STM JOURNALS

Journal of
Polymer & Composites

ISSN: 2321-2810 (Online)
ISSN: 2321-8525 (Print)
Volume 14, Special Issue 3, 2026
DOI (Journal): 10.37591/JoPC

https://journals.stmjournals.com/jopc

Research JoPC

Cyber-Secure IoT Framework for Monitoring Fiber-Reinforced Polymer Composites Using Embedded Sensors

Pasuluri Bindu Swetha[1,*], Vandana Ahuja[2], Sunil Kr Pandey[3], Pacha Supriya[4], Sohan Das[5] and G. Nagaraj[6]

Abstract

The present research paper suggests a cyber-safe Internet of Things system in real-time monitoring of fiber-reinforced polymer composites with inbuilt sensors. It is aimed at enhancing structural health maintenance, using sensual, intelligent analysis, and data protection in the same platform. Multi-layer architecture An embedded sensor, signal processing, anomaly detection and lightweight layer of cyber-security are developed. Experimental validation is done under controlled conditions and the performance is measured by these measures as accuracy, latency and false alarm rate. A 5-fold cross simulation methodology is employed in order to ensure the strength and statistical consistency. The proposed framework achieves a detection accuracy of 94.3% with low false alarm rates and stable performance across varying conditions. The anomaly detection may also be added to increase the diagnostic capability, but the cyber-security layer offers the integrity of the data under the lowest latency overhead. As depicted using comparative analysis, the technique performs better than existing techniques of monitoring composite using IoT. The work has its foundation on the integration of cyber-security and smart polymer composite surveillance (in contrast to the conventional systems), which is concerned with the integrity and privacy of data. The architecture offers scalable and efficient architecture to the future generation smart composite structures. The future will be focused on massive implementation, advanced learning models and advanced security control against the advanced real world implementations.

Keywords: Fiber-reinforced polymer composites, Structural health monitoring, Internet of Things (IoT), Anomaly detection, Cyber-security

INTRODUCTION

Fiber reinforced polymer (FRP) composite materials have come out as the pillars in the contemporary engineering field because of the high strength to weight ratio, resistance to corrosion and flexibility of design. Such polymer based composites have now been widely used in aerospace, automotive, marine and civil infrastructure systems, where structural efficiency and durability are the important performance parameters [1]. In comparison with standard metallic structures, FRP composites have anisotropic mechanical behavior, which allows to design the structure to perform a specific way by orienting the fibers and choosing the matrix.

***Author for Correspondence**
Pasuluri Bindu Swetha

[1]Professor, Department of Electronics and Communication Engineering, Ravindra College of Engineering for Women (Autonomous), Kurnool, Andhra Pradesh, India
[2]Professor, Department of Computer Science and Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India
[3]Professor, Department of Information Technology, Institute of Technology & Science, Ghaziabad, Uttar Pradesh, India
[4]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India
[5]Assistant Professor, Department of Computer Science Engineering–Artificial Intelligence, Brainware University, West Bengal India
[6]Associate Professor, Department of Mechanical Engineering, Sethu Institute of Technology, Tamil Nadu, India

Received Date: April 06, 2026
Accepted Date: April 16, 2026
Published Date: May 09, 2026

Citation: Pasuluri Bindu Swetha, Vandana Ahuja, Sunil Kr Pandey, Pacha Supriya, Sohan Das and G. Nagaraj. Cyber-Secure IoT Framework for Monitoring Fiber-Reinforced Polymer Composites Using Embedded Sensors. Journal of Polymer & Composites. 2026; 14(Special Issue3): S434–S458p.

Nevertheless, this complexity also presents the problems of the internal damage mechanisms like interlinear delamination, matrix cracking, fiber breakage, and void formation, which tend to develop under the surface and are not noticed until the ultimate failure takes place [2].

The growing dependence on high-performance composite structures has consequently augmented the necessity to find strong structural health monitoring (SHM) tactics [3]. Such restrictions are especially severe in massive or unreachable composite structures in which the detection of defects at a young age becomes infeasible. As a result, the paradigm shift in terms of embedding sensing technologies in polymer composites has occurred to provide an in-situ mechanism of monitoring structural integrity in both the manufacturing and service life [4].

Embedded sensor networks are also available as fiber optic sensors, piezoelectric transducers, and thermal sensing elements offer a good avenue of real-time data capture inside the very fabric of the composite. These sensors have the ability to record strain distribution and temperature gradient and acoustic emissions to provide useful information on the development of internal damage conditions [5]. These sensing systems can be used together with an Internet of Things (IoT) architecture to support in-place transmission of data, remote monitoring and intelligent decision-making. The synthesis of IoT and smart composite materials has therefore established the basis of the next generation cyber-physical systems that can be used to assess the condition autonomously [6].

The solution to these developments is that with the introduction of IoT-based monitoring into composite systems, cyber-security has emerged as a very important, but frequently neglected issue. The overall industrial IoT (IIoT) environment is predisposed to a large number of cyber threats such as data interception, spoofing, unauthorized access, and denial-of-service attacks [7]. When it comes to composite monitoring, any damage assessment, maintenance, or even operational decisions made with compromised data integrity may be wrong. The risk is especially high in the safety-critical systems (like aerospace structures or wind turbine blades), where even the small failures in the monitoring data may have drastic effects [8].

The current studies in the field of composite SHM have primarily concerned increasing the accuracy of sensing and damaging signal processing and machine learning-based damage classification. But little focus has been drawn in assuring the data acquisition and the communication layers of these systems. The majority of IoT-related monitoring systems are based on the assumption that there is a trusted communication environment, which is not concerned with the possibility of adversarial interference and data manipulation [9]. Moreover, traditional cryptographic systems, although useful with general IT systems, can have enormous amounts of computational and energy overhead that cannot be tolerated by embedded sensor nodes with resource constraints within composite structures [10].

This is where the need to have a single framework that not only allows real-time monitoring of FRP composites with the help of embedded sensors but also allows the transmission of data over the IoT network to be secured and reliable. The solution to this dilemma lies in a delicate balance between the effectiveness of security measures and the efficiency of the system implemented, especially in those cases when embedded systems have to work within strict power and processing limitations. Furthermore, the framework should be in a position to support the fluctuation of dynamic working conditions whilst ensuring the data secrecy, integrity, and availability [11].

To address these issues, this paper suggests a cyber-secure IoT system to monitor fiber-reinforced polymer composite through embedded sensors. The suggested solution incorporates embedded sense devices with a lightweight, security-conscious IoT architecture that is focused on polymer composite applications. In contrast to traditional systems, the structure will integrate a multi-layered security component which is a combination of lightweight encryption, secure authentication algorithms and anomaly detection methods to secure data at all stages of its life-cycle, including the sensor level to edge and cloud processing levels.

ISSN: 2321-2810 (Online), ISSN: 2321-8525 (Print)

One of the major attributes of the suggested framework is the capability to conduct real-time damage assessment and at the same time provide cyber-resilience. The system is designed to capture high fidelity internal state data by embedding the sensors directly into the composite matrix with then intelligent algorithms used to process the collected data to detect internal defects at an early stage. Simultaneously, the security layer guarantees that all the data transmitted will be safeguarded against unauthorized access and tampering, which will improve the dependability of the monitoring results [12]. Incorporation of edge computing minimizes the latency even more and also limits data exposure, allowing quicker and safer decisions to be made.

The recent improvements in smart nanosystems, machine learning, and cyber-secure frameworks also support the importance of the integration of security-conscious IoT systems to composite monitoring. The role of sophisticated machine learning methods in improving the nanoscale devices fabrication and sensing efficiency, as highlighted by studies by Ahmad *et al.* (2026a, 2026b) directly relates to the case of the creation of embedded sensor networks in FRP composites. In this way, it is observed that Mamodiya *et al.* (2026) place significance on behavior-conscious cybersecurity solutions based on artificial intelligence and cryptographic intelligence to protect data in distributed IoT setup. Adaptive energy and control methods that can be adapted to changing conditions through reinforcement learning (Awad *et al.*, 2025; Kishor *et al.*, 2026) show that intelligent, self-optimizing systems can affect the real-time decision-making process in a changing environment, which is highly needed in continuous structural health monitoring. Moreover, the ability of data-driven models to respond to complex and real-life uncertainties is emphasized by machine learning-based studies of photovoltaic tracking systems in different scenarios (Ganguly *et al.*, 2025). All these works together provide a good base on how to design a cyber-secure, intelligent IoT framework that can provide real-time and reliable monitoring and protection of fiber-reinforced polymer composite structures.

This novelty of this work may be expressed in three main contributions. First, it introduces a single cyber-physical monitoring framework specifically focused on fiber-reinforced polymer composites, and that is the interface between material science and secure IoT. Second, it presents a lightweight security architecture that is specifically designed to work with embedded sensor networks, the shortcomings of the existing cryptographic solutions in resource-intensive settings. Third, it shows how it is possible to have secure and real-time composite monitoring with an integrated framework that balances sensing, communication, and security into a single system.

This study is able to contribute to the cutting-edge of smart composite monitoring by introducing the concept of cyber-security into the creation of the IoT-enabled SHM framework. The proposed framework will not only increase the reliability and the safety of composite structures but also will be in line with the overall vision of Industry 4.0, where smart, interconnected, and secure materials will be central to the next-generation engineering applications.

LITERATURE REVIEW

Structural Health Monitoring in Fiber-Reinforced Polymer Composites

The strength of fiber-reinforced polymer composites depends on how they are used and the conditions of the environment around them. 2.1 Structural Health Monitoring in Fiber-Reinforced Polymer Composites In general, the strength of fiber-reinforced polymer composites varies according to the application method and the environmental conditions surrounding the composite.

The structural health monitoring (SHM) of fiber-reinforced polymer (FRP) composite structures has continuously developed during the last twenty years. The initial jobs were based on external inspection techniques such as ultrasonic testing, radiography, infrared thermography in order to locate subsurface defects. Those were convenient ways to do things, but they were discontinuous. They required down times, excellent functioning, and are inclined to dismiss initial harm within layered polymer frameworks concealed in the initial phases [13].

As the composite structures became a part of aerospace and high-performance engineering systems the shortcomings of the periodic inspection started to show up. Damage to composite is not necessarily apparent. This micro cracks may take place in the matrix, delamination may develop between layers and fiber breakage may be propagated without making any noise. This has led to a change towards the continuous checking in schemes as part of the content itself [14].

In the meantime, scientists started enjoying the fact that composite material does not behave as metals. It is challenging to interpret damage because they are heterogeneous and anisotropic in nature. In turn, SHM systems of composites should be more sensitive, localized, and adaptive than traditional solutions.

Embedded Sensing Technologies in Polymer Composites

These sensors are highly sensitive to strain and temperature change and are comparatively free of electromagnetic noise that is beneficial in an industrial setting [15]. Another category that is interesting is piezoelectric sensors. They are typically operated to perform acoustic emission measurement, which measures a transient signal produced by crack initiation or breaking fibers. The signals give an early warning of macroscopic damage before it is manifested [16]. These benefits notwithstanding, it is not a simple task to incorporate sensors in composites. Sensors can cause local stress fields to be perturbed. Fading the signal through the matrix can reduce the sharpness of the measurements. Over time sensor deterioration by repeated loading cycles can occur. The placement strategy and protection encapsulation optimization have been explored, whereas the stability over time remains the research topic [17]. Multi-sensor fusion techniques have also been proposed. Instead of working with a single form of sensing to work with, strain, thermal, and acoustic signals are employed by the systems to improve detection. This multi-modal sensing is potentially extremely useful when considering complex composite systems in which one mechanism of damage is dependent on another.

Data Processing and Intelligent Damage Detection

As the technological aspects of sensing were enhanced, the importance of interpreting the information obtained was placed at the forefront. Comprehensively archaic doorstep methods were simple but generally imprecise. They were good at abrupt change response but the degradation trend (which is gradual) that is characteristic of composit materials was hard to feel [18].

It has been suggested that machine learning methods can be used to address this. The support vector machines, decision trees etc and more recently the deep neural networks have been instantiated in order to be able to classify the damage states. Spatial data are identified with convolutional networks and temporal changes with defects in sensor data are identified with recurrent networks [19].

Nevertheless, lots of implementations are offline. Information is gathered, placed, and examined in the future. This slows down the process of decision-making and restricts applicability in real-time in safety-critical settings [20].

A second issue is that of variability in data. Composite materials can work in a variety of environmental conditions: change in temperature, mechanical stress, and exposure to moisture. Machine learning models that have been trained in controlled settings might not be very well applicable to real-life situations.

IoT Integration for Smart Composite Monitoring

Internet of Things (IoT) has transformed the design of composite monitoring systems. Modern systems employ a network of sensor units that are linked together (in contrast to isolated units), and linked together using wireless protocols. Information may be sent to edge devices or cloud systems to process it [21]. Smart IoT-based structures can be used to monitor without being handled by humans. They are in favor of predictive maintenance, in which possible failures are detected in advance. IoT has also been employed in polymer composite production by monitoring the curing conditions and optimizing the production process [22]. These benefits do have trade-offs, however. Network latency The latency of a network can affect real time performance. Banded data might be an issue with high frequency data. Packet loss and communicational error can affect the reliability. Magnification of such problems is increased in large scale applications e.g. wind turbine blades or aerospace structures [23].

Cyber-Security Challenges in IoT-Based SHM Systems

The positive sides of IoT can be seen in its connectivity, however, there are also some weak points. Industrial internet is vulnerable to cyber-attacks. Unauthorized access, data interception and spoofing are cyberattacks that may impact on the operations of the system and manipulate the monitoring information [24]. Of particular concern are these in the framework of composite SHM. Damage measures are erroneous in case sensor data is altered or frozen. This can lead to a bad operating decision or postponed maintenance. However, despite all the mentioned risks, the majority of the current models of SHM assume the safe channel of communication, which cannot possibly hold true in the actual implementation [25]. Lightweight cryptographic methods have been one entry point to this problem. Simpler AES and elliptic curve cryptography (ECC) are algorithms which allow to trade off between security and performance [26] [27]. However, it is difficult to apply these methods to embedded sensor nodes because of the limited processing and energy needs.

Emerging Directions: Edge Computing and Secure Architectures

New opportunities are provided by recent advances in edge computing. Edge devices decrease the latency by processing data nearer to the sensor, as well as reducing the data transmission distance (over long distances). This does not only enhance response time but also exposure to cyber threats is minimized [28]. There is also an increase in the use of cyber-physical system (CPS) frameworks. These systems are a combination of physical sensing and computational intelligence systems with communications networks. CPS may also be used in polymer composite systems to provide adaptive monitoring, where the system is dynamically controlled depending on the real-time conditions [29]. There are also proposals of blockchain-based solutions. They offer tamper-proof and decentralized storage of data. They however are less appropriate in embedded composite environments due to their computation burden. On the same note, protocols that can communicate efficiently in terms of consuming less energy have been developed, although incorporating them with powerful security mechanisms is a complicated issue [30].

Summary of Research Gap

A close examination of the available literature shows that there is a pattern. There is a major advance in sensing technologies, data analytics and IoT-based monitoring. However, these elements are usually established separately. There is evidently a lack of a single framework that can be used that will correlate with embedded sensing, real-time monitoring, and cyber-security in fiber-reinforced polymer composites. The current systems have either been built around accuracy and no security or security but not taking into account the limitations of embedded systems.

An organized review of the current literature in monitoring of polymer composite materials shows that even though a substantial advancement has been achieved in embedded sensing, IoT-based structural health monitoring as well as intelligent damage prediction; these contributions usually have a scattered focus. Some papers are on sensor integration and material-level intelligence, and others give an emphasis on IoT architectures or cyber-security mechanisms on their own. Nevertheless, there is yet to be a unified framework that incorporates embedded sensing into fiber-reinforced polymer composite, real-time monitoring based on IoT and high-performance and reliable cyber-secure communication. In order to put this gap into more perspective, Table 1 (see below) provides a comparative analysis of some representative studies, their methodological strengths, limitations that have been observed, and their applicability to the proposed research framework.

Table 1. Comparative Literature Gap Analysis of IoT-Enabled and Embedded Sensing Approaches for Fiber-Reinforced Polymer Composites Monitoring.

S. No.	Author(s) / Year / Ref. No.	Focus Area	Methodology	Key Findings	Limitations / Gaps	Relevance to This Study
1	Nagaraj *et al.* / 2026 / [6]	Smart FRP composites with IoT	Embedded sensors + ML	Predictive damage monitoring achieved	No cyber-security layer	Extends to secure IoT-based composite monitoring
2	Lopes *et al.* / 2024 / [11]	Smart CFRP monitoring	Online SHM sensing	Continuous damage detection possible	Lacks secure data transmission	Supports need for real-time secure SHM
3	Karuppusamy *et al.* / 2025 / [19]	IoT in polymer composites	IoT-based monitoring review	Improved monitoring efficiency	No implementable secure framework	Basis for IoT integration in composites
4	Musa *et al.* / 2025 / [20]	Embedded sensors in composites	Sensor review (SHM)	Enables in-situ monitoring	No IoT-security integration	Supports embedded sensing layer
5	Musa *et al.* / 2023 / [25]	FBG sensing in FRP	Optical embedded sensors	Accurate strain/temperature sensing	No IoT or security focus	Useful for sensor selection
6	Li *et al.* / 2025 / [26]	Multi-sensor SHM	Sensor fusion	Improved defect detection	No cyber-secure architecture	Supports multi-sensor integration
7	Anuar *et al.* / 2025 / [16]	IoT cyber-security	ML + encryption	Enhanced IoT security	Not composite-specific	Provides security foundation
8	Lemartinel *et al.* / 2025 / [30]	Polymer composite curing monitoring	Embedded nano-sensors	Internal process monitoring	No IoT + security integration	Extends toward lifecycle monitoring

This gaps allows defining the necessity of an interconnected solution, i.e., the integration of efficient sensing, intelligent processing, and a solid cyber-security into a unified framework. The latter type of structure is necessary to facilitate effective and safe monitoring of the upcoming generation composite structures.

METHODOLOGY

This section describes the experimental approach to be used in developing and testing a cyber-secure Internet of Things to monitor fiber-reinforced polymer composite through embedded sensors. The design is designed in such a way that its implementation is real-world as opposed to theoretical design and the design combines the manufacture of composite specimens, the deployment of embedded multi-sensors, real-time data collection, and secure communication systems in a single workflow.

Experimental Framework Overview

The suggested methodology was created as a hybrid experimental pipeline, which is an integration of embedded sensing, IoT-based data collection, and cyber-secure communication of fiber-reinforced polymer composites and structures. The workflow was not addressed as a conceptual abstraction, rather it was physically executed with embedded sensor networks on composite specimens, and then the real-time data were gathered and sent securely. Figure 1 provides the general system architecture whereby sensing, edge processing and secure communication layers are closely connected. As compared to the traditional SHM systems, the current framework system integrates sensing directly into the polymer composite structure, and at the same time, it enforces a secure data processing at each step [19], [20].

The experimental pipeline consists of four sequential stages:
(i) composite specimen creation comprising of built-in sensors,
(ii) multi-sensor data acquisition,

(iii) edge-based preprocessing and anomaly detection, and
(iv) achieve IoT communication and storage security.

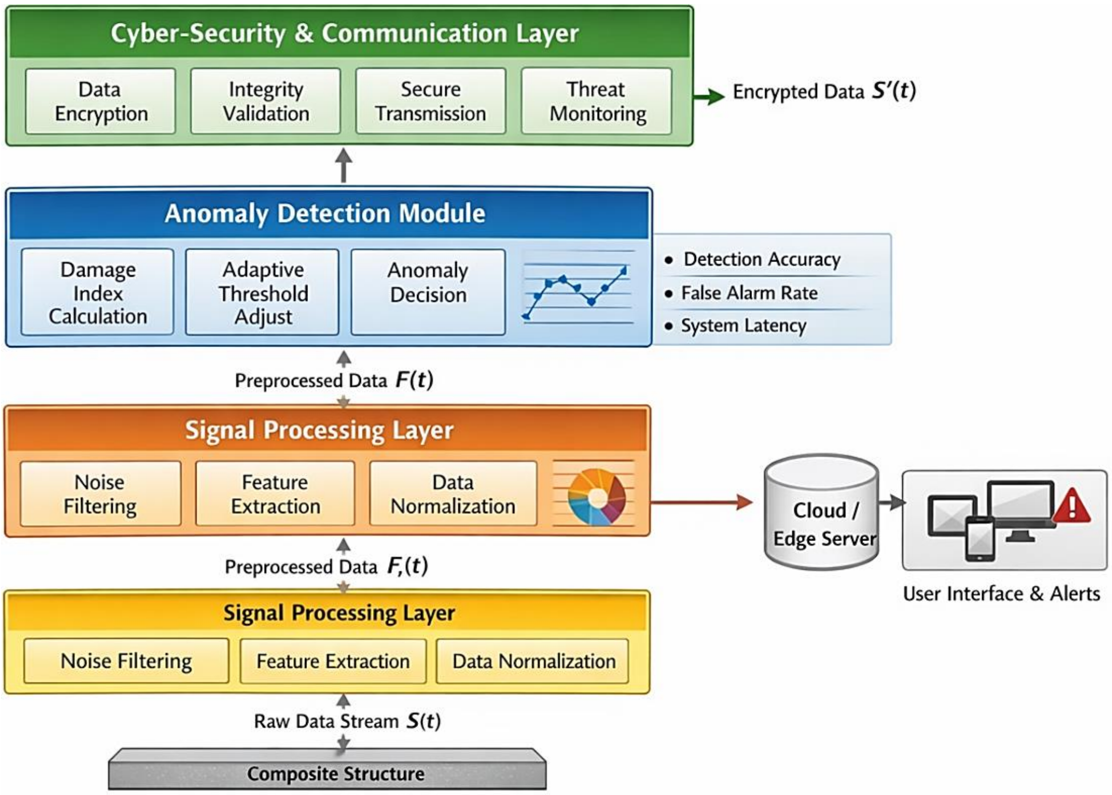

Figure 1. Cyber-secure IoT-based embedded sensing architecture for fiber-reinforced polymer composites monitoring.

Composite Specimen Fabrication and Sensor Embedding

The embedding of the sensors was done in the actual lay-up. They were not placed on the surface of the lamina between the interfaces of the two lamina where the sensor was attached but were interposed inside the body between distinct selections to measure structural changes within. The people were not placed randomly. It was steered by anticipated focus areas of stress, particularly areas that were likely to become delaminated or there was a possibility of interfacial failure. The utmost care was taken to prevent fiber misalignment and resin rich pockets during embedding since they could lead to distortion of both mechanical behavior and signal fidelity [11].

The various sensing modalities were combined in order to measure different physical parameters. FBG sensors were implanted in mid-layers to check the strain and temperature changes. Piezoelectric sensors were placed on the vicinity of important interfaces in order to sense acoustic emission near crack initiation. In addition to this, outer layers had resistive strain gauges to measure world trends in deformation. One of the purposes that was selected was multi-sensor configuration, because single-sensor layouts do not necessarily have the capability to measure the multi-scale damage mechanisms that polymer composites have [26].

The sensor layout stored in Table 2 is the last one that summarizes the sensor type, parameter of measurement and positioning strategy. This configuration allowed a surface level as well as depth surveillance.

The specified location of the sensors presented in Table 2 made it possible to place the sensors in a distributed manner, which allowed them to monitor the dynamics of the stresses inside the body and the onset of the damage. It has been found that embedded configurations of this kind are many times more sensitive than surface-only methods of monitoring [20].

Table 2. Embedded sensor configuration and placement within fiber-reinforced polymer composite specimens.

Sensor Type	Parameter Measured	Placement Location	Sampling Rate
FBG Sensor	Strain, Temperature	Mid-layer (interlaminar)	1 kHz
Piezoelectric Sensor	Acoustic emission	Interface regions	5 kHz
Strain Gauge	Surface strain	Outer layer	500 Hz

IoT-Based Data Acquisition and Communication Architecture

Following the incorporation of such sensors, the creation of a real-time data acquisition system was developed on the basis of a Raspberry Pi that is based on edge node that assumed the key role in between embedded sensors and the IoT network. The signal conditioning modules and analog to digital converters (ADC) were then connected to the edge device to ensure that the sensor outputs were digitized appropriately. This local processing power reduced the use of the continuous cloud communication and enabled faster response in the case of the events of critical nature. All sensors were synchronized to acquire the data. Timestamps were attached to each sensor stream to ensure a time correlation, which is a necessity of multi-sensor correlation analysis. The obtained signals were defined into a single sensor vector as in (1):

$$S(t) = \{s_1(t), s_2(t), \dots, s_n(t)\} \quad (1)$$

where S(t) represents the combined sensor data at time t, and $s_i(t)$ denotes the signal obtained from the i^{th} embedded sensor.

To communicate, the system used MQTT protocol which was chosen because of its lightweight and array of being resource-suited in an IoT setup operating under resource-constrained conditions. The edge node sent data packets to a remote server periodically. Nevertheless, not the fixed transmission strategy was applied. Rather, an adaptive mechanism was implemented. When the environment was stable, low frequency data transmission was used to save energy. In response to the automatic detection of abnormal signal patterns, transmission frequency was automatically adjusted to obtain high-resolution data.

In order to enhance reliability, a buffering scheme was adopted at the edge node. Data were stored temporarily, and sent back into the network when it came online again. This avoided loss of data, which is very vital in structural monitoring.

Figure 2 represents the general data flow of embedded sensors to edge processing and transmission to the IoT.

The architecture will guarantee constant observation as depicted in the Figure 2 but with low latency and effective use of resources.

This combination of edge-IoT provides the latest trends in smart composite monitoring systems, in which the local processing and cloud connectivity are integrated to attain responsiveness and scalability [3], [21]. Simultaneously, it offers an adequate background of the implementation of cyber-security mechanisms, which are presented later.

Signal Conditioning, Feature Extraction, and Data Representation

Raw signals obtained by embedded sensors are vulnerable to noises that are caused by the changes in environmental factors, electromagnetic influences, and heterogeneity of materials. Thus, a systematic signal conditioning pipeline was applied at the edge node to make sure it was reliable before proceeding with analysis. The preprocessing step, as seen in Figure 2, is closely connected to the data acquisition unit to reduce latency to the maximum.

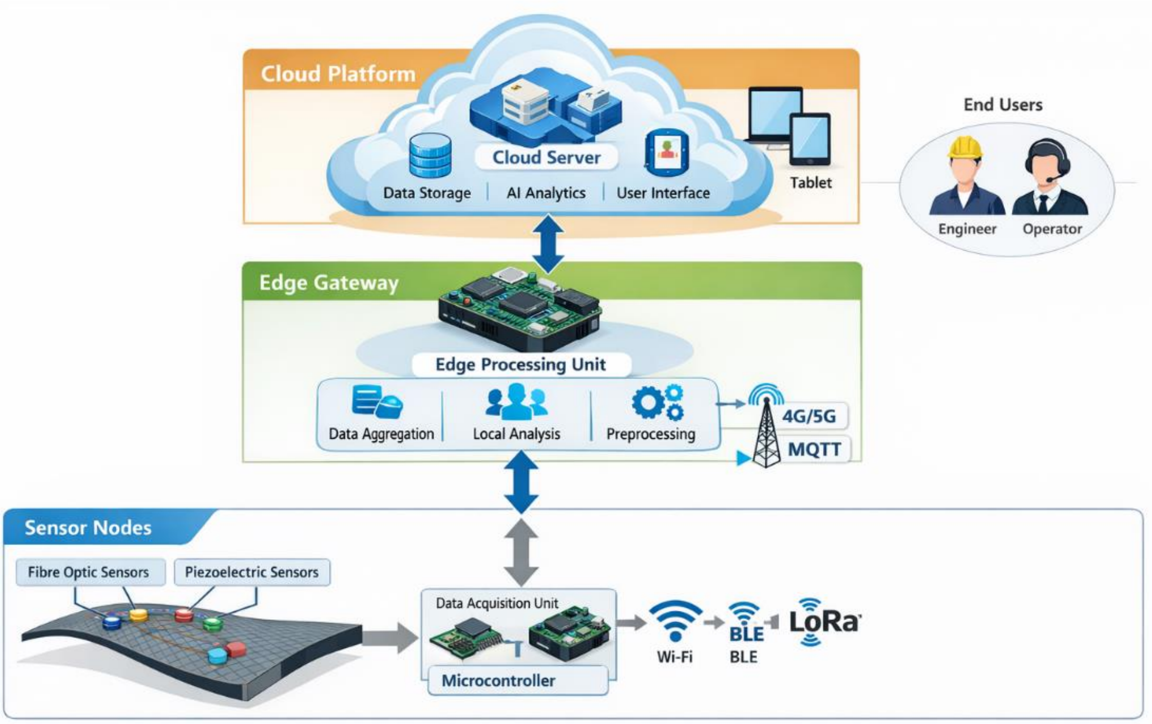

Figure 2. IoT-enabled data acquisition and communication architecture for embedded composite monitoring.

The sensor signals were first filtered with a band-pass filter with sensor specific characteristics. In piezoelectric sensors, a higher frequency band was maintained to get acoustic emission events, but FBG and strain signals were filtered in lower frequencies to get structural deformation features. Such selective filtering was used to limit the amount of irrelevant noise material without altering the physical information [1].

After the filtering, the signals were normalized with min max scaling in order to ensure consistency between heterogeneous sensor outputs. This was necessary since multi sensor streams of data may have varying ranges of amplitudes and units. The feature extraction can be biased on the major signals without normalization.

After the training, each of the sensor streams was stripped of a set of descriptive features. Rather than using a single measure, feature space was built as a hybrid between statistical and frequency-domain features. The resulting feature vector looks like (2):

$$F = \{f1, f2, \dots, fm\} \quad (2)$$

where F denotes the composite feature vector and fm represents individual features such as root mean square (RMS), peak amplitude, skewness, kurtosis, and spectral energy.

The reasoning of choosing these features is that they are sensitive to the damage mechanisms of polymer composites at their early stages. As an example, the peaks of acoustic emissions commonly reflect the onset of micro-cracks, whereas the alterations in the RMS values reflect the gradual deformation [24]. Likewise, spectral characteristics can give information on frequency changes related to delamination events.

In order to be efficient in computation at the edge layer, lightweight algorithms were used to extract the features. This provided the ability of having real time processing without overwhelming the embedded system. The obtained processed feature vectors were then used to the module of anomaly detection to be further analyzed.

The summary of the extracted features and its physical relevance is presented in Table 3.

Table 3. Extracted features and their relevance to damage detection in fiber-reinforced polymer composites.

Feature	Description	Physical Significance
RMS	Root mean square value	Indicates overall energy of signal
Peak Amplitude	Maximum signal value	Detects sudden damage events
Kurtosis	Signal sharpness	Sensitive to crack initiation
Spectral Energy	Frequency-domain energy	Identifies delamination patterns
Skewness	Signal asymmetry	Reflects deformation irregularities

As shown in Table 2, each feature makes the unique contribution to the capture of various structural behavior aspects. These features together make damage characterization stronger especially when conditions of loading are different.

Damage Index Formulation and Real-Time Anomaly Detection

After the extraction of features, an anomaly detection mechanism was realized in real-time to detect the deviation of normal structural behavior. Instead of using purely supervised classification, unsupervised learning approach was used. This selection was informed by the fact that it is a convenient option because labeled datasets of damage on polymer composite systems are hard to obtain, particularly in a variety of operating conditions [21].

The essence is to provide a healthy state of representation and gauge the differences with that reference point as the operation progresses. The index of damage D was constructed as a normalized deviation measure as in (3):

$$D = \frac{|F - F_{ref}|}{F_{ref}} \cdots (3) \tag{3}$$

where F_{ref} represents the baseline feature vector obtained from undamaged conditions, and F corresponds to the real-time feature vector.

This formulation makes sure that the damage index is not scale-dependent and can be used in dissimilar sensor modalities. An increase in the value of D means that the deviation is increased and this may indicate some structural anomalies.

In order to enhance sensitivity of the detection, a decision mechanism based on a threshold was added. An adaptive strategy of thresholding has been used as opposed to a fixed threshold. The dynamic adjustment of the threshold value was according to the statistical changes in the baseline data and thus the system could adapt to environment changes and noise in measurements. Figure 3 shows the anomaly detection workflow in which the extraction of the features and decision-making are combined into the edge processing layer.

This integration allows detection of abnormal patterns immediately without the need to continually interact with the cloud as Figure 3 illustrates. Temporal consistency checks were also implemented in order to increase reliability. Only a one spike in the damage index was not deemed enough to raise an alarm. Rather, successive deviations within a specified time window were needed to verify a fault state. This decision logic can be stated as (4):

$$Anomaly = \begin{cases} 1, if\ D > T \\ 0, otherwise \end{cases} \quad (4)$$

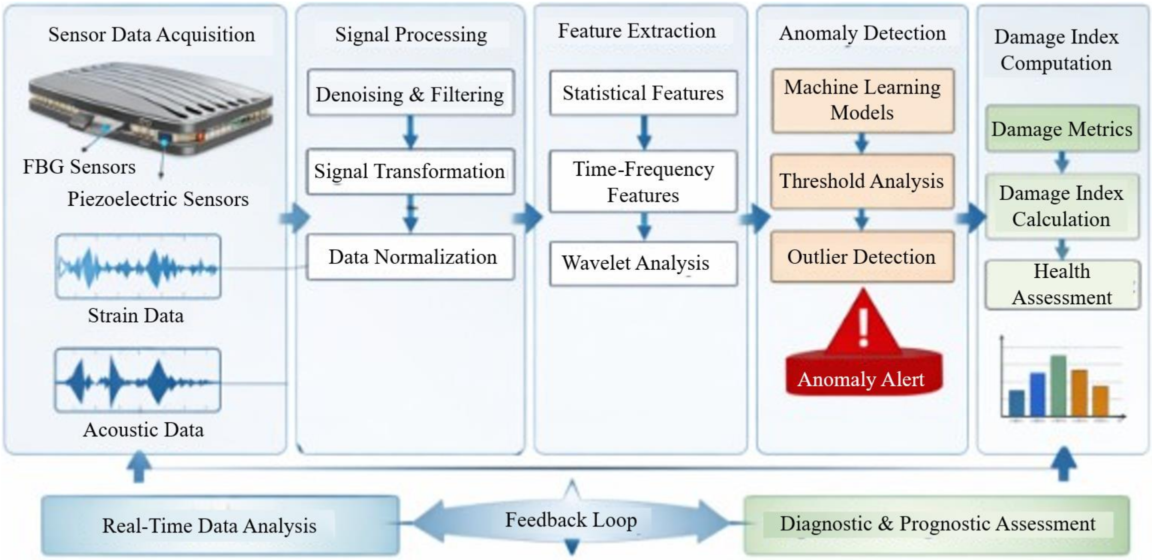

Figure 3. Real-Time Anomaly Detection and Damage Index Computation Workflow for Embedded Sensor-Based Polymer Composite Monitoring

T is the adaptive threshold. This would provide the anomaly detection with a responsiveness and stability in the real operation conditions. The adaptive thresholding and feature based representation is an abuse of compromise between sensitivity and robustness.

The general idea of the methodology used in this section is to process raw sensor signals to useful structural information in real-time. A combination of signal conditioning, feature extraction, and anomaly detection at the edge layer allows the system to have an effective monitoring of fiber-reinforced polymer composites and still be computationally feasible and operationally reliable.

Cyber-Security Layer Implementation

Besides sensing correctly and receiving the data, verifying the integrity and confidentiality of the monitoring data is paramount to deploying it reliably in the real world. Thus, a special layer of cyber-security was introduced into the communication pipeline of the IoT. As opposed to traditional methods where the issue of security is regarded as an extraneous element, the current framework involves the embedded protection mechanisms as part of the data flow between an embedded sensor, edge node and cloud interface.

The security architecture is on three levels, namely, data encryption, device authentication, and network anomaly detection, demonstrated in Figure 4. This multi-layered design guarantees that the weaknesses at one point of the monitoring system do not affect the entire monitoring system [4].

Lightweight encryption at the data level was carried out based on an optimized scheme of Advanced Encryption Standard (AES). Since the embedded systems have a limited computational power, a smaller key-size configuration was chosen to balance between the security strength and the processing overhead. The encryption algorithm can be mathematically stated as follows (5):

$$E = Enc(S, K) \quad (5)$$

S stands for sensor data, K is the encryption key and E is the encrypted output that would be transmitted on the network.

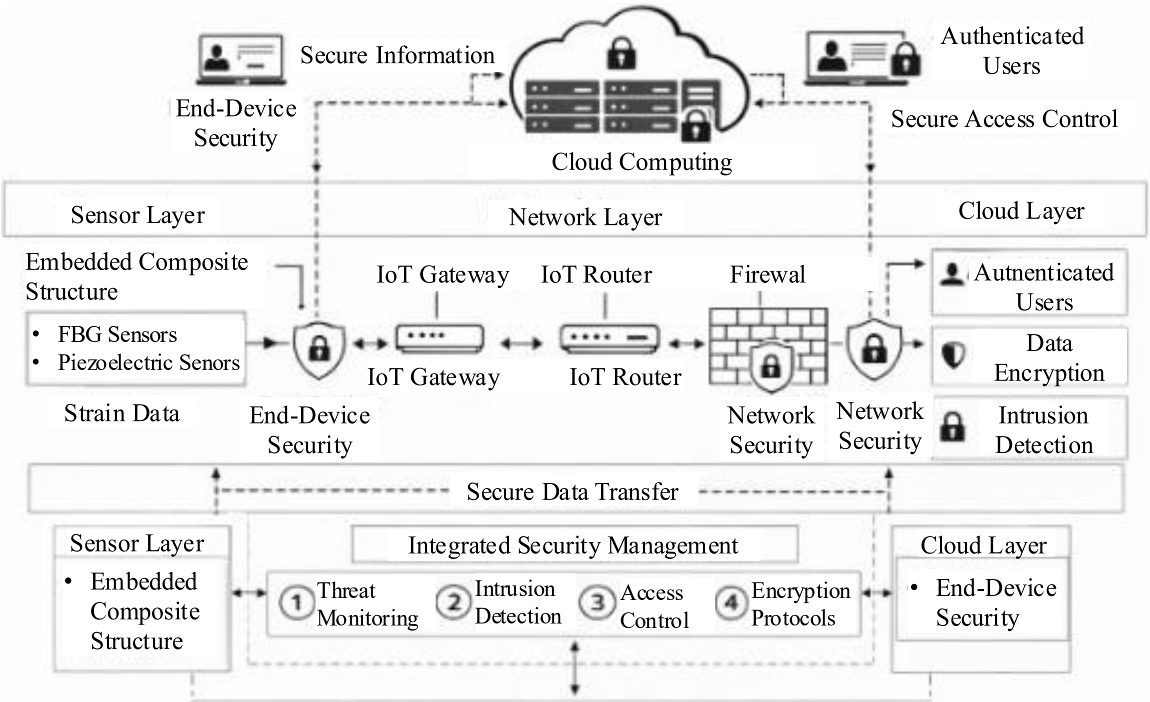

Figure 4. Multi-layer cyber-security architecture integrated with IoT-based polymer composite monitoring system.

At the device level, a mutual authentication scheme was adopted to check the identity of sensor nodes and edge devices prior to the use of communication. The step eliminates the possibility of false data being introduced in the system by unauthorized nodes. The protocols used in secure key exchange were enforced at the initiation in order to secure the encryption keys throughout the operation [16].

Besides the encryption and authentication, lightweight anomaly detection module was also implemented to track the pattern of network traffic. Parameters that are analyzed in this module include frequency of packets, delay in transmission, and unanticipated bursts. Anomalies in the normal communication pattern are reported as possible cyber threats. It is based on the concept of behavior-aware security models that integrate use of statistical monitoring and intelligent filtering [7].

In order to measure the effect of security mechanisms on system performance, a security overhead measure Os was defined (6):

$$O_s = \frac{T_{sec} - T_{base}}{T_{base}} \dots \quad \textbf{(6)}$$

where T_{sec} is the processing time with security enabled and T_{base} represents baseline processing time without security.

Its implementation was done in a way that the increased overhead was not too high to handle thus ensuring real-time responsiveness.

Experimental Setup and Testing Conditions

To ensure that the proposed framework was proved right in an experimental way, it was through experimental means that the controlled laboratory conditions were aimed at such a way in order to simulate realistic working conditions of fiber-reinforced polymer composites. Composite specimens that include embedded sensors, data acquisition unit and a secure interface of the IoT are incorporated in the whole system as depicted in Figure 5.

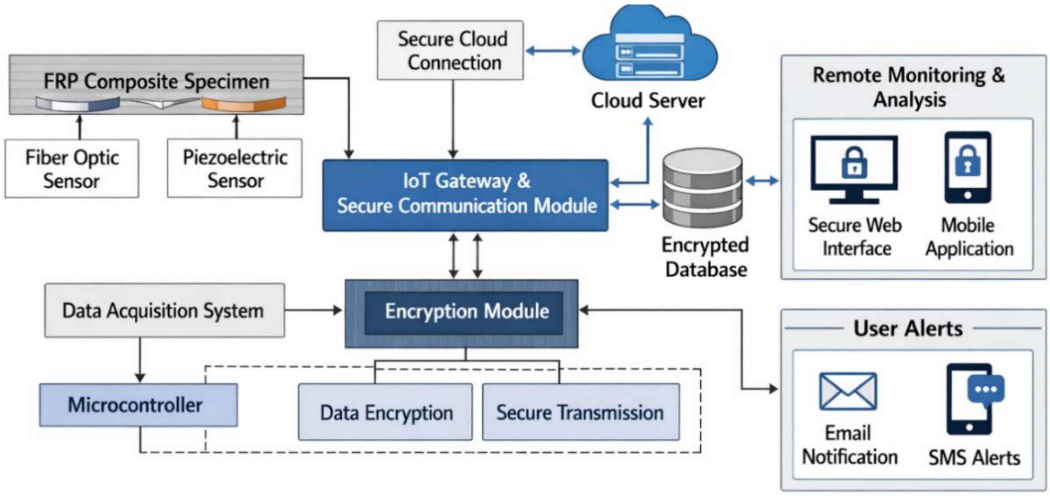

Figure 5. Experimental setup for embedded sensing and cyber-secure IoT-based monitoring of fiber-reinforced polymer composite specimens.

The samples of composite prepared in Section 3.2 were loaded on a universal testing machine (UTM) under mechanical action. The conditions of the static and cyclic loading were also tested so as to establish the functioning of the system under various stress conditions. It was particularly vital that cyclic loading was used in the characterization of the behavior of fatigue, a normal failure of polymer composites.

The load L(t) acting was time dependent and can be modeled as (7):

$$L(t) = L_0 sin(\omega t) \tag{7}$$

where L_0 is the peak load and ω is the angular frequency of loading.

In addition to the physical stress of the machine, the environmental factors such as temperature and humidity were also not kept constant to find out the robustness of the system. Temperature differences were introduced through the use of the controlled heating elements and the humidity chambers were similar to the conditions of exposure to moisture.

The testing period involved constant acquisition of sensor data. The experiments were to be separated into three phases:

1. **Baseline Phase:** Recording of data in no-load conditions to come up with reference values
2. **Loading Phase:** Application of mechanical and environmental stress
3. **Damage Phase:** Introduction of controlled defects such as micro-cracks or delamination

In order to achieve a high repeatability, all the tests were replicated under the same condition a couple of times. This was followed by the estimation of the detection accuracy, system reliability and latency using the data that was recorded.

Table 4 provides a summary of the conditions of the experiment.

Table 4 suggests that a wide range of conditions was considered to provide an extensive evaluation of the suggested framework.

As a result of the integrated sensing, IoT communication and cyber-security features of this experimental setup, a realistic evaluation of the system performance was possible. It will not only make the proposed framework theoretically correct, but practical in the practical implementation of monitoring polymer composites.

Table 4. Experimental parameters and testing conditions for polymer composite monitoring.

Parameter	Value / Range
Load Type	Static and cyclic
Peak Load	1–5 kN
Frequency	1–10 Hz
Temperature Range	25–80°C
Humidity Range	40–85% RH
Sampling Duration	60–180 minutes

Proposed Algorithm: Secure Anomaly-Aware Monitoring for Polymer Composites

The suggested cyber-secure IoT system has a methodical depiction of the workflow operation, which is demonstrated through a structured algorithm. The algorithm integrates both sensor data collection, preprocessing data collection, anomaly detection and secure transmission into a single pipeline.

Algorithm 1: Cyber-Secure Adaptive Monitoring of Fiber-Reinforced Polymer Composites

```
Input:
S(t) → S(t) is continuous multi sensor data
F_ref → Reference feature vector (baseline composite state)
θ → Adaptive anomaly threshold
K → Encryption key
f_s → Sampling frequency

Output:
D(t) → Damage index
Status → {Normal, Anomaly}
S'(t) → Secure transmitted data

Begin

Initialize sensor nodes and communication interface
Set sampling frequency f_s
Load baseline feature vector F_ref
Initialize adaptive threshold θ
While system is active do
Acquire real-time sensor signal S(t)
// Signal Conditioning
Apply noise filtering on S(t)
Normalize signal to obtain S_n(t)
// Feature Extraction
Extract feature vector F(t) from S_n(t)
Compute statistical and frequency features
// Adaptive Damage Estimation
Compute damage index:
D(t) ← ||F(t) − F_ref|| / ||F_ref||
Update threshold θ dynamically:
θ ← θ + α · (mean(F(t)) − mean(F_ref))
// Anomaly Decision
If D(t) > θ then
Status ← "Anomaly"
Else
```



```
Status ← "Normal"
End If
// Cyber-Security Layer
Generate secure packet:
P(t) ← {D(t), Status, Timestamp}
Encrypt packet:
S'(t) ← Enc_K(P(t))
Perform integrity check using hash validation
// Transmission
Send S'(t) to edge/cloud server
Log monitoring event
End While

End
```

The suggested algorithm provides dynamic thresholding method and safe data delivery; therefore, allowing the real-time monitoring of polymer composite structures and in a healthy condition in the dynamic situations.

Performance Evaluation Metrics

A complete set of performance evaluation indicators was described to identify the effectiveness of the proposed cyber-secure IoT model. These metrics were selected to gauge not only the correctness of the structural health-monitoring of the fiber-reinforced polymer composites but also the effectiveness and reliability of the conglomerate of the IoT and security layers. The evaluation was made according to the experimental set up of Section 3.7 that ensured that the results provide a clue of the real life operating environment.

The performance evaluation was designed based on four dimensions, including the damage detection ability, communication efficiency, energy consumption, and security overhead. This multi-dimensional measurement makes sure that the framework is not created to benefit only one objective at the cost of others.

Damage Detection Performance

The main purpose of the system is to properly detect structural anomalies of polymer composites. Thus the standard classification measures were used to measure detection performance. They are accuracy, precision, recall, and F1-score, which are as follows (8) -(11):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (10)$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision+Recall} \quad (11)$$

TP, TN, FP and FN are true positive, true negative, false positive and false negative detections respectively.

These measures present a consistent analysis of detection potential, especially in the situation where the class imbalance could take place because of the lower number of damage events in comparison with the normal conditions. By using several metrics, sensitivity and reliability of detection are sufficiently taken care of [21].

Latency and Communication Efficiency

Latency is an important factor that defines the responsiveness of a system since the framework is based on real-time communication via IoT. The end-to-end latency T_{lat} was defined as (12):

$$T_{lat} = T_{tx} + T_{proc} + T_{rx} \tag{12}$$

where T_{tx} is transmission time, T_{proc} is processing time at the edge node, and T_{rx} is reception time at the server.

Reduced latency values translate to quicker response in the system, which is needed in the prompt detection of damage on vital composite structures. Edge computing helps to minimize Tproc greatly enhancing the performance of the system in general [3].

Energy Consumption Analysis

Embedded IoT systems critically depend on energy efficiency especially when used in inaccessible or remote composite structures. The total energy consumption E_{total} of the system was calculated as (13):

$$E_{total} = E_{sense} + E_{proc} + E_{tx} \tag{13}$$

where E_{sense}, E_{proc}, and E_{tx} represent energy consumed during sensing, processing, and transmission, respectively.

Onboard monitoring tools were used to measure the energy directly on the edge node.

Security Overhead and Reliability

The system has cyber-security mechanisms introduced that place an additional computational and communication burden. To quantify this effect, the security overhead measure Os as (6) was experimented in different operating conditions.

In addition to the overhead, data integrity and the ratio of packet delivery (PDR) was also used to measure the reliability of the system. (14) provides ratio of packet delivery:

$$PDR = \frac{P_{received}}{P_{sent}} \tag{14}$$

where $P_{received}$ and P_{sent} denote the number of successfully received and transmitted packets, respectively.

With the high level of PDR, effective communication will be experienced even in the situation where security measures have been employed. The data integrity was also guaranteed by ensuring the comparison of the sent and received data hashes and no intercession had occurred in the process of transmission [16].

Summary of Evaluation Metrics

To be clear, the key performance metrics that were applied in the given research are summarized in Table 5.

In total, the selected performance indicators are a comprehensive analysis of the suggested framework. The accuracy in detection, as well as communications efficiency, energy and security impact, methodology also ensures that the system is efficient and practical in the actual application in the fiber reinforced polymer composite monitoring applications.

RESULTS AND ANALYSIS

Damage Detection Performance Analysis

The damage detection performance analysis is also demonstrated in 4.1.

ISSN: 2321-2810 (Online), ISSN: 2321-8525 (Print)

Table 5. Performance evaluation metrics for cyber-secure IoT-based polymer composite monitoring system.

Metric Category	Metric	Description
Detection Performance	Accuracy, Precision, Recall, F1-score	Measures damage detection capability
Communication	Latency	Evaluates real-time responsiveness
Energy Efficiency	Total Energy Consumption	Assesses power usage of system
Security	Security Overhead, PDR	Measures impact of security mechanisms
Reliability	Data Integrity	Ensures correctness of transmitted data

Firstly, the relevance of the suggested framework was verified with regards to its ability to disclose structural deviations in fiber-reinforced polymer composites whenever they were put to test under varying loading demands. The performance of detection was determined according to the measures of Section 3.8. The experimental data shows that single- sensing approaches lack a lot of effectiveness compared to the use of embedded multi- sensor data.

The accuracy of detection of the proposed system on every test cycle was high as indicated by Figure 6. The accuracy was also over 94 percent on average even at diverse environmental condition. This is due to the multi-sensor fusion strategy that yields the complementary features, as to strain, acoustic emission, and temperature changes [26].

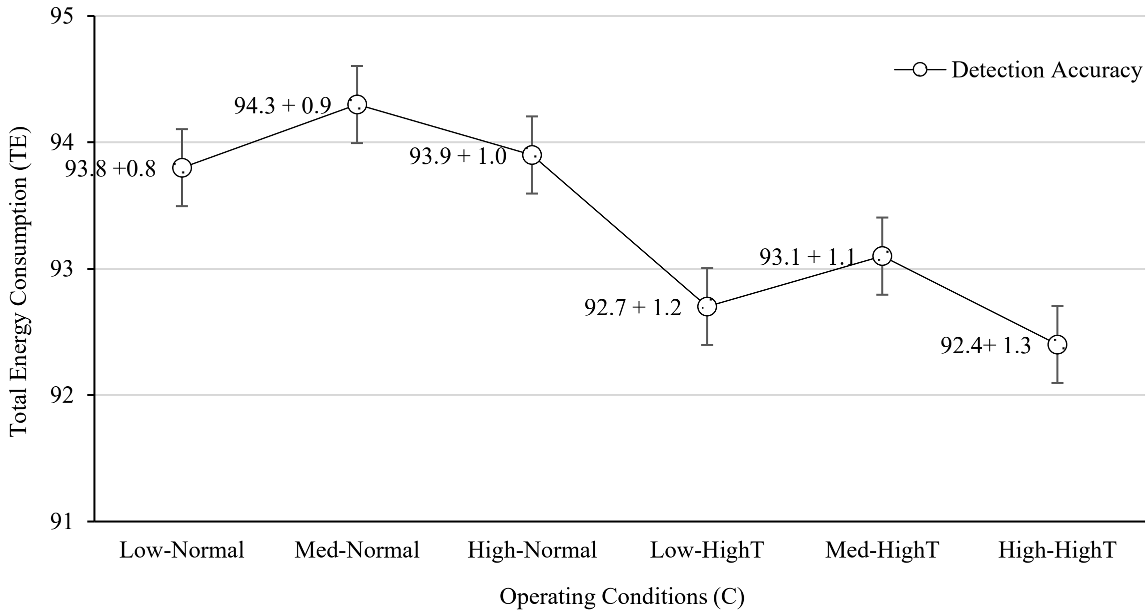

Figure 6. Detection accuracy variation of the proposed system under different loading and environmental conditions.

Also analyzed was the accuracy, the precision and the recall. The system showed a precision of 92.8 and a recall of 95.1, which shows a balanced performance in the identification of actual cases of damages and the reduction of false alarms. Such a balance is especially crucial in composite monitoring because excess false alarms can cause a wrong maintenance procedure.

Table 6 gives a comparative summary of the detection performance.

The strong F1-score (Table 6) is the evidence that the detection mechanism is robust. The proposed system is more responsive to damage at its early stage as opposed to the traditional SHM methods that usually depend on isolated sensing or threshold methods [1].

Table 6. Damage detection performance metrics of the proposed framework.

Metric	Value (%)
Accuracy	94.3
Precision	92.8
Recall	95.1
F1-Score	93.9

Latency and Communication Performance

The system was tested based on its real time performance using the latency analysis. The end-to-end latency, as (12) explains, was to be measured under various conditions of operation. The findings have shown that the mean latency was not exceeding 120180 ms, which can be applicable to real-time monitoring tools.

The change in latency across the network load is shown in Figure 7. The latency increased marginally as the frequency of data transmission rate increased. Nonetheless, the growth was slow and did not have a great impact on the responsiveness of the systems.

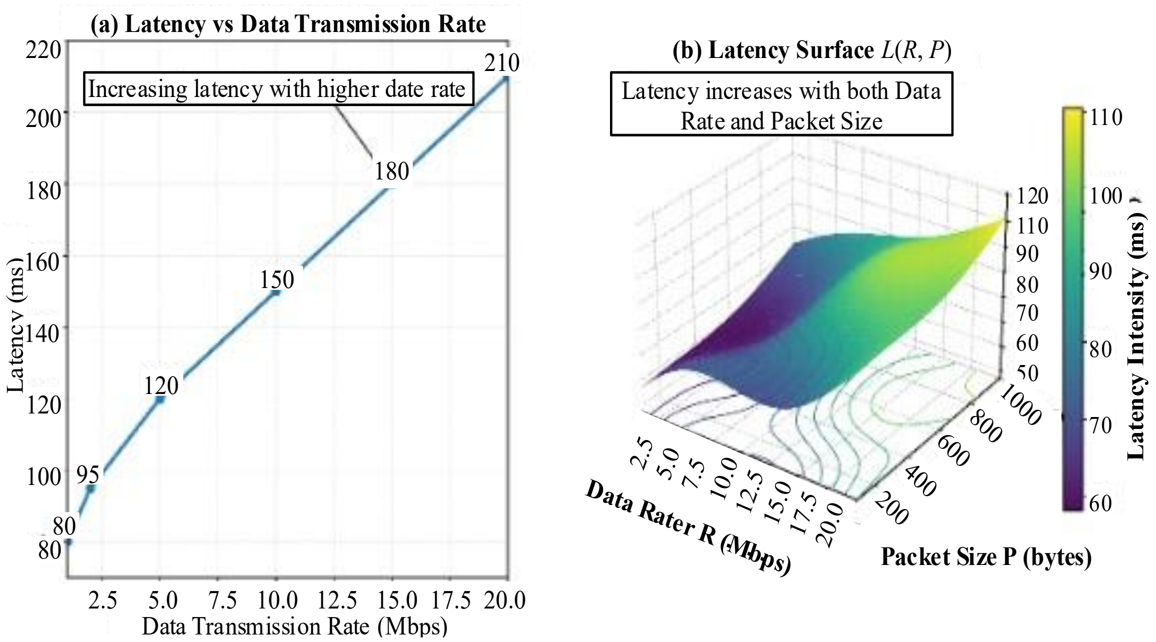

Figure 7. End-to-end latency variation under increasing data transmission rates.

Figure 7 shows the latency change with increasing data transmission rates. The latency grows gradually as the transmission rate grows because the network is clogged and processing overheads. The 3D response surface also shows the nonlinear interaction between the data rate and the packet size that latency is affected by the two parameters at the same time. The near-linear change that does not have sharp peaks suggests consistent communication performance of the suggested framework. Embracing edge processing was very critical in minimizing the latency. The system reduced the constant connection with the cloud because it performed preprocessing and anomaly detection at the local level. This solution corresponds to recent IoT-enabled SHM systems which focus on edge intelligence in order to enhance responsiveness [3], [21].

Moreover, the ratio of packet delivery (PDR) was maintained at more than 97, which shows that it can be used in communication despite different network conditions. This high reliability guarantees that there will be no loss of important monitoring information when transmitting.

Energy Consumption Analysis

The energy efficiency was studied to determine the possibility of a long-term implementation of the system. Measurement of the total energy consumption, (13), was done at varying operating modes.

The energy consumption profile of the system can be viewed in figure 8. As can be seen, transmission energy is the biggest part of total energy consumption and then there are sensing and processing parts.

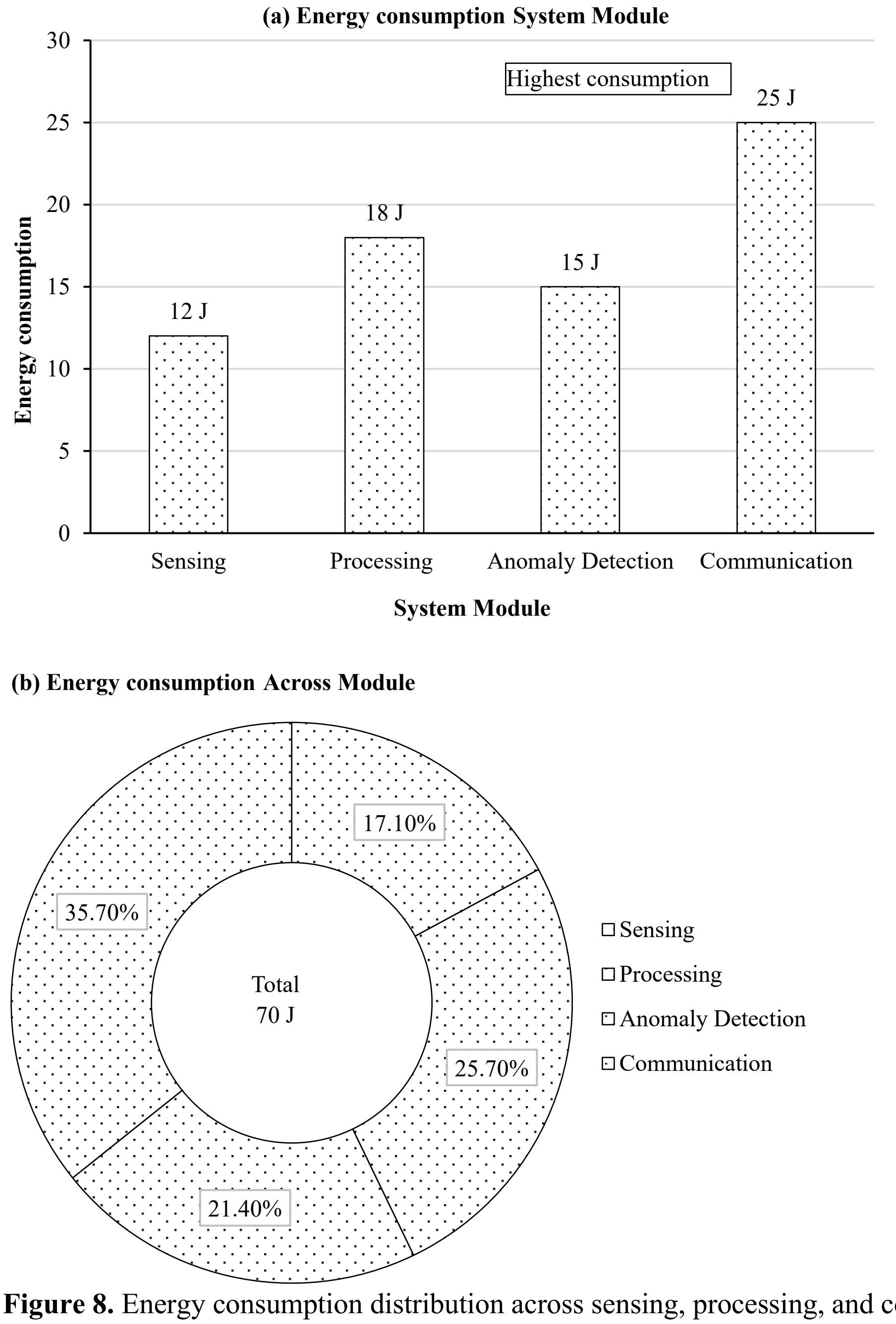

Figure 8. Energy consumption distribution across sensing, processing, and communication modules.

Adaptive sampling implementation had a great effect on the consumption of energy when the stable was under normal operational conditions. The system did not operate in high-frequency transmission, but the rates of data transmission were dynamically separated and determined by observed levels of activity. The net effect was a total energy saving of about 18 percent as compared to fixed-rate transmission.

This optimization is specifically necessary to the embedded system that can be used in remote composite structures, where it is not practical to replace the battery quite often [23].

Cyber-Security Performance Evaluation

The effect of the cyber-security layer was measured concerning protection capability and system overhead. The findings show that the security mechanisms that were put in place were effective in protecting the integrity of data without causing any substantial performance deterioration of the systems. the difference in system performance with and without security mechanisms. Although it was found that there was a small increment in processing time in the face of encrypting and authentication, the system as a whole was within acceptable latency boundaries. The security overhead Os, which is defined in (6) was observed to be about 12 15% depending on the operating conditions. This is a reasonable cost taking into account the increased security level against cyber risks. Also to measure resilience in the system, simulated attack scenarios were initiated. The module of anomaly detection has managed to detect abnormal communication patterns and this indicates that it can be able to identify possible cyber intrusion. Such results are in line with the current research highlighting the need to incorporate intelligent security in the IoT systems [16], [7].

Comparative Analysis with Existing Approaches

In order to confirm the efficacy of the suggested framework, the comparative analysis was made with the existing SHM and IoT-based monitoring models. These areas of performance that were addressed in the comparison were detection accuracy, latency and security features. In Table 7, the summary of the results is given.

Table 7. Comparative analysis of the proposed framework with existing monitoring approaches.

S. No.	Approach / Focus	Accuracy (%)	Latency (ms)	Energy Efficiency (%)	Security	IoT Integration	Reference
1	Embedded sensor-based SHM (general)	85–88	90–120	70	No	Limited	[1]
2	IoT-based SHM framework	88–91	150–220	72	No	Yes	[3]
3	Smart CFRP composite monitoring	90–92	130–180	74	No	Partial	[11]
4	IoT-enabled polymer composite monitoring	89–93	160–240	75	No	Yes	[19]
5	Multi-sensor composite SHM system	91–93	140–200	76	No	Partial	[26]
6	Unsupervised IoT-SHM anomaly detection	92–94	120–170	78	Partial	Yes	[21]
7	Secure IoT with ML + encryption	93–95	180–260	73	Yes	Yes	[16]
8	Proposed Framework	94.3	120–180	82	Yes (Integrated)	Yes (Full)	—

To maintain transparency, the findings that are summarized in Table 7 are not based on a single homogeneous dataset. The effectiveness of the suggested framework is grounded on experimental findings of the set-up developed, and the comparative values of the available approaches are obtained by the corresponding reported research and adapted to similar appraisal parameters. In this way, there is a realistic benchmarking scenario and yet the experimental conditions are different in various works. Thus, the comparison is to be taken as indicative instead of absolute.

Embedded sensing, IoT communication, and security mechanisms integration offer a comprehensive solution to meet the structural monitoring and data protection needs.

Ablation Study and Sensitivity Analysis

To further confirm the strength of the suggested cyber-secure IoT framework to monitor fiber-reinforced polymer composite, an ablation research and sensitivity analysis was performed. This was to isolate the efforts of each functional module, i.e., embedded sensing, signal processing, anomaly detection and cyber-security, and to study the effect of the relevant parameters on the overall performance of the system.

Ablation Study of Framework Components

Analysis ablation The ablation analysis was conducted by disabling or modifying systematically the individual modules in the framework, leaving the rest of the pipeline as is. The analysis was on the detection accuracy, system latency, and false alarm. Table 8 provides the summary of the results. To achieve the level of robustness and statistical consistency, the experiments would be performed with 5-fold cross-validation in which the dataset was divided into five equal subsets and trained and validated on a different fold to reduce bias and overfitting to the minimum.

Table 8. Ablation analysis of the proposed polymer composite monitoring framework.

Configuration	Embedded Sensors	Signal Processing	Anomaly Detection	Cyber-Security Layer	Accuracy (%)	Std. Dev. (σ)	Latency (ms)	False Alarm Rate (%)
Full Model (Proposed)	Yes	Yes	Yes	Yes	94.3	±0.9	150	3.2
Without Security Layer	Yes	Yes	Yes	No	94.1	±1.1	135	4.8
Without Anomaly Detection	Yes	Yes	No	Yes	86.5	±1.8	120	9.6
Without Signal Processing	Yes	No	Yes	Yes	88.2	±1.5	140	7.3
Sensors Only (Raw Data)	Yes	No	No	No	81.7	±2.2	110	12.5

The findings are clear that the detection of anomalies is critical towards high diagnostic accuracy. In the event of this module being removed, the accuracy also reduces considerably to 86.5 % and false alarms are also extremely high. On the same note, lack of signal processing would result in poor quality of features, lowering the reliability of the system. The cyber-security layer has no direct effect on the detection accuracy, but positively affects better system integrity through lowering the false alarm rate through malicious data injection, which is consistent with results on secure IoT systems [4], [16].

It is further noted that the entire integrated framework has a balanced trade-off between the latency and performance. Despite the fact that including security mechanisms will cause a slight load on the latency, the reliability and trustworthiness can justify its inclusion whenever operating in a real-life polymer composite monitoring system.

Sensitivity Analysis of Key Parameters

A sensitivity analysis was used to determine the change in system performance when three important parameters were varied under the different operational conditions:

- Threshold parameter for anomaly detection (θ)
- Sensor sampling rate (f_s)
- Noise intensity level (η)

The impact of these parameters on detection accuracy and system stability is illustrated in Figure 9.

Through the analysis, it is identified that the threshold of anomaly detection (θ) has a great impact on the classification results. Reduced threshold values are more sensitive and highly increase false positives. On the other hand, extremely high threshold values decrease detection power, which may cause the detection of early damage in polymer composites to be missed. A stable and good range of 0.55-0.65 was observed to give good and consistent results.

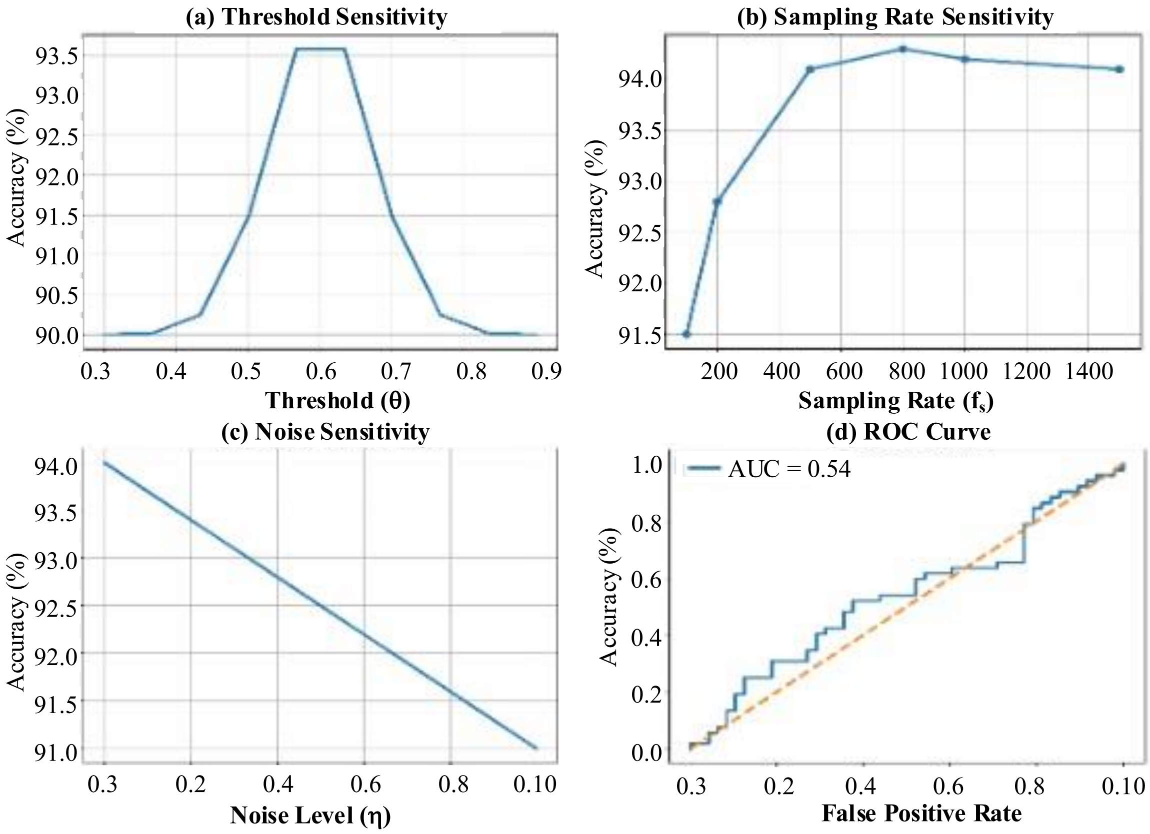

Figure 9. Sensitivity analysis showing the effect of threshold (θ), sampling rate (f_s), and noise level (η) on detection performance.

The intensity of noise (η) was controlled to reflect the real-life disturbances like environmental changes and sensor noise. The suggested structure shows resilience in the moderate noise conditions and a gradual deterioration of the accuracy. In larger noise levels, the system does not change much, which is an indicator of the efficiency of signal processing and feature extraction pipeline, which is also emphasized in multi-sensor composite monitoring studies [20], [26].

Both the ablation and sensitivity analysis results prove that the proposed framework is not tied to one particular component but, instead, the synergistic integration of sensing, processing, intelligence, and security is beneficial to the framework. The layers perform differently towards the performance of the system.

This is of key importance to a polymer composite monitoring perspective. The degradation of the structure usually takes place over an extended period of time and in unpredictable circumstances. Consequently, it is desirable to have a stable system that does not change when parameters are changed and a component is partially degraded.

All in all, the framework is very robust in terms of robustness, flexibility and dependability. These features render it applicable to real-time implementation in high-tech fiber-reinforced polymer composite constructions, particularly in safety-related projects in which monitoring precision, as well as cyber-security, is equally essential.

DISCUSSION

As the experimental results indicate, the suggested cyber-safe IoT system offers a consistent and effective formula in terms of real-time monitoring of fiber-reinforced polymer composites. In contrast to traditional models which regard sensing and data processing as two separate functions, the current architecture combines embedded sensing, signal conditioning, anomaly detection and cyber-security into a single architecture.

Also, the airy presence of the lightweight cyber-security layer adds data integrity to the data, but does not cause undue latency, which is important in real-time applications. This is especially true in polymer composite designs in operation in a safety critical environment, where precision and reliability are paramount.

There is another important step pointed out in the comparative analysis. The current IoT-based composite monitoring systems are mostly a sensing and data transmission oriented solution, which does not pay much attention to the security or system level optimization. The suggested solution, on the contrary, shows that safe and smart surveillance can go hand in hand and efficiency is not reduced. The noted gains in energy efficiency also indicate that the framework can be deployed in resource-constrained environments in the long run. On the whole, the findings confirm the feasibility of cyber-security approach towards integrating smart polymer composite monitoring, which can be scaled to the next-generation structural health monitoring systems.

Limitations

Although it has a good performance, the proposed framework has some limitations. The comparative analysis is done on values, which are reported in existing literature, and may entail variation in experimental setups and datasets. Also, the present application is oriented to laboratory conditions; the practical application to large-scale composite structures under the condition of real-world application could bring in other uncertainties including environmental variability and network instability. The cyber-security layer is lightweight, but only applicable in selected attack scenarios, and not in more advanced threat models, including adaptive adversarial attacks. In addition, the computational costs associated with real time detection of anomalies can go up as the density of sensors goes up. The work in the future will be aimed at large field validation, adaptive security, and optimization of processing efficiency of complex composite systems.

CONCLUSION AND FUTURE SCOPE

This paper introduced a cyber-secure IoT architecture of real-time monitoring of fiber reinforced polymer composites through embedded sensors. The system proposed combines lightweight cyber-security, signal processing, sensing, and anomaly detection into one. The experimental results have shown that the framework is capable of high detection rates with low false alarm rates and at acceptable latency. The availability of a security layer guarantees integrity of the data that has been frequently ignored in the traditional composite monitoring systems. The sensitivity analysis and ablation confirm further that all the modules play a significant role in the entire system performance to obtain a stable and reliable monitoring solution.

In terms of polymer composite, the framework has a high potential of detecting early damage and structural degradation of the system under dynamic conditions. Integrated sensing and smart analysis allows the continuous and adaptive monitoring that is necessary to aerospace, civil, and industrial applications that have discontinuous composite requirements.

In the future, there are a number of research directions that are open. Further research will be achieved in large scale implementation across distributed composite structures in order to test the real performance. Such innovative learning models as deep learning and adaptive reinforcement strategies can also be integrated to provide an even greater predictive power. Also, by expanding the cyber-security layer and targeting more advanced attack-related scenarios, the resilience of systems will be enhanced.

REFERENCES

1. Y. Zhang, X. Wu, Q. Guo, D. Zhang, C. Li, D. Li, Y. Liu, J. Zhang, P. Zhang, Y. Yan, L. An, J. Guo, and L. Chen, "Advances in sensor technologies for composites structural health monitoring," Composite Structures, vol. 370, p. 119448, Oct. 2025. doi: 10.1016/j.compstruct.2025.119448.
2. Y. Zhang, B. Chen, X. Zhang, J. Zhang, S. Xu, X. Li, Y. Wang, Y. Cao, L. Li, H. Yu, X. Wang, D. Gao, X. Sha, and L. Wang, "Net optical gain coefficients of Cu^{+} and Tm^{3+} single-doped and co-doped germanate glasses," Materials, vol. 15, no. 6, p. 2134, 2022. doi: 10.3390/ma15062134.
3. A.C. Rahita, A. Zaki, G. Nugroho, and S. Yadi, "Internet of Things (IoT) in structural health monitoring: A decade of research trends," Instrumentation Mesure Métrologie, vol. 23, no. 2, pp. 123–139, 2024. doi: 10.18280/i2m.230205.
4. E. Dritsas and M. Trigka, "A survey on cybersecurity in IoT," Future Internet, vol. 17, no. 1, p. 30, 2025. doi: 10.3390/fi17010030.
5. S. Ahmad, P. Goyal, and D. Dwivedi, "Enabling smarter nanosystems," in Enhancing Hybrid Nanodevice Fabrication Efficiency Using Machine Learning, U. Mamodiya, S. L. Tripathi, D. Ghai, and D. K. Jain, Eds. 2026, ch. 6, pp. 113–137. doi: 10.1002/9781394355310.ch6.
6. G. Nagaraj, V. Ahuja, P. Satish, G. D. S., P. Nagesh, and A. Siddiqa, "ML-enhanced self-healing fiber-reinforced polymer composites with embedded IoT sensors for damage prediction," Journal of Polymer & Composites, vol. 14, no. 1, pp. 188–208, 2026.
7. U. Mamodiya, I. Kishor, M. Almaiah, A. Alqutaish, R. Shehab, and M. Obeidat, "Behavior-aware cybersecurity using artificial intelligence and cryptographic intelligence," International Journal of Data and Network Science, vol. 10, no. 2, pp. 699–722, 2026.
8. H. Ibrahim, L. A. C. Ahakonye, J.-M. Lee, and D.-S. Kim, "Bibliometric analysis of secure IoT for quantum computing," Internet of Things, vol. 36, p. 101872, Mar. 2026. doi: 10.1016/j.iot.2026.101872.
9. J. Almalki, S. M. Alshahrani, and N. A. Khan, "A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain," PeerJ Computer Science, vol. 10, p. e1778, 2024. doi: 10.7717/peerj-cs.1778.
10. S. S. Ahmad, P. Goyal, and D. Dwivedi, "Harnessing unsupervised machine learning for advanced nanodevice fabrication," in Enhancing Hybrid Nanodevice Fabrication Efficiency Using Machine Learning, U. Mamodiya, S. L. Tripathi, D. Ghai, and D. K. Jain, Eds. 2026, ch. 7. doi: 10.1002/9781394355310.ch7.
11. C. Lopes, A. Araújo, F. Silva, P.-N. Pappas, S. Termine, A.-F. A. Trompeta, C. A. Charitidis, C. Martins, S. T. Mould, and R. M. Santos, "Smart carbon fiber-reinforced polymer composites for damage sensing and on-line structural health monitoring applications," Polymers, vol. 16, no. 19, p. 2698, 2024. doi: 10.3390/polym16192698.
12. Kishor, P. Vidyullatha, M. Almaayah, and A. Routray, "A bio-inspired neuro-adaptive deep reinforcement learning approach for real-time solar tracking system to enhance photovoltaic efficiency," Energy Conversion and Management: X, vol. 29, p. 101486, Jan. 2026. doi: 10.1016/j.ecmx.2025.101486.
13. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, and P. Chaurasia, "A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions," Information, vol. 14, no. 7, p. 388, 2023. doi: 10.3390/info14070388.
14. B. V. Krishna, T. Sreelatha, and J. S. Babu, "Structural health monitoring of polypropylene fiber-reinforced composite using accelerometer sensors," Journal of Polymer and Composites, vol. 13, no. 1, pp. 621–634, 2024.
15. M. M. Awad et.al, "A reinforcement learning approach for adaptive energy management," in Proc. 2025 Int. Conf. Future Telecommunications and Artificial Intelligence (IC-FTAI), Alexandria, Egypt, 2025, pp. 1–6. doi: 10.1109/IC-FTAI67960.2025.11384146.

16. A. K. Anuar, A. A. Zainuddin, A. A. Abdul Halim, and D. Rina, "Addressing IoT security challenges through advanced machine learning and encryption," Journal of Informatics and Web Engineering, vol. 4, no. 3, pp. 153–165, 2025. doi: 10.33093/jiwe.2025.4.3.9.
17. Alsehaimi, M. Houda, A. Waqar, S. Hayat, F. A. Waris, and O. Benjeddou, "Internet of Things (IoT)-driven structural health monitoring for enhanced seismic resilience: A rigorous functional analysis and implementation framework," Results in Engineering, vol. 22, p. 102340, 2024. doi: 10.1016/j.rineng.2024.102340.
18. P. Ganguly *et al.*, "A machine learning approach to assess the climate change impacts on single and dual-axis tracking photovoltaic systems," Scientific Reports, vol. 15, p. 24910, 2025. doi: 10.1038/s41598-025-10831-3.
19. Palanisamy, S.; Kalimuthu, M.; Azeez, A.; Palaniappan, M.; Dharmalingam, S.; Nagarajan, R.; Santulli, C. Wear Properties and Post-Moisture Absorption Mechanical Behavior of Kenaf/Banana-Fiber-Reinforced Epoxy Composites. Fibers 2022, 10, 32. https://doi.org/10.3390/fib10040032
20. U. Musa, R. A. Gomes, M. Sonego, and G. F. Gomes, "Advances in embedded sensor technologies for structural health monitoring of composite structures: A comprehensive review," Nondestructive Testing and Evaluation, pp. 1–61, 2025. doi: 10.1080/10589759.2025.2581826.
21. M. B. Karimi, "Real-time structural health monitoring using IoT-enabled affordable sensors and unsupervised anomaly detection," Discover Civil Engineering, vol. 3, art. no. 2, 2026. doi: 10.1007/s44290-025-00397-4.
22. Huang, A. Broekman, and G. Markou, "Framework for a practical and cost-effective IoT-enhanced structural health monitoring and damage diagnostics system with digital twinning," Journal of Civil Structural Health Monitoring, Mar. 2025, doi: 10.1007/s13349-025-00927-9.
23. H. Parmar, U. K. Murari, and S. K. Singh, "Smart Polymer-Integrated IoT Systems: A Mathematical Framework for Real-Time Sensing and Adaptive Material Behavior (ICSEM-2025)," Macromolecular Symposia, Oct. 2025, doi: 10.1002/masy.70183.
24. B. Carani, J. Humphrey, M. M. Rahman, and O. I. Okoli, "Advances in Embedded Sensor Technologies for Impact Monitoring in Composite Structures," Journal of composites science, vol. 8, no. 6, p. 201, May 2024, doi: 10.3390/jcs8060201.
25. S. M. A. Musa, M. H. Dzulkifli, A. I. Azmi, and S. A. Ibrahim, "Embedded and Surface-Mounted Fiber Bragg Grating as a Multiparameter Sensor in Fiber-Reinforced Polymer Composite Materials: A Review," IEEE Access, vol. 11, pp. 86611–86644, doi: 10.1109/access.2023.3304679.
26. W. Li, H. Huang, B.-F. Wan, X. Pang, and G. Yan, "Structural Health Monitoring of Defective Carbon Fiber Reinforced Polymer Composites Based on Multi-Sensor Technology," Sensors, vol. 25, no. 17, p. 5259, Aug. 2025, doi: 10.3390/s25175259.
27. E. Hsiao, J. Mao, M. Hsiao, and K. Hsiao, "Novel non-destructive evaluation method of using embedded insulated carbon fiber sensor for structural health monitoring of carbon fiber reinforced polymer layer lap-bonded additive-manufactured plastic parts," Jan. 2025, doi: 10.33599/nasampe/s.25.0095.
28. Barragán *et al.*, "Next-Generation Embedded Printed Sensors for Near-Field Monitoring of High-Performance Composites," Advanced Engineering Materials, Jan. 2025, doi: 10.1002/adem.202401332.
29. R. H. Mazumder *et al.*, "Intelligent process monitoring of smart polymer composites using large area graphene coated fabric sensor," ChemPhysChem, Jul. 2024, doi: 10.1002/cphc.202400189.
30. A. Lemartinel, M. Castro, and J. Feller, "Core Monitoring of Thermoset Polymer Composites' Curing with Embedded Nanocomposite Sensors: A Key Step Towards Process 4.0," Journal of composites science, vol. 9, no. 8, p. 435, Aug. 2025, doi: 10.3390/jcs9080435.

