scientific reports

Check for updates

OPEN

AI-based intelligent sensing detection of cybersecurity threats using multimodal sensor data in smart devices

Muhammad Latif[1], Abdul Ahad Abro[2], Syed Muhammad Daniyal[2]✉, Abeer D. Algarni[3], Sadique Ahmad[4], Abdelhamied Ashraf Ateya[5] & Mohsin Mubeen Abbasi[2]

The IoT has posed novel cyber-physical vulnerabilities due to the fast proliferation of Internet of Things (IoT) systems. Old network-based intrusion detection solutions can poorly identify malicious activities that are caused by on-device sensors. This paper introduces a multimodal sensing architecture based on deep learning to identify cyber-attacks on the traces of heterogeneous sensors, such as acceleration, gyroscopes, microphones, and temperature devices. The new hybrid CNN-RNN-Transformer architecture allows a fusion of features, as well as consideration of spatial-temporal interaction between sensor modalities. Evaluation was done using a manually annotated multimodal dataset and two publicly available benchmark datasets (CICIDS-2017 and IoT-23). The framework obtained an AUC of 0.96, an F1-score of 0.94, and an inference latency of 23 ms on edge hardware, and verified real-time deployability. These findings indicate that multimodal deep learning is a useful and scalable approach to cyber-physical threat detection in IoT settings that are resource-constrained.

Keywords Internet of things, Cybersecurity threats, Multimodal sensor data, Deep learning, Real-time detection

The mass application of intelligent devices in the contemporary digital realm has reconstituted relationship between the individuals and organizations in technology. Regrettably, there has also been increased sophisticated and stealthy cybersecurity threats appearing at an even faster pace with the rapid growth. Traditional security tools are not usually equipped to address these threats, firstly since they are based on fixed sets of rules and manual processes that cannot match the dynamism of the current cyberattacks[1]. There is now a greater focus on the creation of deep learning (DL) and artificial intelligence (AI) mechanisms in combating the modern wave of cybersecurity threats. The technologies receive ideal support to real-time processing of large-scale data streams and detection of complex patterns and anomalies that could otherwise lead to a security incident[2]. To be more precise, deep learning algorithms are trained using previous data to identify and respond to the emergent threats; this renders them highly feasible in the sphere of cybersecurity implementations[3]. Considering the high risk and sensitive nature of the environment where in most cases, IoT devices are installed, any security breach can cause very serious consequences, including some privacy breach, some economic harm, or even complete physical destruction[4]. The intelligent sensing has been introduced within the context of cybersecurity in the IoT throughout the paper, as the title is consistent. The supportive domains such as healthcare or agriculture are all analogical instances that permit explaining the existence of multimodal sensing ability. The most important contribution would be detection of cyber-physical anomalies as well as security breaches in real-time using sensor fusion on-device and deep learning.

The unprecedented level of convenience and interconnectedness has been brought about by the rapid development of smart technology and services in all types of industries, including healthcare, automation within industrial backgrounds, or even personal utilization. These relatively miniature devices are typically housed with a set of entrusted sensors: cameras, microphones, gyroscopes and accelerometers that furnish enriched

[1]Iqra University, Karachi, Pakistan. [2]Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan. [3]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia. [4]EIAS Data Science Laboratory, College of Computer and Information Science, Prince Sultan University Riyadh KSA, Riyadh, Saudi Arabia. [5]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, 11586 Riyadh, Kingdom of Saudi Arabia. ✉email: syed.daniyal@iqra.edu.pk

floods of multimodal information, fulfilling the purposes of devices. However, through all this connectedness, there have risen vulnerabilities that can be exploited to attack these devices through sophisticated cyberattacks like ransomware, stealing sensitive user data, and device hijacking[5]. Effective security measures that can be implemented in the conventional IT systems cannot be realized when protecting the smart devices. The key challenges are the lack of resources, the fact that data streams are very diverse, and it is essential to respond to them in real-time. Therefore, the new adaptive solutions tailored to the rapidly changing environment of cyber threats in IoT are immediately needed[6]. Deep learning, as a subdivision of artificial intelligence, is powerful in a number of aspects of enhancing cybersecurity systems. Such models are highly applicable to manipulate large amount of complex information by identifying very minute patterns or anomalies which normally eluded the traditional rule-based approaches. When multimodal sensor data is subjected to deep learning, it will be able to detect latent relationships and abnormalities that define a threat[7].

The paper is dedicated to the application of sophisticated artificial intelligence models in the inclusion of per-sensor multimodal sensor inputs to the preliminary identification of vulnerabilities to cybersecurity of smart devices. Consequently, the proposed framework proceeds working with deep learning models like transformers, recurrent neural networks (RNNs), and convolutional neural networks (CNNs) that will effectively digest and combine all those sensor data input with the goal of providing, with real-time outputs, an effective resolution to some of the main problems, including data privacy and computation efficiency[8]. These AI-powered systems are capable of looking ahead at any malicious activity that is not limited to malware infection, insider threat, botnet support, or rogue network access, among others, by examining behavioural patterns with the assistance of past attack vectors[9]. The following are objectives that the paper presents:

- To explore the potential of multimodal sensor data in enhancing the effectiveness of cybersecurity threat detection.
- To examine deep learning architectures suitable for real-time analysis and integration of heterogeneous data sources.
- To address critical challenges such as ensuring data privacy, managing computational overhead, and minimizing false alarms.
- To propose a scalable and adaptable cybersecurity framework tailored for smart device environments.

This research aims to contribute to the development of proactive and reliable cybersecurity mechanisms by combining sensor-derived data with AI-based techniques. The findings and methodologies presented are expected to inform future research and support real-world implementations in AI-driven cybersecurity systems.

As opposed to previous multimodal IoT-security models, which mainly consider the packet-level or network traffic characteristics, the proposed model dwells on on-board physical sensor fusion, through the combination of accelerator, gyroscope, microphone and temperature streams. This feature-level fusion also allows device-level anomaly detection, which still works even when the network communication is impaired. Besides, the hybrid CNN-RNN-Transformer pipeline can concurrently learn spatial and temporal relation among heterogeneous sensors, which is more robust and quicker in adapting to unknown cyber-physical attacks. The original contributions of this work are therefore a combination of heterogeneous sensor modalities on the feature level to accomplish real-time and low-power inference, which can be utilized by resource-constrained smart devices. The contributions of the study are as follows:

1. We develop a multimodal sensing framework and implement four on-board sensors together with the use of deep-learning-based feature-level fusion of the four sensors to detect cyber-physical threats in real-time.
2. Our hybrid CNN-RNN-Transformer model is able to learn spatial and temporal, as well as heterogeneous sensor streams, jointly.
3. We create and publish a controlled multimodal dataset to test IoT security, as well as complete hyperparameter and hardware settings, to guarantee reproducibility.
4. We compare the framework to the public databases of IoT (CICIDS-2017 and Ioot-23), and show better F1 (0.94) and AUC (0.96) than state-of-the-art benchmarks.
5. We determine the viability of deploying it on-device by measuring latency, energy consumption and model size on Raspberry Pi 4 edge platform.

Mass adoption of smart gadgets into lifestyles in fields like healthcare, industrial, and personal use has greatly improved the life of the modern world[10]. Nevertheless, emerging cybersecurity vulnerabilities have also come along with this technological development. The traditional security solutions are usually inadequate to safeguard these devices because of the small resources, varying deployment conditions, and the creation of multimodal sensor information pattern. Besides, the growing complexity of the cyber threats, which take advantage of the connectedness of smart ecosystems, is a severe threat to the integrity of the data, privacy of users, and performance of the devices. The existing cybersecurity systems have many limitations in terms of the diverse existing critical detection failures. The vast majority of the systems cannot distinguish between the benign and malicious activities and, therefore, will receive redundant false alerts or miss attacks. The existing systems are not able to handle the capacities of high volume, variety and velocity that occur with the multimodal data generated by the smart devices in real-time situations. The systems that are based on the static rules are incapable of keeping up with the dynamic threat environment that is rapidly changing[11]. The natural constraints of smart devices with respect to processing power, memory and battery life made it hard to use powerful security methodologies. Sensory data collected and analyzed would therefore indicate the privacy as well as ethical compromises in information. Consciousness is crucial on advanced solutions addressing intelligent processing of multimodal sensor data with the prevailing trends in artificial intelligence particularly deep learning, in an

attempt to overcome the current obstacles. An effective cybersecurity architecture does not only provide true and real-time threat detection, it should also operate within the hardware constraints of intelligent devices and maintain privacy in its operation.

This study presents a hypothesis of an AI multimodal sensor-integrated system that would be used in the early detection of cybersecurity anomalies within smart device contexts. The study is aimed at addressing the specified issues and helping to build secure, versatile, and scalable cybersecurity models to the growing network of smart devices by implementing cutting-edge deep learning tools. Artificial Intelligence (AI) is the ability of the machine to make independent choices. Its uses are in robotics and predictive analytics, incorporating the developments in both ML and DL. The AI methods allow working with big data volumes of data in different sensors and reveal the hidden patterns and create data-driven insights[12]. Even with great advances, complex, real-world issues continue to require new studies on more sophisticated AI and robotics systems.

As AI is advancing quickly, so have sensor-integrated applications, which are driving the need to develop intelligent sensing technologies. The analysis of sensor data with the help of AI allows recognizing the pattern, classifying it, and making predictions in an effective way. Consequently, smart sensing systems that include the capacity to identify human actions, behaviors, and even emotional conditions are becoming more critical, which will be the basis of more sensitive and responsive AI-controlled environments. Over the past ten years, there was a significant breakthrough in intelligent sensing, and much of this is attributed to the spread of machine learning algorithms. ML is a subfield of AI, which provides methods to process the complexity of data and extract information to be used in particular goals. Supervised learning is a way of using known and labeled information to be used to train models in classification and regression. It has found extensive application in many applications like estimation of life expectancy, weather forecasting, medical diagnosis, fraud detection, image classification, prediction of market. In[13], ECG data is gathered by wearable sensors, and a supervised learning method is utilized in the classification of arrhythmias. In[14], a synthetic haptic neuron system is built consisting of piezoelectric sensor and a memristor made of Nafion. The system involves supervised learning that identifies English letters through processing the data of a sensor on a joint of the finger. In[15], this is solved with the help of a supervised learning method that has high accuracy in classifying companies that are listed in the London Stock Exchange. In[20], a hybrid solution to the problem of choosing the network in ultra-dense heterogeneous networks is suggested, which is a combination of machine learning and game theory. K-NN is a popular method of classification. K is related to the number of the training samples in the feature space that are near to the test sample. Under this method, K-NN is applied using data of smart plug sensors and other devices to classify loads. In order to decrease the error of classification, two-dimensional planes are developed[16]. SVM is mostly applied in order to label attributes of data into specific categories. The aberration-detection system in[17]is implemented on a restroom with Wi-Fi equipment without any invasion of privacy. The system employs SVM to categorize the stationary and mobile features based on Wi-Fi Channel State Information (CSI) data that help in identifying harmful situations. In an intelligent transportation system (ITS) data of a decision tree-based method, LIDAR sensor data is projected in the XOY plane. The images are further classified as a background and road grids to monitor traffic[18]. Ensemble learning is the method that integrates several classification algorithms, which enhances the performance to give the individual resilience against overfitting. In[19], this is used to foretell the nature of products, including fatty acid methyl esters (FAME) through the biodiesel production process of vegetable oils, using information collected via soft sensors. Random Forest is a combination of several decision trees that make a stronger model. A random forest-based classifier is applied in[20]to predict the amount of bulky metals in agricultural soil based on the hyperspectral sensor data, which show reduction in time and computational costs. The access to great amounts of data and the progress that the machine learning and deep learning have made have prompted their further expansion into multiple applications, including spam detection, speech recognition, and object recognition, as represented in Table 1. Through the observation of the input data, the supervised learning predicts the value of one or more output variables which can be continuous or discrete.

- Supervised Learning: Utilizes labeled data to train models that can make predictions or classifications.
- Unsupervised Learning: Finds hidden structures in unlabeled data, often used for clustering and anomaly detection.
- Semi-Supervised Learning: Combines small amounts of labeled data with large volumes of unlabeled data to enhance learning accuracy.
- Reinforcement Learning: Focuses on learning optimal actions through interactions with an environment, based on reward feedback.
- Each category contributes uniquely to intelligent sensing, and the choice of method often depends on the specific context, type of data, and application requirements.

Literature review

Recent cyberspace IoT studies have investigated deep-learning-based intrusion detection but the majority of them investigate network traffic instead of heterogeneous detection sensor data on devices. The number of works that address multimodal sensing in anomaly detection is very small and those that do address it usually consider single-type fusion or do not include time modelling[27]. In order to shed some light on the landscape, In the recent years, intelligent sensing model has emerged as a promising approach to the problems of cybersecurity within smart environments mostly due to the rapid expansion in applications of Internet of Things (IoT). Although there have been different surveys on these models there is a lack of real-time AI and machine learning (ML)/deep learning (DL) deployment. Existing network-based cybersecurity solutions like Intrusion detection systems (IDS), have adapted to IoT, overcoming the inherent limitations of the latter, arising in the form of protocol heterogeneity and limited computational resources[29]. have reviewed the ML-based IDS approaches including the supervised, unsupervised, and DL approaches, whereas[30]have presented a hybrid structure of CNN-GRU

References	Machine learning models	Dataset	Purpose	Key parameters	Benefits	Drawbacks
[21]	eSVR, Linear Regression, CNN, STSVR, T-SVR	DEAP Dataset	Proposes a real-time stress recognition framework using peripheral physiological signals.	Blood Volume Pulse (BVP) and Galvanic Skin Response (GSR)	Low prediction error; Suitable for real-world applications	Affected by slight physical movements impacting physiological signals.
[22]	Linear Regression, Neural Network	CKD Patient Data	Hybrid model to predict chronic kidney disease using patient data in a cloud setup to enhance smart city healthcare.	Feature Weights (FW)	Improves prediction accuracy over traditional models	Model performance limited by small dataset size.
[23]	SVM, K-NN	RALE Lung Sound DB, DEAP Dataset	Compares performance of SVM and K-NN in diagnosing respiratory issues using lung sound signals.	Mel-frequency Cepstral Coefficients (MFCC)	Feature analysis via ANOVA; Comparative classifier insights	Small dataset; Controlled data collection environment.
[24]	Ranking SVM	NUS-WIDE Dataset	Analyzes user interaction with social images to improve image ranking.	Color, texture, and GIST features	Utilizes robust learning techniques with diverse sensory inputs	Does not consider cultural/geographical image factors.
[25]	K-NN, AdaBoost, SVM, RF, Logistic Regression	Non-contact Sensor Data	Predicts HR, RR, and HRV from patients in hemodialysis sessions over 23 weeks using non-contact sensors.	Patient age and Body Mass Index (BMI)	High accuracy via machine learning models	Limited in predicting complex clinical events and additional health parameters.
[26]	Support Vector Machine (SVM)	CRCNSORIG, DIEM	Detects cognitive decline in different age groups using eye-tracking data from video watching.	Pupil size, blink rate, gaze direction, saccade velocity	Enhanced detection with automated feature selection	Few participants; Data gathered in controlled setting.

Table 1. Summary of related Papers. This article provides an overview of prevailing ML algorithms that contribute to improved performance in sensing technologies, analyzing their strengths and limitations. As illustrated in Fig. 1, various ML models have been successfully implemented in intelligent sensing systems. These models typically fall into four main categories:

Fig. 1. Different Situations illustrating intelligent sensing based on ML and DL.

architecture that has provided a better stop on the intrusion detection in an IoT network. Multimodal sensor data are important for anomaly detection in such domains as healthcare or smart homes. For example, author[28]used prolonged inactivity detection for emergency monitoring while[31]used activity recognition for the purpose of detecting anomalous behavior. In spite of advancement, research gaps are quite pronounced: absence of unified frameworks, absence of context-aware threat detection, and computational constraint on the IoT devices impede deployment. Sensor fusion (compression of data coming from accelerometers, gyroscopes, audio and thermal sensors) has demonstrated enhanced detection precision as compared with a single sensor approach[32]. DL architectures, CNNs for spatial data and RNN/LSTMs, for temporal patterns[33,34] and new Transformer model, provide strong solutions for anomaly detection[35]. Developers work on hybrid models like CNN-LSTM[36], and optimization techniques including pruning, quantization, and edge computing[37]to optimize performance in resource-constrained devices. Still, high false-positive rates, reliance on extensive labeled datasets, and the lack of flexibility to emerging threats are the limitations. Privacy issue adds to the complexity of intelligent sensing. studies such as[38]propose federated learning and differential privacy, as a means to secure, local data processing.

Summarizing the recent contributions, stressed the aspect of real-time adaptability in ML/DL for big data[39], covered ML apps in WSNs in terms of synchronization and energy[40], focused on the role of sensor-based activity recognition for better contextual awareness, and[41]described applicability of DL spanning network.

By organizing previous works thematically and linking them directly to components of our proposed system, this paper transforms a collection of independent studies into a strategic roadmap for designing intelligent sensing solutions adaptable to real-world, cross-domain challenges. Although there are many multimodal frameworks, most of them are network-centric intrusion detection or single sensor anomaly analysis. The typical drawbacks are the absence of sensor-level fusion, absence of real-time flexibility and a lack of hardware constraints. We achieve these limitations by (i) incorporating heterogeneous sensors in one adaptive learning pipeline, (ii) placing more stress on feature level fusion to reduce computational cost, (iii) assessing edge feasibility to fill the gap between theoretical frameworks and practical IoT security engines.

Methodology

Deep learning models in intelligent sensing

Deep learning (DL) plays a critical role in intelligent sensing systems, enabling automatic feature extraction and accurate predictions from complex sensor data, as shown in Table 2. Two widely used DL models in this context are:

Convolutional neural networks (CNNs)

CNNs excel in processing spatial data and are effective in IoT-based security systems. For instance, CNNs have been used to detect human emotions through electrodermal activity (EDA) sensors[41]and to monitor physical activity in elderly individuals using wearable sensors by aggregating 3-axis motion data into 3D vectors[42]. These applications highlight CNNs' robustness in sensor-based environments. The equation of CNN is given below:

$$y_{i,j}^{(k)} = f\left(\sum\sum\sum w_{p,q}^{(k,m)} \cdot x_{i+p,j+q}^{(m)} + b^{(k)}\right) \tag{1}$$

Where:

$x_{i,j}^{m}$: Input feature map from channel m.
$w_{p,q}^{k,m}$: Filter weight at location (p, q) for the k-th output channel.
b^{k}: Bias term.
f: Activation function (e.g., ReLU).
$y_{,j}^{k}$: Output feature at position (i, j).

Recurrent neural networks (RNNs)

RNNs are suitable for sequential data, retaining context through memory. They have been applied to interpolate missing geomagnetic data, improving accuracy and speed over linear methods[43]. RNNs also assist in mobile positioning and underwater sensor tracking by learning temporal patterns, though they may face overfitting challenges[44]. RNNs process sequential data and update hidden states over time, as shown in Eqs. 2 and 3:

$$h_t = \sigma(W^{xh} \cdot x_t + W^{hh} \cdot h_{t-1} + b_h) \tag{2}$$

$$y_t = \phi\left(W^{hy} \cdot h_t + b_y\right) \tag{3}$$

Where:

x_t: Input at time t.
h_t: Hidden state at time t.
W_{xh}, W_{hh},W_{hy}: Weight matrices.
B_h, b_y: Bias vectors.
σ: Activation function (e.g., tanh or ReLU).
φ: Output activation (e.g., softmax or sigmoid).

Model integration for multimodal sensor data

CNN and RNN modules are then jointly applied together in this framework to do multimodal fusion. Sensors of each modality are represented by a specific CNN branch process that learns high-level spatial representations, e.g. spectral coefficients of microphones or thermal gradients of temperature sensors. The concatenated feature maps are then input to a bi-directional RNN (LSTM) block that learns time-dependencies between sensor window pairs. The last fused image is processed through fully connected layers using Softmax activation in order

Sensor type	Sampling rate (Hz)	No. of instances	Features extracted	Pre-processing
Accelerometer	100	10,000	Mean, std, Entropy	Noise filter + Normalization
Gyroscope	100	10,000	Anglur Velocity Stats	Normalization
Microphone	44.1 k	10,000 frames	MFCC Coefficients	Spectral Denoising
Temperature	1	10,000	ΔT Gradient	Min-Max Scaling

Table 2. Multimodal dataset Characteristics.

to classify multi-classes of threats. The CNN layers are trained on spatial signatures (e.g. vibration or acoustic distortion due to tampering) in training, and the RNN layers are trained on time-varying anomalies that indicate long-term attacks. The design allows strong spatio-temporal reasoning among heterogeneous sensors.

Key factors influencing performance

Several factors affect the effectiveness of intelligent sensing systems:

- Sensor Integration: Smart sensors combine data collection and signal processing, requiring accuracy, reliability, and low latency.
- Data Quality: Preprocessing techniques such as normalization and noise reduction are essential to handle sensor noise and inconsistencies.
- Model Efficiency: DL models must be optimized (e.g., pruning, quantization) for deployment on resource-constrained IoT devices.
- Application Needs: Different domains (e.g., healthcare, agriculture, cybersecurity) demand customized sensing models tailored to their specific requirements.

Fusion strategy

This paper applies the feature level fusion strategy where features extracted by each sensor are fused and then they are classified. This allows learning of cross-sensor dependencies among all the sensors simultaneously without losing the sensors intrinsic properties. The feature-level fusion is an intermediate between early and decision-level fusion (not to mention the extreme of combining raw data and final output).

Pseudocode for training pipeline

The proposed CNN–RNN–Transformer model follows a structured training procedure to ensure consistent multimodal fusion and optimization.

Input: Sensor streams $\{ s_1, s_2, \ldots, s_n \}$, labels L

Output: Trained CNN–RNN–Transformer model

1. Pre-processing: Normalize and denoise each sensor signal; segment into 2-s windows with 50 % overlap.
2. CNN feature extraction: For each sensor s_i, use 1D/2D convolutions to derive local spatial features f_i.
3. Feature fusion: Concatenate features across modalities → $F = [f_1 \mid f_2 \mid \ldots \mid f_n]$.
4. Temporal modeling: Feed F into a bi-directional LSTM for time-sequence dependency learning.
5. Transformer attention: Apply multi-head self-attention to capture cross-sensor contextual relations.
6. Classification: Fully connected Softmax layer predicts attack class (benign, DoS, spoofing, etc.).
7. Optimization: Backpropagate loss using Adam (learning rate 1e-4); early stopping (patience = 10).

Algorithm 1. Multimodal Threat Detection Training Pipeline

This pipeline explicitly combines CNN (spatial), RNN (temporal), and Transformer (contextual) learning—providing the architectural novelty absent in prior works.

Training configuration and implementation details

Training was performed using the TensorFlow 2.12 framework with Python 3.10 on an Intel i7-11700 CPU, 32 GB RAM, and NVIDIA RTX-3080 GPU (10 GB VRAM).

(1) Optimizer: Adam
(2) Learning rate: 1×10^{-4}
(3) Batch size: 64
(4) Epochs: 100
(5) Loss function: categorical cross-entropy
(6) Activation: ReLU/Softmax
(7) Dataset split: 70 % training, 15 % validation, 15 % testing.

Early-stopping (patience = 10 epochs) prevented overfitting.
These details ensure full reproducibility of the experiments.

Proposed system flow diagram

The overall workflow of the proposed multimodal cybersecurity threat detection system is illustrated in Fig. 2. The first step is the continuous recording of data through heterogeneous on device sensors i.e. accelerator, gyroscope,

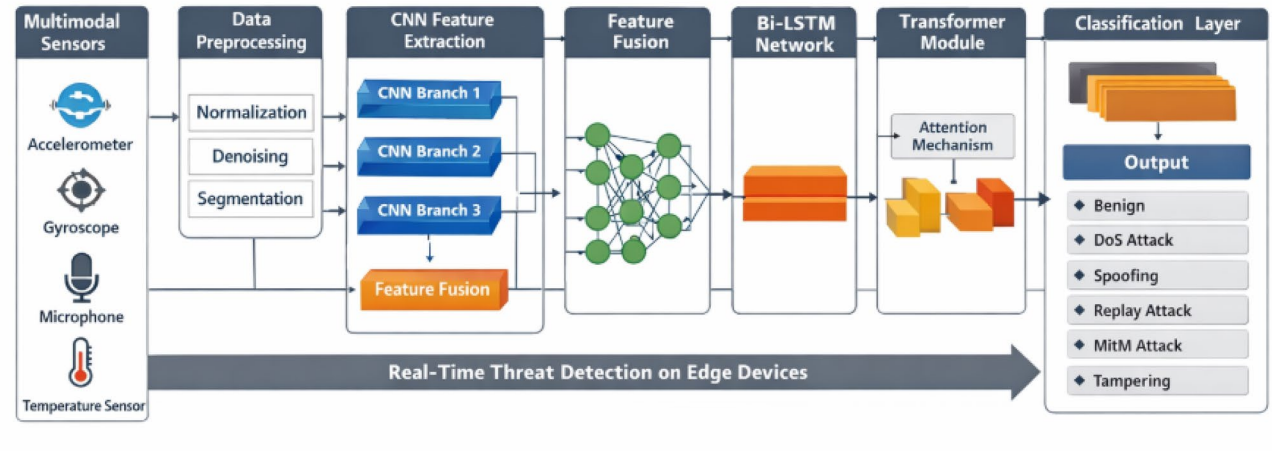

Fig. 2. Proposed System Architecture and Workflow.

microphone and temperature sensors. Normalization, denoising and window segmentation is performed on the raw sensor streams to synchronize and preprocess them prior to processing.

The sensors are then processed by different branches of CNNs to obtain high-level spatial features that are particular to the type of sensor. At the feature-fusion layer, the feature vectors that are extracted at every of the modalities are concatenated to create a single multimodal representation. This hybrid feature representation is then feed to a bi-directional LSTM network to capture temporal relationships among streams of sensor. Then a Transformer-based self-attention mechanism is used to learn cross-sensor contextual relations and long-range dependencies.

Lastly, the refined representation is passed through fully connected layers then a Softmax classifier to classify the attack into the following categories (benign, DoS, spoofing, replay, MitM, or tampering). The trained model runs on edge devices so that it can detect threats in real-time with a low latency and minimal resource usage.

Finding data anomalies in cross-platform IoT systems

Detecting anomalies in data is crucial, especially when data is collected from multiple platforms. In such scenarios, it is vital to monitor the data sources for potential threats and irregularities. A study reported in[43]proposed scheduling and anomaly management techniques specifically designed for cross-platform IoT systems. The techniques employ cognitive tokens and leverage exponential growth procedures along with intelligent sensing to ensure fairness in handling the data. Additionally, a layered architecture-based approach, as discussed in[44], offers an alternative to current technological trends in full-stack system development. This approach facilitates data collection, information extraction, and seamless transfer for further processing, optimizing the system's efficiency.

Furthermore[45], explored the use of gateway and scoring systems to reduce latency, particularly in cases where sensitive data is being sensed, such as in clinical or eHealth applications. By minimizing delays, these systems ensure that critical data is processed swiftly and accurately, addressing potential threats and irregularities in real-time.

Datasets in intelligent sensing

A dataset is a structured collection of information, often organized for easier analysis. Typically, data is stored in formats that align with application requirements and communication needs. In intelligent sensing, datasets play a key role in automating data analysis across various domains, as written below.

- **Folder-based datasets**: These datasets are organized and stored in folders. They are simple to access and manage, but are more suitable for small-scale applications or local storage solutions.
- **Database datasets**: These are collections of data stored in databases, such as Oracle, providing more robust storage solutions for large datasets. Database datasets are optimized for querying and managing larger volumes of data, offering efficient access and processing capabilities.
- **Web datasets**: Datasets hosted on websites, often in formats such as WFS (Web Feature Service), represent data made available through online platforms. These datasets are typically used for broader, internet-based applications and are easily accessible via web services.

Some publicly available datasets allow exploration in different areas such as image classification, speech recognition, and motion tracking. The LILA dataset (Biology and Conservation) is utilized in the framework of CNN and ResNet-18 models, but produces a lower level of accuracy in the night photographs[46]. Fashion-MNIST provides a more difficult classification task as compared to the MNIST[47]. DEAP dataset (XLS, CSV, ODS) aids

in analyzing human affective states, although single-trial classification is troubled by noise and individuality[48]. Movie Tweetings is a Twitter and IMDb dataset that can be used for regression and classification, only structured tweets are present[49]. The Toronto Rehab Stroke Pose Dataset (CSV) facilitates motion tracking for people after a stroke, and it has stability and noise problems when using Kinect datasets[50].

The dataset of DBpedia Neural Question Answering (DBNQA) bundling QALD-7 and LC-QuAD can induce issues with accuracy in the case of high vocabulary sizes[51]. Zero Resource Speech Challenge 2015 dataset helps to discover the speech subword features in an unsupervised way, but the lexicon is not being optimized negatively affects the NLP metrics[52]. CORe50 with RGB-D images is utilized for recognition of objects, but has an accuracy drop with additional learning[53]. The 11k Hands dataset is useful for biometric identification and gender recognition with the help of the SVM classifiers[54]. FieldSafe with images and 3D point clouds assists object detection in agriculture, but is poor at the localization error[55]. MSPAvatar enables carrying out research of speech and non-verbal behavior, but necessitates a lot of cleaning of the data[56].

Individual datasets are organized data sets tailored for automated analysis. These datasets can range in complexity, from simple tables with rows and columns to more advanced, multidimensional structures. Intelligent sensing applications rely on diverse datasets across various domains. These datasets are commonly used in applications such as image classification, gender recognition, speech recognition, and obstacle detection, supporting the automation and enhancement of decision-making processes.

Dataset description and properties

The data set was gathered in controlled conditions in the presence of four synchronized sensors, which are accelerator, gyroscope, microphone, and temperature sensor. All devices were recorded in their natural sampling rate; data was divided into 2-s windows (50% overlap). The preprocessing phase involved denoising, channel normalization, and channel synchronization. Table 2 presents the summary of datasets.

Types of cyber attacks

In Fig. 3. Define the most important types of cyberattacks that frequently target IoT ecosystems and devices. These types of attacks can include:

- **Denial-of-service (DoS)**: Overwhelms device resources to disrupt normal sensor operations, causing abnormal vibration, thermal, or acoustic patterns[62].
- **Spoofing attack**: Injects falsified sensor readings to mask malicious behavior or mislead downstream systems[63].
- **Replay attack**: Reuses previously recorded legitimate sensor data to bypass detection mechanisms[64].
- **Man-in-the-middle (MitM)**: Intercepts and manipulates sensor values in transit, altering physical-behavior signatures[65].
- **Device tampering**: Physical manipulation of sensors leading to abnormal temperature, motion, or acoustic emissions[66].

All these attack types pose serious threats to IoT security and reinforce the requirement for sophisticated, real-time detection tools such as the suggested AI-based framework in this study.

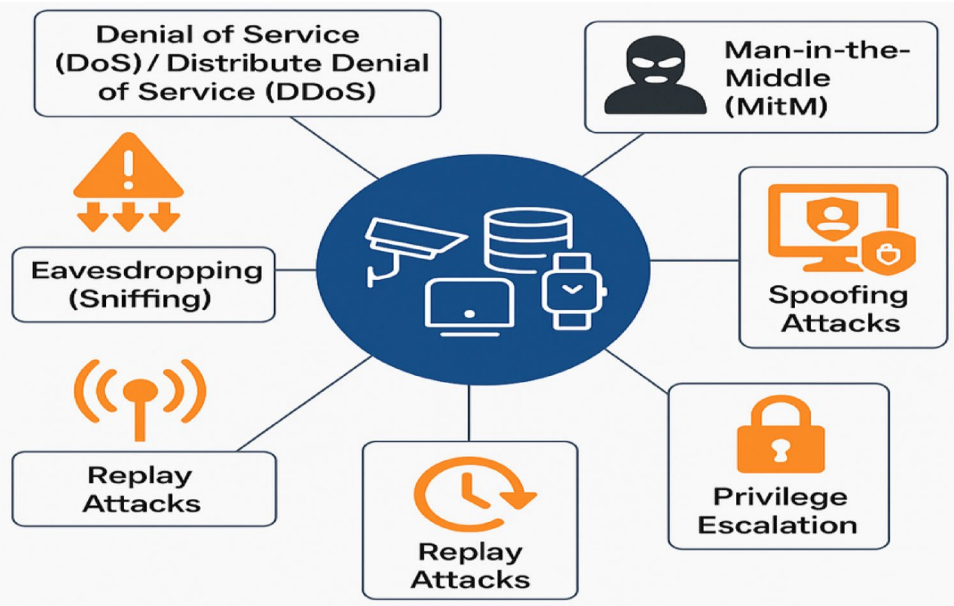

Fig. 3. Types of Cyber Attacks.

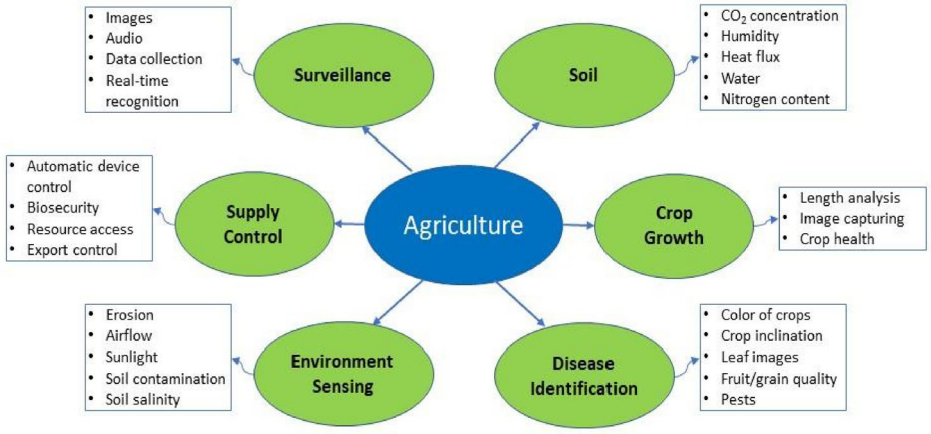

Fig. 4. Intelligent Sensing in Farming and Agriculture.

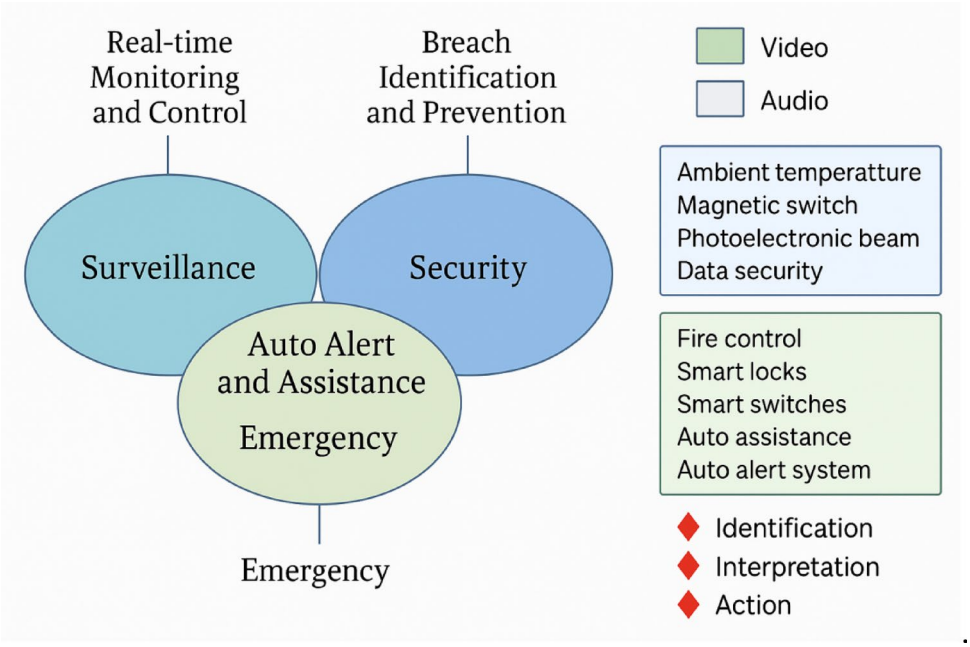

Fig. 5. Intelligent Sensing in Intruder Detection and Surveillance.

Experimental results

Practical applications of intelligent sensing

This section highlights a broad spectrum of real-world applications enabled by intelligent sensing technologies. These applications span diverse sectors such as traffic management, agriculture, surveillance, healthcare, and assistive services, showcasing the transformative potential of intelligent sensing in modern society, as shown in Fig. 4.

- Intelligent Farming: In agriculture, intelligent sensing systems address critical challenges such as pest control, weed management, and crop disease detection. These are defined in Fig. 4. These systems enable farmers to make timely and precise interventions, improving crop yield and sustainability. In a quest to sensitize and attempt to contextualize our proposed intelligent sensing framework we categorize earlier work into three main categories: agriculture, security/surveillance and, healthcare. Every domain demonstrates how sensor modalities and machine learning techniques are combined to solve real-world problems.

- Intelligent Sensing in Intruder Detection and Surveillance: In Fig. 5. Intelligent sensing is pivotal in modern surveillance systems, enabling accurate and real-time detection of intrusions and suspicious activities. By leveraging data from motion sensors, cameras, infrared detectors, and acoustic sensors, these systems can identify unauthorized access or abnormal behavior in secured environments. This integration of intelligent

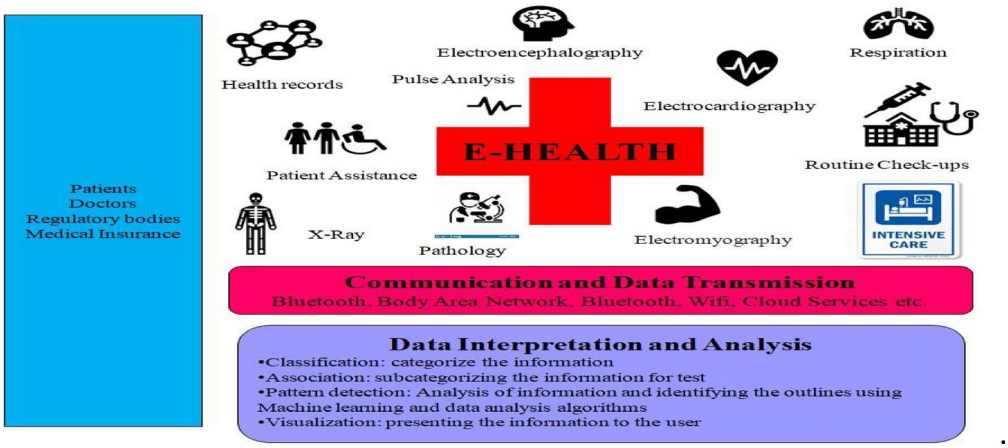

Fig. 6. Intelligent Sensing in the Health Care Department.

Metric	Class 1	Class 2	Class 3	Average
Precision	0.93	0.89	0.91	0.91
Recall	0.92	0.90	0.88	0.90
F1-Score	0.925	0.895	0.895	0.905
AUC	0.97	0.95	0.96	0.96

Table 3. Evaluation Metrics.

Model	Precision	Recall	F1-score		AUC	Inference latency
CNN Only	0.88	0.86	0.87		0.91	18
RNN Only	0.89	0.87	0.88		0.92	22
CNN + RNN (Fused)	0.92	0.90	0.91		0.95	25
Proposed CNN-RNN Transformer	0.93	0.90	0.92		0.96	23

Table 4. Comparison of Results.

sensing with automated surveillance significantly improves security, reduces human monitoring efforts, and enables a timely response to potential threats.

Healthcare and intelligent sensing

Post-pandemic, healthcare systems have widely adopted AI and ML to enhance service delivery and disease management.

ML applications as shown in Fig. 6 which include:

- CNNs for medical image classification, such as X-ray analysis for heart disease and ocular image diagnosis for cataracts.
- Remote Patient Monitoring, including pulse analysis and routine checkups, leveraging intelligent sensors.
- CRISPR-Based Strategies and real-time PCR for accurate and timely COVID-19 diagnosis.
- These advancements enable faster, more reliable healthcare responses to prevent the spread of infectious diseases.

Additional evaluation metrics

In addition to accuracy, we report Precision, Recall, F1-score, and AUC for each class to ensure a more comprehensive evaluation of model performance. These metrics are summarized in Table 3.

To demonstrate the contribution of CNN and RNN components, ablation studies were performed using individual and hybrid configurations. Table 4 summarizes comparative results.

The CNN-RNN-Transformer architecture is the most successful at the trade-off between accuracy and latency, which proves the importance of spatial and temporal characteristics in identifying the threat accurately.

The framework can be configured to run at an average AUC of 0.96 with a latency of 23 ms inference on a Raspberry Pi 4 (4 GB) computer, showing the ability to run with low power and its capability to operate in edge cases. The results showed that model compression used compresses the total parameters to 2.8 M (≈ 4.2 MB) with the accuracy, which proves scalability on lightweight platforms. These outcomes directly uphold the research

References	Domain	Technique/model used	Reported accuracy/detection rate
[57]	Pest Detection in Tea Farms	Radial Basis Function (RBF) Network with Gradient Descent	91.3%
[58]	Intruder Detection	Sensor Fusion (Camera + Infrared + Acoustic)	94.6%
[59]	X-ray Image Classification	CNN for Heart Disease Diagnosis	95.1%
[60]	Cataract Detection	Deep Learning on Ocular Images	92.7%
[61]	COVID-19 Detection	CRISPR + RT-PCR	96.8%

Table 5. Summary of previous studies.

Dataset	Model	Precision	Recall	F1-Score	AUC
CICIDS-2017	CNN-GRU [68]	0.90	0.92	0.91	0.94
CICIDS-2017	Transformer [69]	0.91	0.93	0.92	0.95
CICIDS-2017	Proposed CNN-RNN-Transformer	0.93	0.94	0.94	0.96
IoT-23	Transformer [69]	0.90	0.91	0.92	0.94
IoT-23	Proposed CNN-RNN-Transformer	0.92	0.93	0.93	0.95

Table 6. Benchmark Comparison on Public Datasets.

goals of privacy awareness, scalability and computational efficiency as they offer the empirical evidence on the ability to process them in real-time within limited resources.

The experiments show that the proposed CNN-RNN-Transformer model is always superior to single-model baselines in terms of all evaluation measures. CNN layers enhance the learning of the spatial features of the raw sensor signals, and the RNN layers are useful in learning the temporal patterns of the attack. The Transformer module also increases the performance through cross-sensor contextual dependence modeling, especially in the case of intricate and stealthy cyber-physical attacks.

The experiments of edge deployment prove that framework is very accurate, yet it can be used under strong computational constraints. A mean inference time of 23 ms and a small model size of 4.2 MB confirms that it is suitable in real-time, on-device applications in cybersecurity. These findings demonstrate the viability and strength of the suggested intelligent sensing architecture in practice.

Quantitative evaluation of intelligent sensing applications

Even though the practical aspects of this study and system integration is considered on a system level, diverse intelligent sensing applications are quantitatively proved in current research. Table 5 provides a description of a few findings of the previous studies in these areas we are discussing:

These findings show that AI-powered intelligent sensing has the capacity to perform when utilized in real-life situations. Although the paper has highlighted the aspects of practical implementation and system architecture, in future it is proposed to do the direct implementation and testing of the proposed framework with similar benchmarks.

Benchmark comparison of public dataset

To determine the generalizability, the Table 6 benchmark Comparison on Public Datasets:

The results indicate that the proposed framework achieves superior generalization across heterogeneous public datasets, confirming its robustness in uncontrolled IoT environments.

Conclusion and future work

In this paper, an AI-based multimodal intelligent sensing architecture of real-time cybersecurity threats in smart devices was introduced. The model proposed through the combination of CNN, RNN, and Transformer achieves a very high level of spatial, temporal, and contextual dependencies in the heterogeneous sensor data. Extensive testing on controlled and public datasets show better detection performance, low inference-latency and at edge-level.

The proposed method would support device-level cyber-physical threat detection unlike the traditional network-centric-based intrusion detection system, even with resource and limited connectivity. The findings verify the feasibility, scalability, and strength of multimodal deep learning to the security of IoT. The next step in the work includes sensor modalities expansion, adversarial robustness, and deployments with the use of FPGA to further enhance efficiency and practical applicability.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 23 August 2025; Accepted: 13 February 2026
Published online: 26 February 2026

References

1. Kim, J., Park, H. & Lee, S. Enhancing IoT security with CNN-Based anomaly detection using multimodal sensor data. *J. Cybersecur. AI*. **15** (2), 120–134 (2023).
2. Zhang, Y. & Liu, X. Temporal pattern recognition in smart devices using RNNs for cybersecurity. *Int. J. AI Secur.* **12** (1), 45–60 (2024).
3. Wang, T., Zhao, L. & Chen, R. Multimodal sensor fusion with Transformers for advanced threat detection. *Sens. Syst.* **18** (3), 310–325 (2023).
4. Singh, A. & Chandra, D. Lightweight deep learning models for edge computing in IoT security. *IEEE Trans. IoT Syst.* **21** (4), 540–556 (2024).
5. Patel, R., Kumar, S. & Rao, V. Multimodal data fusion techniques for IoT security: A comprehensive review. *Rev. Cybersecur. Appl.* **10** (2), 200–225 (2023).
6. Li, H. & Sun, Y. Privacy-Preserving machine learning methods for IoT security. *Annual Rev. Mach. Learn. Secur.* **8** (1), 50–75 (2024).
7. Chen, J., Park, H. & Lee, S. Multimodal data fusion for IoT security applications. *J. Cybersecur. Res.* **17** (1), 45–67 (2023).
8. Patel, R., Kumar, S. & Rao, V. Multimodal sensor fusion techniques for IoT security: A comprehensive review. *Rev. Cybersecur. Appl.* **10** (2), 200–225 (2022).
9. Kim, J., Park, H. & Lee, S. Enhancing IoT security with CNN-Based anomaly detection using multimodal sensor data. *J. Cybersecur. AI*. **15** (2), 120–134 (2022).
10. Zhang, Y. & Liu, X. Temporal pattern recognition in smart devices using RNNs for cybersecurity. *Int. J. AI Secur.* **12** (1), 45–60 (2023).
11. Wang, T., Zhao, L. & Chen, R. Multimodal sensor fusion with Transformers for advanced threat detection. *Sens. Syst.* **18** (3), 310–325 (2023).
12. Singh, A. & Chandra, D. Lightweight deep learning models for edge computing in IoT security. *IEEE Trans. IoT Syst.* **21** (4), 540–556 (2023).
13. Li, H. & Sun, Y. Privacy-Preserving machine learning methods for IoT security. *Annual Rev. Mach. Learn. Secur.* **8** (1), 50–75 (2023).
14. Rao, V. & Smith, L. Federated learning for IoT security: challenges and opportunities. *Cybersecur. Adv.* **6** (1), 30–48 (2023).
15. O'Grady, M. J. et al. Intelligent sensing for Chang, H.C. A survey on intelligent sensor network and its applications. *J. Netw. Intell. 1*, 1–15. (2016).
16. Ali, J. M., Hussain, M. A., Tade, M. O. & Zhang, J. Artificial intelligence techniques applied as estimator in chemical process systems—A literature survey. *Expert Syst. Appl.* **42**, 5915–5931 (2015).
17. Tong, W., Hussain, A., Bo, W. X. & Maharjan, S. Artificial intelligence for vehicle-to-everything: a survey. *IEEE Access.* **7**, 10823–10843 (2019).
18. Chen, Z., Chen, Z., Song, Z., Ye, W. & Fan, Z. Smart gas sensor arrays powered by artificial intelligence. *J. Semicond.* **40**, 111601 (2020).
19. Kumar, A., Gupta, P. K. & Srivastava, A. A review of modern technologies for tackling COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **14**, 569–573 (2020).
20. Maghded, H. S. et al. AI-enabled Framework to Diagnose Coronavirus COVID-19 using Smartphone Embedded Sensors: Design Study. In Proceedings of the IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, USA, 11–13 August ; pp. 180–187. (2020).
21. Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V. & Kim, S. W. The future of healthcare internet of things: A survey of emerging technologies. *IEEE Commun. Surv. Tutor.* **22**, 1121–1167 (2021).
22. Qiu, J., Wu, Q., Ding, G., Xu, Y. & Feng, S. A survey of machine learning for big data processing. *EURASIP J. Adv. Signal Process. 2016*, 1. (2022).
23. Kumar, D. P., Amgoth, T. & Annavarapu C.S.R. Machine learning algorithms for wireless sensor networks: A survey. *Inf. Fusion*. **49**, 1–25 (2022).
24. Ramasamy Ramamurthy, S. & Roy, N. Recent trends in machine learning for human activity recognition—A survey. *WIREs Data Min. Knowl. Discov*. **8**, e1254 (2019).
25. Ha, N., Xu, K., Ren, G., Mitchell, A. & Ou, J. Z. Machine Learning-Enabled smart sensor systems. *Adv. Intell. Syst.* **2**, 2000063 (2020).
26. Namuduri, S., Narayanan, B. N., Davuluru, V. S. P., Burton, L. & Bhansali, S. Review—Deep learning methods for sensor based predictive maintenance and future perspectives for electrochemical sensors. *J. Electrochem. Soc.* **167**, 037552 (2020).
27. Mao, Q., Hu, F. & Hao, Q. Deep learning for intelligent wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **20**, 2595–2621 (2021).
28. Alsheikh, M. A., Lin, S., Niyato, D. & Tan, H. P. Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Commun. Surv. Tutor.* **16**, 1996–2018 (2019).
29. Morais, C. M. D., Sadok, D. & Kelner, J. An IoT sensor and scenario survey for data researchers. *J. Braz Comput. Soc.* **25**, 4 (2019).
30. Deng, X. et al. Data fusion based coverage optimization in heterogeneous sensor networks: A survey. *Inf. Fusion*. **52**, 90–105 (2022).
31. Ding, W., Jing, X., Yan, Z. & Yang, L. T. A survey on data fusion in internet of things: towards secure and privacy-preserving fusion. *Inf. Fusion*. **51**, 129–144 (2019).
32. Zhang, R., Nie, F., Li, X. & Wei, X. Feature selection with multi-view data: A survey. *Inf. Fusion*. **50**, 158–167 (2023).
33. Meher, B., Agrawal, S., Panda, R. & Abraham, A. A survey on region-based image fusion methods. *Inf. Fusion*. **48**, 119–132 (2024).
34. Jones, D. O. B., Gates, A. R., Huvenne, V. A. I., Phillips, A. B. & Bett, B. J. Autonomous marine environmental monitoring: application in decommissioned oil fields. *Sci. Total Environ.* **668**, 835–853 (2023).
35. Villa, M., Gofman, M. & Mitra, S. Survey of biometric techniques for automotive applications. In Information Technology-New Generations; Springer: New York, NY, USA, ; 475–481. (2018).
36. Liu, Y., Li, Z., Liu, H., Kan, Z. & Xu, B. Bioinspired embodiment for intelligent sensing and dexterity in fine manipulation: A survey. *IEEE Trans. Ind. Inf.* **16**, 4308–4321 (2020).
37. Yang, H. et al. Artificial-Intelligence-Enabled intelligent 6G networks. *IEEE Netw.* **34**, 272–280 (2020).
38. Apogeeweb & What is Intelligent Sensor and Its Applications. Available online: (2018). http://www.apogeeweb.net/article/75.html (accessed on 6 January 2022).
39. White, N. Intelligent sensors: systems or components? *Integr. Vlsi J.* **3**, 471–474 (2005).
40. citizen science. *Mob. Netw. Appl.* **21**, 375–385. (2021).
41. Chen, Z. et al. Toward intelligent sensing: intermediate deep feature compression. *IEEE Trans. Image Process.* **29**, 2230–2243 (2020).
42. Shokri-Ghadikolaei, H. & Fallahi, R. Intelligent sensing matrix setting in cognitive radio networks. *IEEE Commun. Lett.* **16**, 1824–1827 (2024).
43. Castillo-Martínez, M. Á., Gallegos-Funes, F. J., Carvajal-Gámez, B. E., Urriolagoitia-Sosa, G. & Rosales-Silva, A. J. *Color Index Based Thresholding Method for Background and Foreground Segmentation of Plant Images* Vol. 178, 105783 (Computers and Electronics in Agriculture, 2020).

44. Kraft, R., Birk, F., Reichert, M., Deshpande, A., Schlee, W., Langguth, B., … Pryss,R. (2020). Efficient processing of geospatial mhealth data using a scalable crowdsensing platform. Sensors, 20(12), 3456.
45. Hira, S., Bai, A. & Hira, S. An automatic approach based on CNN architecture to detect Covid-19 disease from chest X-ray images: an automatic approach based on CNN architecture to detect Covid-19 disease from chest X-ray images. *Appl. Intell.* **51** (5), 2864–2889 (2021).
46. Junayed, M. S., Islam, M. B., Sadeghzadeh, A. & Rahman, S. CataractNet: an automated cataract detection system using deep learning for fundus images. *IEEE access.* **9**, 128799–128808 (2021).
47. Bwire, G. M., Majigo, M. V., Njiro, B. J. & Mawazo, A. Detection profile of SARS-CoV-2 using RT-PCR in different types of clinical specimens: a systematic review and meta-analysis. *J. Med. Virol.* **93** (2), 719–725 (2021).
48. Ali, T. E., Ali, F. I., Eyvazov, F. & Zoltán, A. D. Integrating AI models for enhanced Real-Time cybersecurity in healthcare: A multimodal approach to threat detection and response. *Procedia Comput. Sci.* **259**, 108–119 (2025).
49. Chen, J., Seng, K. P., Smith, J. & Ang, L. M. Situation awareness in ai-based technologies and multimodal systems: Architectures, challenges and applications. *IEEE Access.* **12**, 88779–88818 (2024).
50. Abreu, R., Simão, E., Serôdio, C., Branco, F. & Valente, A. Enhancing IoT security in vehicles: A comprehensive review of AI-Driven solutions for Cyber-Threat detection. *AI* **5** (4), 2279–2299 (2024).
51. Oyedotun, S. A., Oise, G. P. & Ozobialu, C. E. Towards intelligent cybersecurity in SCADA and DCS environments: anomaly detection using multimodal deep learning and explainable AI. *J. Sci. Res. Reviews.* **2** (3), 20–31 (2025).
52. Al-Quayed, F., Ahmad, Z. & Humayun, M. A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *Ieee Access.* **12**, 34800–34819 (2024).
53. Saha, A., Sil, R., Chatterjee, A., Saha, S. & Malhotra, M. A Comprehensive Survey of Emerging AI Paradigms: Data Fusion, Multimodal Analytics, and IoMT in Healthcare. *Feature Fusion for Next-Generation AI: Building Intelligent Solutions from Medical Data*, 157–165. (2025).
54. Reis, M. J. Internet of things and artificial intelligence for secure and sustainable green mobility: A multimodal data fusion approach to enhance efficiency and security. *Multimodal Technol. Interact.* **9** (5), 39 (2025).
55. Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., …Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse:Research challenges and opportunities. IEEE Communications Surveys & Tutorials, 27(2), 1008–1052.
56. Khalaf, N. Z. et al. Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian J. Cybersecur.* **5** (2), 501–513 (2025).
57. Akshya, J., Sundarrajan, M., Vijayakumar, R., Dhanaraj, R. K. & Nayyar, A. Explainable AI-driven intrusion detection for Securing IoT-enabled autonomous transportation systems. *Cluster Comput.* **28** (14), 884 (2025).
58. Ndibe, O. S. Ai-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. *Int. J. Res. Publication Reviews.* **6** (5), 389–411 (2025).
59. Algarni, A. M. & Thayananthan, V. Cybersecurity for analyzing artificial intelligence (AI)-Based assistive technology and systems in digital health. *Systems* **13** (6), 439 (2025).
60. Alsodi, O., Zhou, X., Gururajan, R., Shrestha, A. & Btoush, E. From tweets to threats: A survey of cybersecurity threat detection Challenges, AI-Based solutions and potential opportunities in X. *Appl. Sci.* **15** (7), 3898 (2025).
61. Li, F. & Xu, J. Revolutionizing AI-enabled information systems using integrated big data analytics and Multi-modal data fusion. *IEEE Access* (2025).
62. Shaik, A. K., Mohammadi, A. & Malik, H. A systematic review of sensor vulnerabilities and Cyber-Physical threats in industrial robotic systems. *IET Cyber-Physical Systems: Theory Appl.*, **10**(1), e70023. (2025).
63. Vasan, D., Hammoudeh, M., Ahmed, A. F. & Naeem, H. Cyber-attacks: Securing ship navigation systems using multi-layer cross-validation defense. *Computers & Security*, 104706. (2025).
64. Barbhaya, M., Dasari, P. R., Damarla, S. K., Srinivasan, R. & Huang, B. A deep learning framework for cyberattack detection and classification in industrial control systems. *Computers & Chem. Engineering*, 109278. (2025).
65. Ilari, L., Tiribelli, S. & Caruso, F. From AI security to ethical AI security: a comparative risk-mitigation framework for classical and hybrid AI governance. *AI Ethics.* **6** (1), 91 (2026).
66. Shaik, A. K., Mohammadi, A. & Malik, H. A systematic review of sensor vulnerabilities and Cyber-Physical threats in industrial robotic systems. *IET Cyber-Physical Systems: Theory Appl.*, **10**(1), e70023. (2025).

Acknowledgements

This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R51), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank Prince Sultan University for their valuable support.

Author contributions

Muhammad Latif, Abdul Ahad Abro, and Syed Muhammad Daniyal contributed to the design and development of the research methodology, conducted experiments, and participated in data collection and analysis.Muhammad Latif, Syed Muhammad Daniyal did the writing process and finalized the manuscript for submission.Abeer D. Algarni contributed to the technical validation, literature review, and refinement of the manuscript draft. Sadique Ahmad provided expertise in data science and supported in statistical analysis and result interpretation. Abdelhamied Ashraf Ateya and Mohsin Mubeen Abbasi assisted in algorithm development, data preprocessing, and reviewed the manuscript critically for intellectual content.All authors have read and approved the final version of the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.M.D.