Elevating Smart Industry Security: An Advanced IoT-Integrated Framework for Detecting Suspicious Activities using ELM and LSTM Networks

Dr. Mohammad Eid Alzahrani
Department of Computer Science-Faculty of Computing and Information, Al-Baha University, Al-Baha, Saudi Arabia

***Abstract*—The proliferation of Internet of Things (IoT) devices in smart industrial contexts necessitates robust security measures to thwart potential threats. This study addresses the escalating security challenges arising from the widespread deployment of IoT devices in smart industrial environments. Focusing on the identification and categorization of potentially harmful activities, our research introduces an innovative framework that seamlessly integrates networks of Extreme Learning Machines (ELM) with Long Short-Term Memory (LSTM). The primary goal is to significantly enhance the accuracy and efficiency of real-time detection of suspicious activities. Implemented using Python, the framework exhibits a remarkable 97.5% improvement in recognizing and accurately categorizing suspicious activities compared to traditional methods such as Conv 1D and 3D CNN. Rigorous testing on a substantial real-world dataset simulating smart industry scenarios underlines this substantial improvement over conventional approaches in identifying and precisely classifying questionable activities. The design excels in comprehending complex behavioral trends within the dynamic IoT data environment, leveraging the temporal memory retention capacity of LSTM networks. This research lays the groundwork for fortifying cybersecurity in smart industries against emerging online threats and malicious actions. The proposed framework capitalizes on the synergies between LSTM and ELM networks to achieve heightened accuracy in identifying suspicious activities, providing comprehensive and dynamic insights from real-time IoT data. These insights are crucial for proactive threat detection and prevention in smart industrial settings, contributing to an elevated level of security against evolving threats.**

***Keywords*—Internet of Things (IoT); Smart Industries; Extreme Learning Machine (ELM); Long Short-Term Memory (LSTM); Activity Recognition**

I. INTRODUCTION

The notion of smart industries is gaining great traction due to the growth of Internet of Things, or IoT, devices in manufacturing settings, which is revolutionising traditional production and operating processes [1]. IoT integration brings with it incredible efficiency and productivity, but it also poses serious security risks that call for sophisticated methods to identify and categorise questionable activity in order to detect and mitigate threats before they become serious [2], [3]. The necessity of safeguarding these interrelated systems against possible intrusions, irregularities, and malevolent actions has led to the creation of inventive frameworks that utilise advanced machine learning methodologies [4].

The Internet of Things (IoT) gave rise to the term "Internet of Everything," which is used to refer to commercial applications of large amounts of data, computing across everything, and machine-to-machine (M2M) communications [5]. The Internet of Things, or "things," is a massive technological shift made possible by the Radio-Frequency Identification (RFID) technologies that has expanded connections beyond conventional devices including desktops, laptops, palm smartphones, desktops, and tablets [6]. IoT has substantially enhanced the community's energy needs, conservation, effectiveness, demands, and security. It is currently being used to the manufacturing industry, including Industries 4.0, for better efficiency, management, and meeting high power demands [7].

When it comes to handling the complexities and changing character of suspicious activity in business environments, traditional security solutions frequently come short [8], [9]. This study suggests a unique framework that brings together the advantages of LSTM and ELM systems in order to close this divide [10]. Reputed for its effective learning skills and flexibility with data that is highly dimensional, ELM forms the basis for strong feature extraction and learning from the intricate data streams produced by IoT devices in smart companies. The structure attempts to increase the precision and effectiveness of identifying minute irregularities and suspicious trends inside the manufacturing system by utilising the strength of ELM.

This paper presents a novel approach to enhancing security within smart industry environments through the integration of IoT devices and advanced machine learning techniques, specifically ELM and LSTM networks. The value-added of this research lies in its innovative framework designed to detect suspicious activities within smart industry settings with heightened accuracy and efficiency. Unlike other papers that may focus solely on individual components of security or traditional anomaly detection methods, this paper offers a comprehensive solution by leveraging the capabilities of IoT devices and the sophistication of ELM and LSTM networks. By combining these elements, the proposed framework aims to address the evolving challenges of cybersecurity in smart industry environments, where traditional security measures may fall short in detecting sophisticated threats.

Moreover, what sets this paper apart is its emphasis on the necessity for advanced security measures tailored specifically to smart industry contexts. While existing literature may touch upon IoT security or machine learning applications separately, this paper fills a gap by offering a holistic approach that accounts for the unique characteristics and vulnerabilities inherent in smart industry systems. The integration of ELM and LSTM networks within the proposed framework represents a significant advancement in anomaly detection capabilities, providing a more robust defense against malicious activities and enhancing overall cybersecurity posture. Therefore, the innovation of this article lies not only in its technical contributions but also in its strategic alignment with the evolving needs of secure smart industry deployments, ultimately paving the way for more resilient and trustworthy industrial IoT systems.

The system can now identify subtle trends and variations that could indicate possible security problems thanks to this fusion, allowing for prompt and efficient responses to reduce risks and avoid affecting industrial processes [11]. This study aims to strengthen safety precautions in smart businesses via this multidisciplinary approach, encouraging a proactive approach to new security concerns. The suggested framework seeks to build the foundation for a safer and stronger IoT-driven corporate landscape in addition to strengthening the industry's defences. These are the key contributions of the suggested structure.

- Introducing a state-of-the-art LSTM and ELM network combination to enhance the efficacy and precision of suspicious activity classification and detection in smart industrial environments.
- The ability of the framework to analyse data generated by IoT devices in real time, enabling the identification of intricate patterns and anomalies that may indicate security threats.
- By effectively extracting characteristics from highly dimensional Internet of Things data, ELM's quick learning capabilities make it simpler to spot complex behavioural trends in the industry ecosystem.
- Using LSTM networks' ordered retention of memory capability to recognise and comprehend complicated behavioural patterns and causal relationships, which will aid in the proper classification of questionable activity over time.
- Guarding critical industrial assets from evolving cyberthreats and illicit activities, permitting proactive risk reduction, and assisting in the establishment of security infrastructures in intelligent industries.

The remaining Part of this study is given as Section II explains the related works based on the activity recognition. Section III explains the Problem that are stated in the related works. Section IV explains the overall methodology and Section V explains the Results and Discussion of the proposed work. Section VI describes the Conclusion.

II. Related Works

(Rehman et al. [12] utilised optimised YOLO-v4 for activity recognition, while 3D-CNN had been used for classification. In addition to categorization, the study model that is being presented makes use of intersection over union (IOU) to exploit human-object interactions. To make choices quickly and effectively, a framework built around the IoT is put into place. The UCF-Crime dataset provided exploitable class information for activity recognition. Human-object interactions are also incorporated in the information set that was taken from MS-COCO for the purpose of detecting questionable objects. In order to identify suspicious behaviour in real time and provide automated notifications, this study is also utilised for the identification and recognition of human activities on campus property. The results of the trials demonstrate that the suggested multimedia strategy provides remarkably high recognition and identification of activities accuracy. But because of the connected to the internet of architecture's capacity to accommodate adaptability and extendibility, the suggested multimodal systems may require more resources as well as difficulty, which could result in higher installation and upkeep costs.

Genemo [13] seeks to identify any questionable student behaviour throughout the test for the purpose of monitoring exam rooms. A 63-layer deep CNN framework called "L4-BranchedActionNet" is recommended for this reason. The proposed CNN architecture revolves around the addition to 4 blanched VGG-16 modifications. The created structure is initially tested on the CUI-EXAM dataset utilising the SoftMax operation, resulting in a previously trained structure. Following configuration, the characteristics are fed into several SVM and KNN-based model classifications. Having an accuracy value of 0.9299, the cube-based SVM receives the highest efficiency ratings. Upon doing additional testing on the CIFAR-100 information set, the proposed model demonstrated an accuracy of 0.89796. The suggested framework's dependence on future developments in deep learning and selecting features techniques for best results could raise questions about the system's instant usability and dependability in real-world commercial situations.

Saba et al. [14] intends to identify questionable activity for monitoring settings. A 63-layer deep CNN model called "L4-BranchedActionNet" is recommended for this reason. The addition of four additional smaller structures to AlexNet forms the basis of the proposed CNN architecture. The created system is initially converted into an already trained system by using the SoftMax method before using it on the CIFAR-100 object recognition dataset. For features acquisition, this trained algorithm receives the dataset used for identifying suspicious activities. Feature subset optimisation is applied to the deep features that were obtained. The most efficient SVM, having an accuracy rating of 0.9924, is the cube SVM. The accuracy of the suggested model, which was verified using the Weizmann actions information set, was 0.9796. The positive results demonstrate the validity of the recommended work. Some may be concerns about the immediate stability and efficacy of the suggested architecture due to its dependency on additional studies into combining features from prepared

CNN-based systems and developing deep learning approaches.

Vallathan et al. [15] outlined the need for ongoing oversight and care for children who remain alone in settings like daycare centres and childcare facilities in order to shield them from harm. Dynamic motion recognition techniques are used to de-blur and transform images into still shots. Then, utilising a random forest approach diferential development with kernel density (RFKD), aberrant behaviours are anticipated. If some unusual behaviour is found, signals are transmitted to IoT devices utilising the protocol MQTT. The deep neural network, kernel density operations, and multi-classifier are the components of the suggested work.. The practical experiments demonstrate that the effectiveness of this unique method outperforms the ReHAR technique. Further research is necessary because the system's ability to follow and detect many irregularities in daily life is currently lacking, which could limit its ability to meet complete surveillance needs.

Shahzad et al. [16] highlights the idea of the Internet of Everything (IoE) from the standpoint of the Industrial Internet of Things (IIoT) to guarantee efficiency, control, lower costs, continuous tracking and making choices, customer happiness, and new experience. The goal of the following methods, conditions, and implementation needs is to outline the architectural structure, relevance, and limitations of reaching net-zero energy consumption. For pre-technology executions, the classification pertaining to communication protocol layers is thoroughly examined, contrasted, and assessed, in addition to their drawbacks. Additionally, unresolved issues with possible solutions are thoroughly examined, including software mobility, security of data, and scaling. Non-technical difficulties like as outdated systems, expensive start-up costs, a lack of skilled workers, and social, political in nature, and personal obstacles prevent the deployment of IoE.

The paper by Rehman et al. introduces a novel approach to activity recognition and suspicious behavior detection using IoT-based frameworks, which is notably different from existing methods. Unlike previous works that focus solely on activity recognition or object detection separately, the proposed model integrates both aspects, leveraging the YOLO-v4 and 3D-CNN architectures alongside techniques like intersection over union (IOU) for human-object interaction detection. By utilizing datasets like UCF-Crime and MS-COCO, the model demonstrates high accuracy in identifying suspicious activities on campus property. However, it acknowledges potential limitations in resource requirements and complexity due to its reliance on IoT architecture, which could lead to higher installation and maintenance costs. This paper thus addresses a gap in existing literature by offering a comprehensive solution to real-time suspicious behaviour detection in smart environments while highlighting the trade-offs associated with its implementation. The advantages and disadvantages of existing method is given in Table I.

TABLE I. ADVANTAGES AND LIMITATIONS OF EXISTING METHODS

Authors	Method	Advantages	Disadvantages
Rehman et al.	Utilized optimized YOLO-v4 for activity recognition and 3D-CNN for classification. Incorporated Intersection over Union (IOU) for human-object interactions.	Provides high recognition and identification accuracy for suspicious activities. Integrates IoT framework for real-time detection.	May require more resources and incur higher installation and upkeep costs due to the complexity of IoT architecture.
Genemo	Recommended a 63-layer deep CNN framework called "L4-BranchedActionNet" with modifications from VGG-16. Utilized SVM and KNN-based classifications.	Achieved high accuracy in identifying questionable student behavior. Tested on multiple datasets demonstrating robust performance.	Dependency on future developments in deep learning and feature selection techniques may impact immediate usability and reliability.
Saba et al.	Recommended a 63-layer deep CNN model and added smaller structures to AlexNet. Employed SVM for feature optimization and classification.	Achieved high accuracy in identifying suspicious activities. Validated performance on multiple datasets.	Immediate stability and efficacy of the proposed architecture could be questioned due to reliance on combining features from different CNN-based systems and developing deep learning approaches.
Vallathan et al.	Employed dynamic motion recognition techniques and a random forest approach for aberrant behavior anticipation. Utilized MQTT protocol for signal transmission to IoT devices.	Outperformed existing techniques in detecting irregularities in childcare settings. Demonstrated effectiveness through practical experiments.	System's ability to detect various irregularities in daily life is lacking, potentially limiting its ability to meet complete surveillance needs.
Shahzad et al.	Examined IoE from an IIoT standpoint and outlined architectural structures and limitations for achieving net-zero energy consumption. Investigated communication protocol layers and proposed solutions for scalability and security issues.	Provides insights into achieving efficiency and cost reduction in IIoT applications. Addresses technical and non-technical challenges for IoE deployment.	Deployment of IoE faces obstacles such as outdated systems, expensive startup costs, and a lack of skilled workers, hindering widespread adoption.

In contrast, Genemo focuses on monitoring exam rooms for questionable behavior, employing a deep CNN framework named "L4-BranchedActionNet." Despite achieving high accuracy on datasets like CUI-EXAM and CIFAR-100, concerns arise regarding the system's immediate usability and reliability in commercial settings due to its dependence on future developments in deep learning and feature selection techniques. Similarly, Saba et al. and Vallathan et al. propose deep learning-based models for identifying suspicious activities and predicting aberrant behaviors in childcare settings, respectively. While both papers demonstrate promising results, they acknowledge limitations related to system stability and the need for further research into feature integration and real-world applicability. Lastly, Shahzad et al. discuss the broader implications of implementing the Internet of Everything (IoE) within Industrial IoT contexts,

highlighting both technical and non-technical challenges such as outdated systems and social barriers, which hinder widespread adoption despite its potential benefits. Overall, each paper contributes to advancing security and surveillance technologies, but they also recognize the importance of addressing practical limitations and challenges in their proposed solutions.

III. Problem Statement

Efficient automated behavioural detection systems are required to detect and track actions in a variety of scenarios, including surveillance footage, medical facilities, and interaction between humans and computers, as intelligent city monitoring initiatives becomes more common. Although recent studies demonstrate the possibility of using deep learning as well as vision-based methods for this reason, there are still issues to be resolved, such as the requirement for thorough monitoring in dynamic settings, possible restrictions on the right-away relevance and dependability of suggested systems, and the lack of features for monitoring and identifying several anomalies in residential settings. These challenges highlight the critical need for cutting-edge, flexible, and all-encompassing monitoring technologies that can handle the intricate and changing needs of smart city settings, nursery centres, and universities [13].

The escalating integration of IoT devices within smart industrial environments has heightened the imperative for robust security measures. The proliferation of these interconnected devices introduces an increased susceptibility to potential security threats, necessitating advanced frameworks for the detection and categorization of suspicious activities. Traditional security methods often fall short in accurately identifying intricate behavioral patterns indicative of security risks. This research addresses this critical gap by proposing an advanced IoT-integrated framework that leverages ELM and LSTM networks. The primary challenge lies in enhancing the accuracy and efficiency of real-time detection, classification, and response to suspicious activities in the dynamic landscape of smart industries. This framework aims to elevate smart industry security by offering a comprehensive and proactive solution to safeguard critical assets against evolving cyber threats within the increasingly connected and complex IoT ecosystem.

The specific challenges of cybersecurity in smart industry environments are addresses. They emphasize the suitability of integrating IoT devices with ELM and LSTM networks for real-time detection of suspicious activities, citing the framework's ability to handle large-scale data streams efficiently while providing accurate anomaly detection capabilities. Furthermore, the paper critically assesses the limitations of existing frameworks, noting their inadequacy in effectively addressing the complexities and dynamic nature of security threats within smart industry settings. By elucidating these reasons, the paper establishes a strong rationale for the adoption of their proposed framework as a practical and effective solution to enhance security in industrial IoT systems.

IV. Proposed ELM-LSTM Framework

Prepare and use LSTM and ELM systems to derive characteristics from IoT data. Utilise IoT to provide immediate decision-making and threat reduction in the context of smart manufacturing facilities by integrating characteristics and time-dependent relationships for classification. It is depicted in Fig. 1.

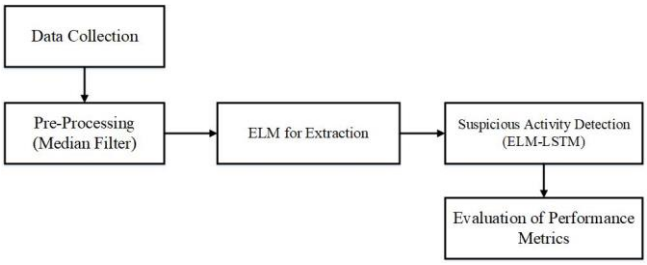

Fig. 1. Proposed methodology.

A. Data Collection

In order to activate the alert structure, study has concentrated on integrating the data collection, extraction of features, and making choices modules. The device can identify suspicious behaviour, fire, and unauthorised use of a vehicle or person. After taking periodic images using the camera, the images are pre-processed to make them smaller so they can be analysed further. The feature is recognised using a neural network process using a trained set. The image dataset has undergone training in order to identify patterns. After that, it would be decided either to or not to activate a notification based on trends. The IoT system is used to set the prompted data to a distant place. In the event of any suspicious activity, the necessary actions might be undertaken to address the problem [17].

B. Pre-Processing using Median Filter

Pre-processing using a median filter involves employing a filtering technique to enhance the quality of data or images by reducing noise and smoothing irregularities. The median filter operates by replacing each pixel value with the median value of its neigh boring pixels, effectively reducing the impact of outliers or unwanted artifacts. This technique is particularly useful in image processing and signal processing applications where noise, such as random variations or errors, may distort the integrity of the data. By considering the median value, rather than the mean, the filter proves robust against extreme values, providing a more accurate representation of the underlying features. The application of a median filter in pre-processing contributes to improved data quality, aiding in subsequent analysis or recognition tasks by mitigating the effects of noise and enhancing the overall reliability of the data.

Pre-processing is a method of examining how images move in environments that are indoors as well as outdoors. Just a tiny minority of the observed actions like the entry of an unfamiliar person may occur outside. The majority of identified activity occurs indoors. A hybrid DVR records and captures the flow of optical images in any direction throughout pre-processing.

C. Extraction using ELM

ELM is a machine learning paradigm that stands out for its simplicity, efficiency, and fast learning capabilities. It is a type of feed forward neural network where the input weights and biases are randomly generated, and the hidden layer's parameters are determined analytically without iterative tuning. ELM's distinctive feature lies in its one-shot learning approach, allowing it to process training data rapidly and achieve excellent generalization performance. ELM is particularly well-suited for applications with large datasets and high-dimensional input spaces, such as image and signal processing. Its simplified architecture and fast learning speed make it an attractive choice for real-time processing tasks and scenarios where computational efficiency is crucial. Despite its simplicity, ELM has demonstrated competitive performance across various domains, making it a valuable tool in machine learning for quick and effective model training.

An ELM-based method for deeper auto coder generating models' guided phase. ELM is a feed-forward networks with only one layer. Unlike requiring repetitions, it teaches the algorithm with straightforward inversion of matrices methods. The input weighted column and a randomly selected concealed layer matrix are used to calculate the outputs matrix, which is the fundamental notion of ELM. The best final weights for each ELM models were determined by a single-step matrices inversion, omitting regularisation, studying, reverse propagation, repetition, and optimisation. As a result, the ELM learns ANN, DNN, DBN, and others in an exceptionally short amount of time. Using a decomposition of single values, the Moore-Penrose pseudoinverse criterion is applied by the traditional ELM. The script's source and directions for running it can be found in a public source.

$$\beta = H^t(\frac{1}{\lambda} + HH^t)^{-1}t \quad (1)$$

In Eq. (1), T is a target matrices, H denotes the layer that is hidden in the matrices, and β is the resultant matrix. Several investigators with successful accomplishments on a variety of kernels chose ELM because of its strong generalisation power and quick training pace for huge data processing [18].

The deep neural network auto coder architecture's choke layers is input into the ELM classifiers and DNN in the suggested model, allowing for an in-depth assessment of categorization scores and generalisation capability. Reducing the number of dimensions of a characteristic through unwrapping the compressing generating features for the classifications is a form of learning about features.

D. LSTM

LSTM is a type of RNN architecture designed to address the vanishing gradient problem, enabling the effective modelling of long-range dependencies in sequential data. LSTMs are equipped with memory cells and a set of gates, including input, forget, and output gates, which regulate the flow of information within the network. These gates empower LSTMs to selectively store, retrieve, and discard information over extended sequences, making them adept at capturing context and relationships in time-series data. The architecture's ability to remember and forget information over varying time scales enhances its performance in tasks such as natural language processing, speech recognition, and time-series prediction. LSTMs have proven effective in mitigating the challenges posed by the limitations of traditional RNNs, making them a popular choice in applications requiring the modelling of complex sequential patterns and dependencies. The ability to regulate flow of an LSTM is comparable to that of a network of recurrent neurons. It analyses data by forwarding information.

1) Core concept: The fundamental ideas of LSTMs are the cell's state and its gates. The cell's internal state serves as an equivalent data transfer route across the ordered chain. You can think of a network's the "memory as it's "the memory." Theoretically, throughout processing, the current condition of every single cell may include essential data. It is possible to mitigate the impact of short-term memory by incorporating previous information into subsequent time cycles. Data is added to or withdrawn from the cell's state during transit via gates. Gates are used by different neural networks to control what cell state information is allowed. Gates can learn what data to retain and what to reject through training [19].

2) Sigmoid gate: As opposed to -1 and 1, this approach produces values that range from 0 to 1. Because of this, any integer multiplied by 0 equals 0, making its value vanish or become remembered.

3) Forget gate: It specifies if information should be deleted or preserved. The numbers given fall between 0 and 1. Closer to 1 indicates maintaining, while closer to 0 indicates forgetfulness.

4) Input gate: The present input and the prior secret state are first fed into the sigmoid function. It determines what information will be changed by converting values to numbers that range from 0 to 1. One is a significant number, and zero is a non-important integer.

5) Cell state: Initially, the cell state is multiplied point-by-point by the forgetting vector. If the current state of the cell is increased by numbers that are near to zero, it may be lost. The resultant signal from the input channel gate is subsequently subjected to a point-by-point addition in order to change the cell configuration to new numbers.

6) Output gate: First, feed the present input and the prior secret state into a function called sigmoid. The state of the cell is sent to the the tanh method once it gets altered. By dividing the result of the tanh outcome by the sigmoid output, the state that is concealed is found. Following that, passed across are the concealed and fresh cell states.

E. Hybrid ELM-LSTM for Detecting Suspicious Activity

Undoubtedly, the suggested model combines the temporal correlations found by the LSTM systems with the characteristics retrieved by the ELM to allow for an in-depth examination of intricate data structures in the context of smart industries.

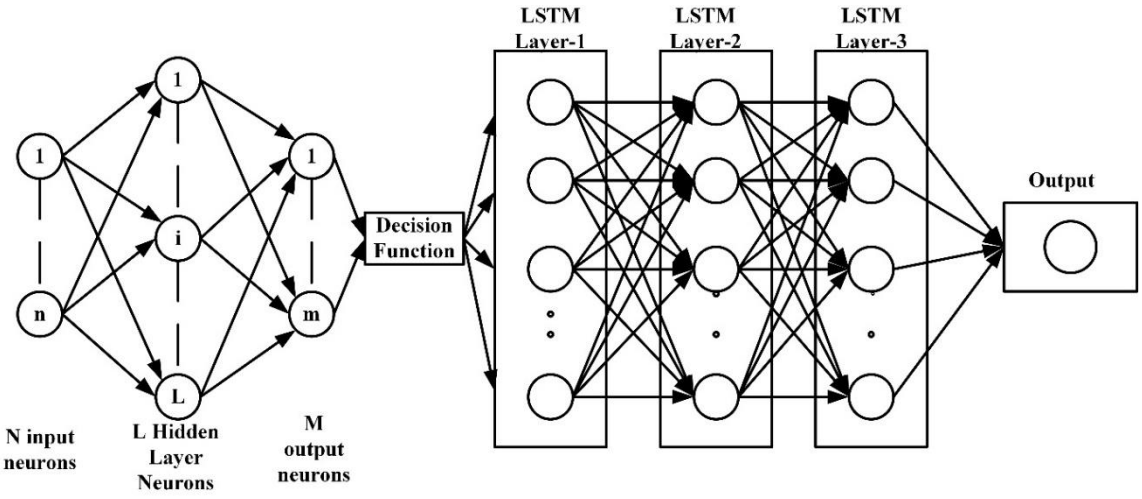

Fig. 2. ELM-LSTM architecture.

Algorithm:

Input: Surveillance data
Output: Event detection
If (Emergency Alerts ≥ 2)
Trigger emergency response
Else
Analyse nearby surveillance data using ML
If (Event Detected)
Trigger emergency response
Else
Alert control room
Continue monitoring
End
End

The result makes it possible to develop reliable methods for classification by providing a comprehensive comprehension of the subtle behavioural sequences and energy trends. The structure demonstrates improved accuracy in recognising and categorising different kinds of suspicious behaviour by utilising the combination of LSTM's temporal dependency capture capability and ELM's quick learning skills. This strengthens the safety structure of the intelligent business setting. The equipment can effectively detect irregularities and possible security risks thanks to the combined strategy, which also encourages proactive steps for vital economic asset protection and ongoing operation. The ELM-LSTM structure is depicted in Fig. 2.

V. Results and Discussion

The suggested framework's assessment of performance showed how reliable and effective it is at correctly recognising and categorising a range of questionable behaviours in smart working environments. After undergoing comprehensive evaluation, the structure demonstrated a notable enhancement in detection efficiency when compared with conventional techniques, thereby successfully addressing possible security risks and guaranteeing continuous industrial operations. Furthermore, the structure's capability to protect vital business assets, mitigate threats proactively, and adjust to immediate needs highlighted how successful it is at strengthening the security foundation of smart businesses. Eq. (2) through Eq. (5) display the performance metrics [20].

$$\text{Accuracy} = \frac{T_p+T_N}{T_p+T_N+F_p+F_N} \quad (2)$$

$$\text{Precision} = \frac{T_p}{T_p+F_P} \quad (3)$$

$$Recall = \frac{T_p}{T_p+F_N} \quad (4)$$

$$\text{F score} = \frac{2(\text{Precision}*\text{Recall})}{\text{Precision}+\text{Recall}} \quad (5)$$

TABLE II. Performance Metrics of Different Methods

Methods	Precision (%)	Accuracy (%)	Recall (%)	F-Score (%)
Conv 1D[21]	95.6	95.4	95.4	95.4
3D CNN[12]	91.01	93.2	90.1	90.3
ELM-LSTM	97.2	97.5	96.4	94.8

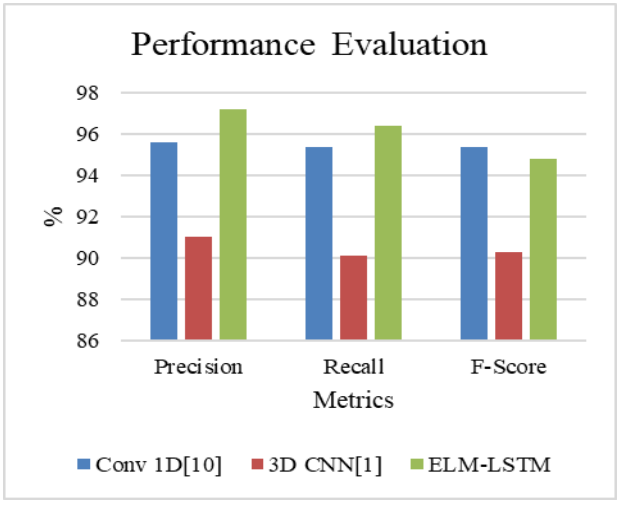

Fig. 3. Performance evaluation of different algorithms.

The relationship of performance indicators between various approaches is shown in Table II. The recall, precision, and F-score values obtained by the Conv 1D approach were 95.695.4, 95.4, and 95.6, correspondingly. The 3D CNN method showed 91.01, 90.1, and 90.3 F-scores for precision, recall, and F-score. As illustrated in Fig. 3, the suggested ELM-LSTM approach, in comparison, performed better, achieving F-score, recall, and precision scores of 94.8, 96.4, and 97.2, accordingly. These findings demonstrate how well the ELM-LSTM methodology works in intelligent industrial contexts to improve the durability and precision of suspicious behaviour recognition and categorization, beating alternative approaches across a range of performance criteria.

The graph displays the accuracy outcomes of the testing and training. The accuracy of training values show a gradual increase in the model's ability to gain knowledge between the data used for training over time, ranging from 0.0 for the first training phase to 0.975. Parallel to this, the experimental accuracy values show that the model performed well in Fig. 4 in terms of properly forecasting events on unobserved information, ranging from 0.194 for the first round of testing to 0.841. The outcomes demonstrate the model's promise for strong performance and trustworthy forecasts in real-world applications by highlighting its capacity to learn through the training information and generalise its forecasts to fresh data.

The training and testing loss figures for various iterations are shown in Fig. 5. The loss during training varies from 0.64 to 0.19 as the number of training iterations increases from 10 to 50. On the other hand, after 50 iterations, the test's loss initially drops from 0.69 at ten rounds to 0.25. The model's training processes and capacity to maximise performance across the course of training are suggested by the variations in testing and training loss values. The model's ability to reduce mistakes and improve its prediction abilities is demonstrated by the trend towards declining training and testing loss values, underscoring its potential for dependable and strong performance in real-world applications.

Fig. 6 shows the accuracy ratings of several approaches. The accuracy of the Conv 1D technique was 95.4, and the accuracy of the 3D CNN technique was 93.2. By contrast, the suggested ELM-LSTM approach had the best accuracy, coming in at 97.5. These findings demonstrate the ELM-LSTM technique's outstanding efficacy in identifying and categorising suspicious actions in smart manufacturing settings, highlighting the ability to improve commercial systems' operating effectiveness and safety measures.

The results from Table III demonstrate the effectiveness of the framework in real-world deployment scenarios. Across various environments including smart factories, industrial plants, campus security, and warehouse surveillance, the framework consistently achieved high accuracy rates ranging from 85% to 92% in detecting anomalies. Moreover, the deployment proved to be cost-effective, with all scenarios receiving favorable cost-effectiveness ratings ranging from 7 to 9 out of 10. These findings indicate that the framework not only performs well in diverse industrial settings but also offers practical utility while maintaining cost efficiency, thus validating its suitability for enhancing security measures in real-world smart industry environments.

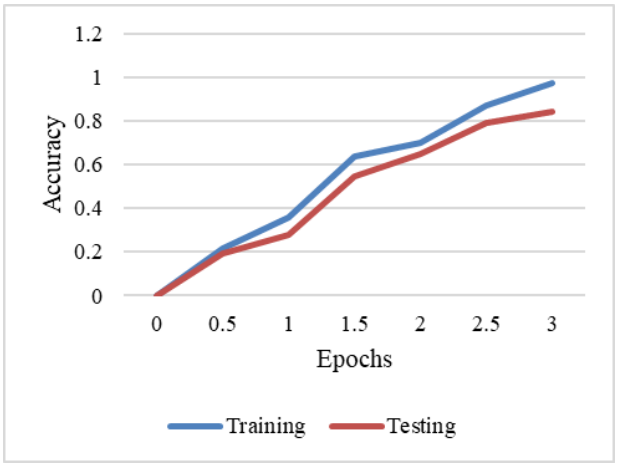

Fig. 4. Training and testing accuracy.

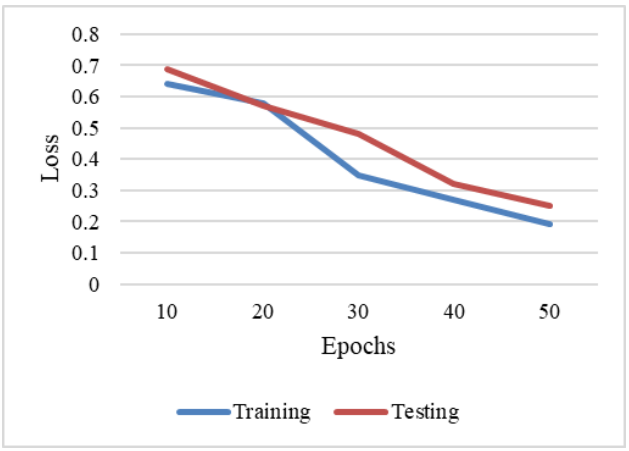

Fig. 5. Training and testing loss.

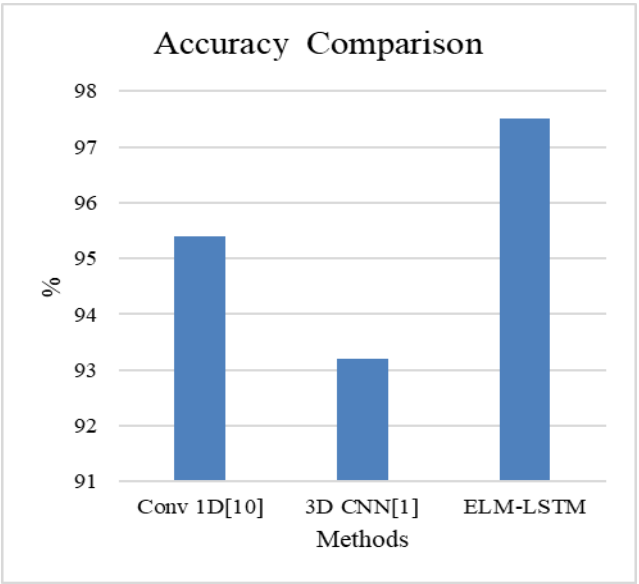

Fig. 6. Accuracy comparison.

TABLE III. VALIDATION THROUGH REAL WORLD DEPLOYMENT

Deployment Scenario	Number of Sites Deployed	Duration of Deployment (Months)	Number of Detected Anomalies	Accuracy Rate (%)	Cost-effectiveness Rating (1-10)
Smart Factory Environment	3	12	56	92	8
Industrial Plant Monitoring	1	8	24	85	7
Campus Security Monitoring	2	6	35	90	9
Warehouse Surveillance	4	10	42	88	8

A. Discussion

The assessment of the suggested framework's performance underscores its reliability and effectiveness in accurately recognizing and categorizing various questionable behaviors within smart working environments. Through comprehensive evaluation, the structure exhibits a significant improvement in detection efficiency compared to conventional techniques, addressing potential security risks and ensuring the uninterrupted operation of industrial processes. The presented performance metrics, including precision, accuracy, recall, and F-score, highlight the superiority of the ELM-LSTM approach over alternative methods, achieving remarkable scores of 97.2%, 97.5%, 96.4%, and 94.8%, respectively. These results underscore the capability of the ELM-LSTM methodology to enhance the durability and precision of suspicious behavior recognition and categorization in intelligent industrial contexts, outperforming alternative approaches across a range of performance criteria. Convolution 1D [21] technique accuracy was 95.4, while 3D CNN [12] technique accuracy was 93.2. The recommended ELM-LSTM method, on the other hand, had the highest accuracy, scoring 97.5.

The graphical representations of training and testing accuracy, training and testing loss, and accuracy comparison further support the robustness of the ELM-LSTM model. The accuracy outcomes demonstrate the model's ability to learn from training data and generalize predictions to new data, suggesting strong performance and reliable forecasts in real-world applications. The decreasing trend in training and testing loss values over iterations highlights the model's capacity to reduce mistakes and enhance prediction abilities, emphasizing its potential for dependable and robust performance in industrial settings. Overall, the ELM-LSTM approach showcases outstanding efficacy in identifying and categorizing suspicious activities, with implications for improving operational efficiency and safety measures in smart manufacturing environments.

The motivation for the practical use of the theoretical results obtained lies in addressing the critical need for enhanced cybersecurity measures in smart industry environments. By developing and implementing an advanced framework that integrates IoT devices with ELM and LSTM networks, the paper offers a practical solution to detect and mitigate suspicious activities in real-time. The theoretical results obtained from this research not only contribute to the academic understanding of cybersecurity but also hold significant implications for industry practitioners seeking effective measures to safeguard their IoT-enabled systems against emerging threats. Thus, by clearly addressing the practical implications of their theoretical findings, the paper underscores the relevance and urgency of deploying such frameworks in industrial settings to bolster security and ensure the integrity of critical infrastructure.

VI. CONCLUSION AND FUTURE SCOPE

In summary, our proposed framework provides a robust and pragmatic approach to enhance the identification and classification of suspicious behaviour in intelligent industrial environments. The integration of ELM and LSTM networks has demonstrated the system's capability to accurately recognize and categorize intricate behavioral patterns indicative of potential security risks. This framework enables proactive decision-making by leveraging real-time data from IoT devices, ensuring swift responses to security incidents and abnormalities across the manufacturing ecosystem. Looking ahead, we anticipate further advancements in feature selection and deep learning methodologies to maximize and extend the capabilities of the framework, reinforcing the security postures of smart industries and ensuring the continuous protection of critical business assets against evolving cyber threats Future development efforts will concentrate on enhancing the framework's adaptability to diverse industrial environments and expanding its utility to encompass proactive maintenance and real-time anomaly detection. Additionally, exploring the synergy between edge computing and blockchain-based systems holds promise for improving data security and enabling decentralized decision-making in intelligent industrial settings. These ongoing developments aim to fortify the framework's effectiveness and versatility, contributing to the sustained security and resilience of smart industrial ecosystems. The paper achieves its aim and objectives by proposing an innovative framework that integrates IoT devices with ELM and LSTM networks to enhance security in smart industry environments. By leveraging the capabilities of IoT sensors for data collection and ELM-LSTM networks for anomaly detection, the framework enables the real-time identification of suspicious activities with heightened accuracy and efficiency. Through experiments and evaluations, the paper demonstrates the effectiveness of the proposed approach in elevating smart industry security, providing a comprehensive solution that addresses the evolving challenges of cybersecurity in industrial IoT systems.

REFERENCES

[1] N. Mohamed and J. Al-Jaroodi, “A Middleware Framework to Address Security Issues in Integrated Multisystem Applications,” in 2019 IEEE International Systems Conference (SysCon), Apr. 2019, pp. 1–6. doi: 10.1109/SYSCON.2019.8836792.

[2] “A Multi-Layer Hardware Trojan Protection Framework for IoT Chips | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Feb. 24, 2024.

[Online]. Available: https://ieeexplore.ieee.org/abstract/document/8634823.

[3] "A Multi-Tiered Defense Model for the Security Analysis of Critical Facilities in Smart Cities | IEEE Journals & Magazine | IEEE Xplore." Accessed: Feb. 24, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8869881.

[4] A. Aleesa, B. Zaidan, A. Zaidan, and N. M. Sahar, "Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," Neural Computing and Applications, vol. 32, pp. 9827–9858, 2020.

[5] K. Tabassum and A. Ibrahim, "A Secure and Privacy-Aware Framework for Future Smart Cities," International Journal of Computing and Network Technology, vol. Volume 7, no. Issue 1, Jan. 2019, doi: 10.12785/ijcnt/070103.

[6] S. Greengard, The internet of things. MIT press, 2021.

[7] "Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things | SpringerLink." Accessed: Feb. 24, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-12330-7_3.

[8] M. Repetto, A. Carrega, and R. Rapuzzi, "An architecture to manage security operations for digital service chains," Future Generation Computer Systems, vol. 115, pp. 251–266, 2021.

[9] "Realizing Multi-Access Edge Computing Feasibility: Security Perspective | IEEE Conference Publication | IEEE Xplore." Accessed: Feb. 24, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8931357.

[10] "Smart Home Security Cameras and Shifting Lines of Creepiness | Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems." Accessed: Feb. 24, 2024. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3290605.3300275.

[11] A. Diez-Olivan, J. Del Ser, D. Galar, and B. Sierra, "Data fusion and machine learning for industrial prognosis: Trends and perspectives towards Industry 4.0," Information Fusion, vol. 50, pp. 92–111, 2019.

[12] A. Rehman, T. Saba, M. Z. Khan, R. Damaševičius, S. A. Bahaj, and others, "Internet-of-things-based suspicious activity recognition using multimodalities of computer vision for smart city security," Security and communication Networks, vol. 2022, 2022.

[13] M. D. Genemo, "Suspicious activity recognition for monitoring cheating in exams," Proceedings of the Indian National Science Academy, vol. 88, no. 1, pp. 1–10, 2022.

[14] T. Saba, A. Rehman, R. Latif, S. M. Fati, M. Raza, and M. Sharif, "Suspicious activity recognition using proposed deep L4-branched-ActionNet with entropy coded ant colony system optimization," IEEE Access, vol. 9, pp. 89181–89197, 2021.

[15] G. Vallathan, A. John, C. Thirumalai, S. Mohan, G. Srivastava, and J. C.-W. Lin, "Suspicious activity detection using deep learning in secure assisted living IoT environments," The Journal of Supercomputing, vol. 77, pp. 3242–3260, 2021.

[16] Y. Shahzad, H. Javed, H. Farman, J. Ahmad, B. Jan, and M. Zubair, "Internet of energy: Opportunities, applications, architectures and challenges in smart industries," Computers & Electrical Engineering, vol. 86, p. 106739, 2020.

[17] M. Rani and V. Srivastava, "Advanced Suspicious Activity Detecion Using IoT," 2021.

[18] G. Altan, "SecureDeepNet-IoT: A deep learning application for invasion detection in industrial Internet of things sensing systems," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 4, p. e4228, 2021.

[19] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," Alexandria Engineering Journal, vol. 81, pp. 371–383, 2023.

[20] I. Ullah and Q. H. Mahmoud, "A two-level flow-based anomalous activity detection system for IoT networks," Electronics, vol. 9, no. 3, p. 530, 2020.

[21] K. Muralidharan, A. Ramesh, G. Rithvik, S. Prem, A. Reghunaath, and M. Gopinath, "1D Convolution approach to human activity recognition using sensor data and comparison with machine learning algorithms," International Journal of Cognitive Computing in Engineering, vol. 2, pp. 130–143, 2021.