviour of both individual items and groups of objects, in contrast to global or contextual anomaly detection. To find collective anomalies, it is also necessary to have prior information about the connection between the data items, such as distance or similarity measurement.

3.3. Challenges in Anomaly Detection for IoT Systems

The process of detecting data anomalies in IoT is complicated by the peculiarities of the data presented in the IoT and constraints imposed by the conditions of an IoT setup. The main challenges include:

- High dimensionality: IoT data is associated with a large number of sensors and a mixed nature of sources, which creates conjugated feature spaces that render the detection of anomalies challenging. Reducing the dimensions of data is often required to ease the analysis.
- Scalability: IoT systems produce high amounts of real time data. Algorithms used to identify them should be able to process high velocity streams effectively and work on a scalable computational and storage infrastructure [16].
- Imbalanced data: IoT datasets are unbalanced by definition as anomalies are much rarer than regular patterns. This may skew models to the majority group and one method of increasing the detection of rare anomalies is the oversampling or under sampling technique.
- Concept drift: IoT environments are constantly changing, and as a result, there is a change in data trends. The model being trained using the previous data might fail to be accurate as new behaviours arise and therefore constant adaptation is required [18].
- Privacy and security: IoT data may include sensitive information, and therefore the method of anomaly detection should not infringe on privacy and provide data protection without affecting the detection performance.

The challenges cannot be well addressed without the creation of advanced algorithms and frameworks that will be able to handle high-dimensional streaming information, learn over changing environments, defend privacy, and enable real-time anomaly detection.

4. Predictive Modeling in IoT Sensor Networks

Predictive models are based on statistical, machine learning, deep learning, and hybrid prediction to predict failures, detect anomalies, and optimize IoT performance. Its applications include machinery health, industrial automation and sensor security as well as smart-city infrastructure. Predictive analytics allow to prevent failures with timely analysis, make decisions, and enhance the resilience of nonhomogeneous IoT systems.

4.1. Techniques for Anomaly Detection

The IoT sensor networks use a variety of methods for spotting outliers.

4.1.1. Statistical Approaches

A statistical method applies statistical procedures and quantitative data in order to interpret information, identify patterns, and make conclusions.

- ARIMA (Autoregressive Integrated Moving Average): ARIMA is a common model because it is easy to use and can be used to represent the linear relationships within a time series data set. It combines autoregressive (AR) and moving average (MA) terms [19], which makes it be able to explain trends and seasonal changes in the series after differencing the series.
- ETS (Exponential Smoothing State Space Model): ETS models are formulated to explicitly represent level, trend and seasonality, not requiring the differencing.

4.1.2. Machine Learning

Machine learning enhances the functions of AI systems because it helps computer systems learn by experience through data and algorithms [20]. Some of the ML approaches that were employed in the detection of anomalies in the IoT systems were described as follows:

- Decision Trees: This is a Nonparametric classification and regression model that produces models that can be easily understood as if-then-else statements.

- Support Vector Machines (SVMs): The support vectors possess sturdy classifiers and regressors that identify optimum hyperplanes to in order to discriminate classes in high-dimensional spaces. It is Outlier resistant and works well with high-dimensional data.
- Random Forest: An ensemble learning technique, Random Forest randomly constructs decision trees to improve predicting accuracy. It works to reduce overfitting through averaging of trees.

4.1.3. Deep Learning

Machine perception and learning of diverse and complicated data are being transformed by deep learning. Similar to neural networks in the human brain, deep learning enables computers to autonomously identify patterns and provide wise decisions from huge unstructured information. Artificial Neural Networks (ANNs): ANNs are based on biological neuronal networks [21], using nonlinear data modelling techniques that are statistical.

CNN (Convolutional Neural Network): CNNs are generally used to process images; however, by treating a sequence of data as a sequence of images, it has been applied to time series processes, too. LSTM (Long Short-Term Memory): The LSTM networks represent a variation of sequential data RNN that are more effective when short-term dependencies on long-term sequence underlying patterns are required.

4.1.4. Hybrid Methods

Hybrid models are models that involve the use of more than one method to exploit the strengths of different methods to increase the level of accuracy in prediction [22]. As an illustration, when a machine learning technique is combined with ARIMA, it would be possible to capture both linear and non-linear aspects of the data. Benefits: Better resistant to data variations, and enhancing accuracy and generalizability. Debits: More complex to implement and tune parameters. The combination of multiple models will increase training time.

4.2. Applications in Smart Environments

Machine learning improves smart environments to make them predictive in maintenance, intelligent in automation, and capable of detecting anomalies, as well as carrying out secure IoT operations in various industries.

4.2.1. Monitoring the Health of Machinery

Machine learning is critical in rotating machinery monitoring, where failures are normally caused by bearing subsystem failures. Recent studies [23] focus on vibration signal analysis with the help of acceleration measurement to identify bearing health and fault location. The advanced signal processing allows creating informative features that differentiate the type of faults and their severity. A multilayer perceptron (MLP) neural network-based diagnostic system that employs a Bayesian automatic relevance determination increases classification accuracy. Relevance based feature selection (Bayesian relevance) helps to find an optimal combination of features to detect faults and enhance reliability.

4.2.2. Robotics or Manufacturing Applications

ML is becoming highly used in robotics to assist very customized manufacturing processes that have to be automated with minimal human interaction. One of the study [24] suggested frameworks combines deep learning techniques with superior physics-based simulation environments, which realistically correspond to real world forces, elasticity, and working behaviours. This simulated data can be efficiently programmed and parameterized in new production tasks. Simulation allows tasks to be learned faster than they can be done in reality whilst the current operations proceed. The practicality of this simulation-based ML model is supported by an industrial case analysis, which demonstrates its promise.

4.2.3. Detection Applications for Iot Sensors

The growth of IoT infrastructures in domains also augers security risks and anomaly threats, which could cause failure of the system. According to [25], DT, RF, and ANNs are some of the algorithms that have been widely tested in detecting IoT attacks using ML models. The acc, prec, rec, F1score, and ROC-AUC are used to evaluate these models to enable reliable anomaly prediction. According to the experimental findings, DT, RF, and ANN models have a high test accuracy of 99.4, which indicates a high ability to detect IoT threats and ensure safe operation in connected sensor networks.

4.2.4. Smart-city IoT Applications

Smart cities are based on IoT ecosystems to improve city life yet the network traffic grows exponentially, providing new cybersecurity threats. Cloud-linked sensor infrastructures necessitate machine learning methods in identifying compromised devices. The work by [26] introduce AD-IoT system, a Random Forest anomaly detection model, detects infected IoT devices on the distributed fog nodes to suppress the spread of attacks. Modern dataset testing demonstrates that the model can attain a high classification rate of 99.34 percent with a small number of false positives. That indicates that ML-based detection solutions are efficient in ensuring safe, real-time smart city functionality. Table I represent these comparisons of ML in anomaly detection below.

Table 1: Comparison of Applications of IoT Anomaly Detection

Applied Domain	Objective	Techniques	Outcomes
Monitoring the health of machinery	Diagnose bearing subsystem faults to prevent machinery breakdowns	Vibration signal analysis, MLP, Bayesian determination, feature fusion	Enhanced fault identification accuracy
Robotics or manufacturing applications	Automate individualized production tasks	Deep learning, simulation-driven ML framework	Faster task mastery in simulation and a validated industrial automation
Detection applications for IoT sensors	Predict anomalies and attacks in IoT systems	Decision Tree, Random Forest, ANN	Achieved 99.4% accuracy for anomaly detection
Smart-city IoT applications	Detect compromised IoT devices to mitigate threats	AD-IoT anomaly detection using Random Forest	99.34% accuracy with low false positive rate

5. Literature Review

The literature reviewed examines the concepts of IDS, anomaly detection and machine-learn security schemes in the case of IoT and WSNs, presenting a limitation to real-time detection, fault differentiation, predictive reliability and resource efficient implementation.

Farooq, Beenish and Fahad (2019) The capacity to support various types of communication applications is a key feature of WSNs, which are large-scale ad hoc networks. Due to its broadcast nature, unsupervised environment, constraints, and security risks, WSN is vulnerable to several dangers. This problem is addressed in the proposed article by researching and comparing several IDS frameworks in order to determine which one is the most effective. In the study, a thorough literature overview of intrusion detection systems is offered together with information on their security needs, security risks, security assaults, and preventative techniques. Additionally, the difficulties of intrusion detection systems are examined [27].

Seo and Chung (2019) The proliferation of sensor data collected by IoT and WSNs, together with advancements in big data analysis tools, has made it possible for users to quickly and effectively make sense of and act upon massive data sets. Smart systems that do not need human input are likely to be susceptible to intrusions from outside networks, and infrequent sensor mistakes may cause them to fail in sustaining optimal settings. Consequently, this study proposes a way to maintain the optimum state in large data systems even if the sensor network fails owing to sensor failure or external interference [28].

Ramotsoela, Abu-Mahfouz and Hancke (2018) Adequate protection of Industrial WSN has become essential due to their expanding usage in many diverse applications, including those involving critical infrastructure. The failure of conventional network security measures is a real possibility; intrusion detection provides a workable solution. Because of its broad detection range and reduced resource needs, anomaly detection a subset of intrusion detection is well-suited for use in IWSNs. With a focus on machine learning techniques, this paper presents a literature overview of recent work in the field. The evaluated work addresses critical water infrastructure as an example of a use case and also highlights considerable research gaps regarding the practical feasibility of these systems [29].

Mamdouh, I. Elrukhsi and Khattab (2018) The network that houses actual appliances, sensors, and gadgets is called the IoT. One of the key components of the IoTs is WSN. These networks are unfortunately susceptible to several security threats. Because of this, ensuring the safety of the IoT and WSN is an absolute must. Devices utilised in these networks have limited resources, which further complicates the situation. A relatively recent and effective method for dealing with these problems is machine learning. Machine learning has a major influence on many solutions for IoT and WSN security systems. This article provides a high-level summary of the many threats that might affect WSNs and the Internet of Things, along with the main machine learning techniques used to counter these threats [30].

Zarpelão et al. (2017) The term "Internet of Things" (IoT) describes a system that connects many types of physical things to the web. While there are numerous advantages, there are also security concerns that arise as the number of Internet-connected gadgets in our everyday lives grows. A review of IDS studies pertaining to the IoT is provided in this paper. The goal is to identify emerging trends, unresolved problems, and potential avenues for future study. The IDSs recommended in the literature were categorised according to the following features: security threat, validation strategy, IDS placement strategy, and detection technique. The different options for each attribute were also described, along with works that either recommend specific IDS schemes for IoT or develop attack detection methods for possible IDS-embedded IoT threats [31].

Clarke and Al Shehri (2017) There has been a dramatic shift in the realm of information and communication technology (ICT) with the advent of WSNs. There have been several security incidents in sensor node applications because of their limited energy, storage, and computing capabilities. Consequently, several strategies and tactics have been suggested to address various vulnerabilities and assaults in order to meet security standards. This paper provides a comprehensive overview of WSN security

measures, including numerous attack types and the methods used to counter them. Finally, this study discusses the advantages and disadvantages of each method [32].

Table II demonstrates some major security research in the IoT and WSN field with weaknesses in IDS, anomaly detection, resource constraints, and discrepancies in predictive analytics, lightweight adaptive models, and real-world validation requirements.

Table 2: Summary of Literature Review Based On Anomaly Detection and Predictive Analytics in IoT Sensor Networks

Authors	Focus	Method	Findings	Challenges Identified	Recommendations
Farooq, Beenish and Fahad (2019)	Intrusion Detection Systems (IDS) for securing Wireless Sensor Networks (WSN)	Comprehensive literature review and comparative analysis of IDS frameworks	Identifies IDS types, security needs, threats, attacks and prevention techniques	Resource constraints, high false alarms, vulnerability due to broadcast nature, weak adaptiveness	Develop lightweight IDS models; enhance anomaly-based intrusion detection; integrate predictive analytics for proactive detection
Seo and Chung (2019)	Maintaining optimal IoT/WSN operation under sensor failure and intrusion	Proposed method for resilience in big data–enabled sensor networks	Demonstrates need for systems to remain stable despite anomalies or attacks	Difficulty distinguishing failure vs intrusion anomalies; limited autonomous response	Combine anomaly detection with predictive modelling; improve self-adjusting smart systems
Ramotsoela, Abu-Mahfouz and Hancke (2018)	Anomaly and intrusion detection in Industrial WSNs using machine learning	Literature survey with industrial infrastructure case context	Shows ML anomaly detection suitable for critical infrastructure with low resources	Lack of real-world deployments, dataset scarcity, scalability constraints	Validate in real industrial environments; develop ultra-light ML models for constrained sensors
Mamdouh, I. Elrukhsi and Khattab (2018)	Machine learning-based approaches to secure IoT and WSNs	Survey of ML solutions for IoT and WSN threats	ML enhances defence against evolving IoT/WSN attacks	Limited energy, memory, processing power; lack of adaptive and evolving learning models	Design lightweight adaptive ML models; integrate predictive security analytics
Zarpelão et al. (2017)	Intrusion Detection Systems for IoT and IDS classification strategies	Survey and classification framework based on detection methods, placement, threats and validation	Provides taxonomy and identifies trends in IDS for IoT	IoT constraints make traditional IDS unsuitable; limited focus on sensor anomaly behaviour	Develop IDS focused on IoT sensor anomalies; integrate predictive reliability and early-warning detection
Clarke and Al Shehri (2017)	Security challenges, attacks and countermeasures in WSN	Survey of WSN security approaches and vulnerability mitigation	Identifies attack types and evaluates defence strategies	Limited anomaly detection focus; lacks predictive threat handling; countermeasures not resource-aware	Combine anomaly detection with security models; introduce predictive analytics for proactive mitigation

6. Conclusion and Future Work

Predictive analytics and anomaly detection are essential in maintaining the security, reliability, and the efficiency of IoT sensor networks. Statistical, machine learning, deep learning and hybrid-based detection have their own advantages in fault, cyber threat and abnormal behavior detection in distributed sensing environment. It is still difficult to process high-dimensional, heterogeneous, and dynamic IoT data with low computational overhead and low energy consumption. The use of context awareness, adaptive thresholds and real time anomaly monitoring helps in enhancing accuracy of detection and resilience of the system. The predictive analytics and anomaly detection could be used together to create proactive maintenance, risks reduction, and stable operations in smart cities, industrial systems, and healthcare. The future work must focus on lightweight energy

efficient models that can stream analytics at the edge in real time with concept drift, uncertainty, and evolving sensor behavior mechanisms. Privacy-saving models, federated learning and transfer learning open opportunities to improve security and the scale of operations without violating sensitive information. Reproducibility and reasonable comparison of models require standardized datasets, protocols of benchmarking and non-instances of evaluation. Also, operational foresight can be enhanced by involving anomaly detection and predictive maintenance, digital twins, as well as autonomous decision-making systems. Academia, industry and regulatory bodies should work together to facilitate quick up-take and to achieve alignment to the real-world implementation needs to support resilient, intelligent and sustainable IoT sensor networks.

References

1. S. Gupta and C. Ravishankar, "Lower bounds for Arrangement-based Range-Free Localization in Sensor Networks," 2012.
2. Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT," *IEEE Access*, vol. 3, pp. 622–637, 2015, doi: 10.1109/ACCESS.2015.2435000.
3. K. Gopalakrishnan and B. Chander, "Security vulnerabilities and issues of traditional wireless sensors networks in IoT," in *Principles of internet of things (IoT) ecosystem: Insight paradigm*, Springer, 2019, pp. 519–549.
4. S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019, doi: 10.5281/zenodo.15362327.
5. M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.
6. M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, 2018, doi: 10.3390/s18092796.
7. J. Sen, "A survey on wireless sensor network security," *arXiv Prepr. arXiv1011.1529*, 2010.
8. M. El Barachi, A. Kadiwal, R. Glitho, F. Khendek, and R. Dssouli, "A Presence-based architecture for the integration of the sensing capabilities of Wireless Sensor Networks in the IP Multimedia subsystem," *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 3116–3121, 2008, doi: 10.1109/wcnc.2008.544.
9. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
10. H. I. Ahmed, A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," *Int. J. Adv. Comput. Res.*, vol. 9, no. 45, pp. 325–350, Oct. 2019, doi: 10.19101/IJACR.2019.940088.
11. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.
12. Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7946–7970, Oct. 2019, doi: 10.1109/JIOT.2019.2907245.
13. M. Ahmad, "Reliability Models for the Internet of Things: A Paradigm Shift," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, IEEE, Nov. 2014, pp. 52–59. doi: 10.1109/ISSREW.2014.107.
14. M. Rassam, A. Zainal, and M. Maarof, "Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: A Survey and Open Issues," *Sensors*, vol. 13, no. 8, pp. 10087–10122, Aug. 2013, doi: 10.3390/s130810087.
15. A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT Healthcare Analytics: The Importance of Anomaly Detection," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 994–997. doi: 10.1109/AINA.2016.158.
16. A. Chirayil, R. Maharjan, and C.-S. Wu, "Survey on Anomaly Detection in Wireless Sensor Networks (WSNs)," in *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, IEEE, Jul. 2019, pp. 150–157. doi: 10.1109/SNPD.2019.8935827.
17. D. ElMenshawy and W. Helmy, "Detection techniques of data anomalies in IoT: A literature survey," *Int. J. Civ. Eng. Technol.*, vol. 9, pp. 794–807, 2018.
18. S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2019, doi: 10.1109/ACCESS.2019.2962829.
19. E. Siow, T. Tiropanis, and W. Hall, "Analytics for the internet of things: A survey," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, 2018, doi: 10.48550/arXiv.1807.00971.
20. L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for Internet of Things," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 8, pp. 1399–1417, 2018.
21. X. Ma *et al.*, "A Survey on Deep Learning Empowered IoT Applications," *IEEE Access*, vol. 7, pp. 181721–181732, 2019, doi: 10.1109/ACCESS.2019.2958962.
22. G. M. Dias, B. Bellalta, and S. Oechsner, "A survey about prediction-based data reduction in wireless sensor networks," *ACM Comput. Surv.*, vol. 49, no. 3, pp. 1–35, 2016.
23. D. Kateris, D. Moshou, X.-E. Pantazi, I. Gravalos, N. Sawalhi, and S. Loutridis, "A machine learning approach for the

condition monitoring of rotating machinery," *J. Mech. Sci. Technol.*, vol. 28, no. 1, pp. 61–71, 2014.
24. M. El-Shamouty, K. Kleeberger, A. Lämmle, and M. Huber, "Simulation-driven machine learning for robotics and automation," *tm - Tech. Mess.*, vol. 86, no. 11, pp. 673–684, Nov. 2019, doi: 10.1515/teme-2019-0072.
25. Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. *Available at SSRN 5266517*.
26. Padur, S. K. R. (2020). From centralized control to democratized insights: Migrating enterprise reporting from IBM Cognos to Microsoft Power BI. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol*, *6*(1), 218-225.
27. Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, V., Enokkaren, S. J., & Attipalli, A. (2021). Systematic Review of Artificial Intelligence Techniques for Enhancing Financial Reporting and Regulatory Compliance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(4), 73-80.
28. Padur, S. K. R. (2019). Machine learning for predictive capacity planning: Evolution from analytical modeling to autonomous infrastructure. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *5*(5), 285-293.
29. Attipalli, A., Enokkaren, S., BITKURI, V., Kendyala, R., KURMA, J., & Mamidala, J. V. (2021). Enhancing Cloud Infrastructure Security Through AI-Powered Big Data Anomaly Detection. *Available at SSRN 5741305*.
30. Singh, A. A. S., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Predictive Modeling for Classification of SMS Spam Using NLP and ML Techniques. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 60-69.
31. Padur, S. K. R. (2020). AI augmented disaster recovery simulations: From chaos engineering to autonomous resilience orchestration. *International Journal of Scientific Research in Science, Engineering and Technology*, *7*(6), 367-378.
32. Reddy Padur, S. K. (2021). From Scripts to Platforms-as-Code: The Role of Terraform and Ansible in Declarative Infrastructure Rollouts. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 621-628.
33. Kothamaram, R. R., Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., & Maniar, V. (2021). A Survey of Adoption Challenges and Barriers in Implementing Digital Payroll Management Systems in Across Organizations. *International Journal of Emerging Research in Engineering and Technology*, *2*(2), 64-72.
34. Padur, S. K. R. (2018). Autonomous cloud economics: AI driven right sizing and cost optimization in hybrid infrastructures. *International Journal of Scientific Research in Science and Technology*, *4*(5), 2090-2097.
35. Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., Maniar, V., & Kothamaram, R. R. (2021). Anomaly Identification in IoT-Networks Using Artificial Intelligence-Based Data-Driven Techniques in Cloud Environmen. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(2), 83-91.
36. Padur, S. K. R. (2021). Bridging Human, System, and Cloud Integration through RESTful Automation and Governance. *the International Journal of Science, Engineering and Technology*, *9*(6).
37. Attipalli, A., BITKURI, V., KURMA, J., Enokkaren, S., Kendyala, R., & Mamidala, J. V. (2021). A Survey of Artificial Intelligence Methods in Liquidity Risk Management: Challenges and Future Directions. *Available at SSRN 5741342*.
38. Padur, S. K. R. (2021). From Control to Code: Governance Models for Multi-Cloud ERP Modernization. *International Journal of Scientific Research & Engineering Trends*, *7*(3).
39. Routhu, K. K. (2021). Harnessing AI Dashboards in Oracle Cloud HCM: Advancing Predictive Workforce Intelligence and Managerial Agility. *International Journal of Scientific Research & Engineering Trends*, *7*(6).
40. Padur, S. K. R. (2021). Deep learning and process mining for ERP anomaly detection: Toward predictive and self-monitoring enterprise platforms. *Available at SSRN 5605531*.