ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

Enhancing Security Through Predictive Analytics and Anomaly Detection in Iot-Enabled Systems

[1] Zaheer sultana *, [2] Deepak kumar

[1] Banasthali Vidyapith, Computer Science and Engineering, PhD Student, India,304022
[2] Banasthali Vidyapith, Computer Science and Engineering, Assistant Professor, India,304022
Corresponding Author Email: [1] zaheersultana786@gmail.com, [2] deepakkumar@banasthali.in

Abstract— ***The framework that uses sophisticated deep learning algorithms and data preparation to improve anomaly detection in Internet of Things systems. In order to standardize location coordinates and minimize the computational load on the network, the first data transformation uses Min-Max normalization. Next, it is shown how to use Principal Component Analysis (PCA) to efficiently reduce dimensionality while maintaining important information in high-dimensional datasets that are frequently used in Internet of Things applications. The process of standardization in principle component analysis (PCA) guarantees fair feature contributions. The covariance matrix is then computed, which makes it easier to extract principal components and capture the maximum variance in the data. Additionally, by using CNNs' ability to autonomously learn hierarchical representations straight from pictures, the paper suggests integrating CNNs for image-based anomaly identification. The CNNs are very good at identifying abnormal from normal patterns across a wide range of domains because they use transfer learning and encoder-decoder architectures to capture complex patterns. With accuracy of 90.91%, recall of 87.9%, F1-score of 90.3%, and a ROC value of 95%, the proposed CNN model shows encouraging results, highlighting its resilience in anomaly identification. Looking ahead, the area of work includes improving methods for detecting anomalies through creative pretreatment of data and fine-tuning CNN structures to make them more flexible in the face of changing Internet of Things scenarios. The investigation of ensemble methods and reinforcement learning offers further opportunities to boost anomaly detection systems' accuracy and robustness. Overall, this study offers a thorough and practical method for IoT anomaly detection, adding to the changing field of intelligent and connected devices.***

Index Terms— ***Anomaly Detection; Min-Max Normalization; Principal Component Analysis; Convolutional Neural Networks; Dimensionality Reduction.***

I. INTRODUCTION

A new age of connectedness has been brought about by the widespread use of Internet of Things (IoT) technology, which has made it possible for objects to communicate and share data with ease. This interconnection creates a multitude of security issues in addition to previously unheard-of potential for efficiency and ease. Protecting these networks from possible attacks becomes critical as IoT-enabled equipment grow more and more integrated into different businesses [1]. Given this, combining anomaly detection with predictive analytics seems to be a potent way to improve security in IoT environments. An enormous network of devices, ranging from sophisticated machines to sensors and actuators, all interacting and sharing data in real-time, characterizes the Internet of Things environment [2]. Potential cyber threats, such as data breaches and unauthorized access to and manipulation of vital systems, might thrive on this interconnected web. Even though they are crucial, traditional security measures frequently fail to meet the dynamic and varied nature of IoT risks. On the other hand, predictive analytics provides a proactive approach by using sophisticated algorithms and historical data to predict possible security breaches before they happen. In the framework of IoT security [3], predictive analytics entails the examination of sizable datasets produced by networked devices.

Predictive analytics use patterns, trends, and correlations found in this data to build models that anticipate possible security concerns. By facilitating proactive decision-making, these models help organizations strengthen their IoT infrastructure against new threats and put preventative measures in place [4]. One of the most important advantages in the continuous fight against cyber threats in the IoT ecosystem is the capacity to anticipate and stop security events before they happen. Anomaly detection, with its emphasis on IoT network real-time monitoring, is a complement to predictive analytics [5]. It entails determining how certain systemic behaviours and patterns deviate from the norm. Anomalies may indicate system faults or possible security breaches. Malicious activity can also be indicated by anomalies. Anomaly detection systems can quickly identify and address unexpected occurrences by utilizing complex algorithms, which reduces the effect of security problems and stops them from getting worse [6]. Predictive analytics and anomaly detection work together to give IoT-enabled systems a strong security foundation. Anomaly detection tracks activity in real time and spots abnormalities that can point to a security breach that is still underway, whereas predictive analytics uses past data to forecast hypothetical risks. In order to address the constantly changing issues surrounding IoT security, a comprehensive plan that combines preventive and reactive methods is formed. The growing use of IoT by many sectors has made the incorporation of anomaly detection and predictive analytics essential to maintaining the robustness and consistency of networked systems.

The key contributions of this study are as follows:

- A crucial step in the data preparation stage is the application of Min-Max normalization to the location coordinates (x, y, z). This method guarantees that the numerical properties are set to a desired range, usually [0,1]. The network's capacity to converge is enhanced and the computational burden is lessened as a result. Data may be prepared for analysis and target identification algorithms by applying Min-Max normalization, which is well-known for putting data into a consistent scale.
- The Principal Component Analysis (PCA) technique is used to reduce dimensionality, which is particularly important when working with high-dimensional datasets that are frequently encountered in Internet of Things (IoT) applications. The main components of PCA are a new collection of uncorrelated variables that are created from the original characteristics. They are ranked according to how much variance they can explain. This lowers the complexity of the data while maintaining critical information, which helps to improve analysis and target identification algorithms.
- The data is first standardized, which eliminates the mean and uses the standard deviation to scale the data, before PCA is used. Standardization guarantees that every feature makes an equal contribution to the analysis. The PCA procedure then computes the covariance matrix of the standardized data. The interactions between various properties are captured by the covariance matrix, which offers important insights into the interdependencies between variables.
- Convolutional Neural Networks (CNNs) are a key contribution for image-based anomaly identification. Hierarchical representations and patterns may be automatically learned from photos by CNNs. Employing CNNs for anomaly detection involves many fundamental tactics, including the encoder-decoder architecture, transfer learning, and one-class classification methodology. CNNs have demonstrated to be versatile in finding abnormalities in a variety of circumstances by the application domains, which include security monitoring, industrial defect identification, and medical picture analysis.

The research began with a preliminary study of the literature review, which is presented in Section 2. Next, research gasps are presented in Section 3. The research was performed according to the proposed research methodology and is presented in Section 4. The results of the study are presented and discussed in Section 5. Finally, the conclusions and limitations are presented in Section 6.

II. LITERATURE WORKS

The Internet of Things' (IoT) explosive growth has made it necessary to thoroughly investigate a variety of architectural frameworks in order to properly handle the wide range of devices and applications that are part of its ecosystem [7]. This literature study explores several IoT designs and offers a thorough examination of their functionality, parts, and topologies. Both centralized and decentralized architectures are included in the survey, along with their benefits and drawbacks. Important factors like security, interoperability, and scalability are examined in detail to provide insightful information on how IoT systems are changing. Despite offering a thorough overview of current IoT designs, the study is limited by how dynamic the IoT space is. Some of the designs provided may become obsolete or inadequately adaptive to new requirements due to the rapid growth of technology and standards. Furthermore, by concentrating on generalized qualities, the survey may fail to capture the subtleties of particular use cases or sectors. To customize architectural considerations to the specific requirements of different IoT applications, further study could be needed for a more detailed understanding. Notwithstanding these drawbacks, the study provides a useful starting point for understanding the broad patterns and difficulties in the wide field of IoT configurations.

The Internet of Things study examines popular IoT architectures, from centralized to decentralized models, explaining their features and characteristics [8]. It also analyses the underlying protocols that control Internet of Things connection, emphasizing their functions in guaranteeing smooth connectivity and data interchange. The investigation goes further and includes an overview of applications in a number of fields, demonstrating the revolutionary potential of IoT in industries including smart cities, healthcare, and agriculture. The purpose of this research is to provide readers a comprehensive knowledge of the complex interactions that exist between applications, protocols, and architectures in the ever-changing IoT world. This study is thorough in its analysis of IoT architectures, protocols, and applications, but it suffers from the inherent difficulty of staying relevant in real time. Some parts of IoT standards and techniques may become obsolete or inadequately representative of current circumstances of the industry due to their fast evolution. Furthermore, the extensive coverage may jeopardise in-depth study by perhaps ignoring subtleties unique to certain use cases. To overcome these drawbacks, it is advised to conduct ongoing updates and further research in order to stay abreast of IoT advancements and guarantee that the insights gained from this review will be relevant for a long time.

Prediction work introduces a predictive model for making decisions on patient disposition, addressing the crucial topic of optimizing resource allocation in emergency rooms [9]. This research uses machine learning approaches to predict if a patient should be hospitalized or released from the emergency department with the goal of improving efficiency and responsiveness. The model makes use of past patient data to find trends and variables that affect disposition choices, which helps to allocate resources in a proactive and knowledgeable manner. In the end, the project hopes to improve emergency department operations by providing medical professionals with a tool that helps them allocate resources in advance depending on patient outcomes. Although the suggested predictive model offers a potential way to enhance the distribution of resources in emergency rooms, the intricacies of healthcare dynamics are the cause of its shortcomings. The dynamic character of patient situations and the constantly changing field of medical knowledge make it difficult to keep the model accurate over time. Furthermore, because the model depends on past data, it might not be able to quickly adjust to abrupt changes in patient demographics or medical procedures or properly capture new trends. Furthermore, careful thought must be given to the ethical issues around patient privacy and data security when using these prediction technologies. Continuous model validation and improvement, together with a strong framework for data governance and ethical usage, are essential to addressing these issues and guaranteeing the model's useful and long-lasting use in emergency healthcare settings.

Equitable allocation of healthcare resources study introduces fair survival models in an effort to support the moral and just allocation of healthcare resources [10]. The study suggests models that include fairness issues in addition to predicting patient survival outcomes in the context of resource allocation, namely in healthcare settings. Our method attempts to correct for differences in resource distribution by adding fairness criteria into survival models, guaranteeing that decision-making procedures are impartial and reliable. The work offers a fresh viewpoint on striking a balance between equity considerations and forecast accuracy by using a variety of datasets to train and verify these fair survival models. In order to create a more equitable and just healthcare system, the ultimate objective is to arm legislators and healthcare managers with instruments that support equitable resource distribution. Although the implementation of fair survival models is a big step in the right direction for allocating resources in healthcare fairly, there are some disadvantages that should be taken into account. There are difficulties in defining fairness in a way that is generally applicable, and fairness measurements are intrinsically context-dependent. The models' dependence on past data may unintentionally reinforce preexisting biases, and the training data's comprehensiveness and representativeness determine how well the models reduce gaps. Furthermore, balancing fairness and predictive accuracy may need thorough calibration in order to achieve the best possible balance. We also need to continue paying attention to ethical issues, especially as they relate to how fairness indicators are interpreted and used. In order to achieve a more equal and efficient distribution of healthcare resources, it is imperative that there be constant engagement with stakeholders in the healthcare industry and that the models be continuously improved based on input from the actual world.

Predictive Modelling paper explores the complex field of predictive modeling [11] for readmissions from hospitals with the goal of illuminating the difficulties present in this vital area of healthcare and offering workable answers. Healthcare systems are heavily burdened by hospital readmissions; predictive modelling provides a proactive means of identifying individuals who may be at-risk. The study explores the challenges of developing precise prediction models, taking into account characteristics related to patient demographics, medical history, and socioeconomic status. It also examines issues with temporal dynamics, interpretability of models, and data quality. In order to increase the efficacy of hospital readmission prediction models, the study not only identifies these issues but also suggests workable remedies, such as enhanced data gathering tactics and sophisticated machine learning approaches. Although this study offers insightful information, it must be understood that it has inherent limitations. Predictive models can only be useful if thorough and current data are available, and there are still issues with maintaining consistency and completeness in healthcare databases. As patient demographics change and healthcare procedures become more dynamic, certain prediction models may become less reliable over time. Additionally, there is a trade-off between the accuracy of sophisticated models and their interpretability and their ability to effectively convey results to healthcare practitioners. A constant focus is needed on ethical issues, especially those pertaining to biases present in historical data. The continued usefulness and dependability of predictive models for hospital readmission depend on addressing these issues through continual multidisciplinary cooperation, validation research in many healthcare settings, and a dedication to moral and open model development.

III. PROBLEM STATEMENT

The Internet of Things' (IoT) explosive growth has made it necessary to investigate several architectural frameworks in order to accommodate a range of devices and applications. But the dynamic nature of IoT poses problems as well since standards and technology are always changing, which results in out-of-date designs and an inability to meet new demands. Further research is required to customise architectural considerations for various IoT applications, as current literature may ignore certain use cases or sectors. Healthcare practices are dynamic, and data quality and interpretability are major obstacles to the use of predictive modelling in identifying at-risk patients, especially for hospital readmissions. The application of these prediction systems requires careful consideration of ethical issues, especially those pertaining to patient privacy and data security. In order to overcome inequities and biases, fair survival models have been introduced into healthcare resource allocation; however, due to the difficulty of establishing fairness measures that are relevant to all situations and the possibility of bias reinforcement in historical data, this approach must be carefully considered. Finding the right balance between predictability and fairness is a difficult task that calls for constant fine-tuning and ethical examination. For the Internet of Things, healthcare predictive modelling, equitable resource allocation, and ethical application, creative solutions and ongoing model improvement are required. Resolving these problems would help create more reliable and fair systems in these important domains.

IV. PROPOSED

The proposed data pre-processing methodology integrates Min-Max normalization, Principal Component Analysis (PCA), and Convolutional Neural Networks (CNNs) to optimize anomaly detection in IoT-enabled systems. Min-Max normalization ensures that position coordinates are scaled to a standardized range, minimizing computational load and aiding network convergence. PCA is employed for dimensionality reduction, transforming high-dimensional data into uncorrelated variables while preserving crucial information. Subsequently, CNNs, equipped with encoder-decoder architectures and transfer learning, are harnessed for image-based anomaly detection, enabling automatic learning of hierarchical representations from images. This comprehensive approach enhances the efficiency and accuracy of anomaly detection in diverse IoT applications, offering adaptability and robustness across different domains. Fig. 1 depicts the Proposed Workflow for Anomaly Detection.

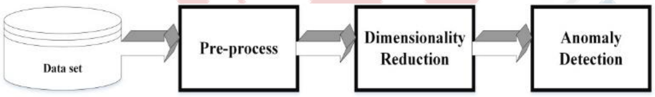

Fig. 1. Proposed Workflow for Anomaly Detection

A. Data Pre-Processing

The transformed data has been subjected to data standardization in an effort to lighten the network's computational load. The position coordinates, x, y and z are normalized using a Min-Max method to the range [0,1] [12]. The ability of the network to converge is improved by using Max-Min normalization and learning bounded objectives. The basic data preparation technique of min-max normalization to guarantee that the numerical characteristics or parameters are adjusted to a particular range, often between 0 and 1. In order to improve the suitability for analysis and target detection algorithms, raw data values must be standardized in this procedure. By aligning the data into the algorithms' desired inputs range, min-max normalization increases the efficiency and precision of the techniques. By moving these outliers closer to the top or lower boundaries of the normalized range, Min-Max normalization may assist in highlighting them and make them easier to differentiate from regular traffic patterns. The initial data set is transformed linearly by the Min-Max normalization approach. When some characteristic's minimum and maximum values are normalized using the Min-Max formula, the initially set value of the attribute gets replaced with the value within the interval [0,1]. The formula is given in (1):

$$X_{Norm} = \frac{X-X_{min}}{X_{max}-X_{min}} \quad (1)$$

Where Min and Max be the minimum and maximum values of typical X_{Norm}, accordingly, the initial value of X is changed by Min-Max normalization to the value in the range [0,1].

B. Dimensionality Reduction using PCA

Reducing dimensionality is an essential step in the preparation of data, particularly when working with high-dimensional datasets that are frequently used in Internet of Things applications. A popular method for reducing feature dimensions while keeping important information intact is principal component analysis, or PCA [13]. Converting the original characteristics into a new collection of uncorrelated variables known as principle components and ranking them according to how much variance they explain is the main goal of principal component analysis (PCA). PCA seeks to maintain the greatest amount of variation in the data while projecting it onto a lower-dimensional subspace. Examine a dataset consisting of n observations and d features. This dataset can be expressed as a $n \times d$ matrix X, in which a feature is represented by a column and each observation by a row.

1) Standardization

Standardizing the data is generally advantageous prior to using PCA. To do this, remove the mean from the data, then scale it using the standard deviation to centre it. By ensuring that every characteristic contributes equally to the analysis, standardization keeps factors with greater scales from swaying the outcomes. To calculate the standard deviation σ for each feature, remove the mean μ and divide the result is expressed in (2):

$$X_{Standardized} = \frac{X-\mu}{\sigma} \quad (2)$$

2) Covariance Matrix

The covariance matrix of the standardized data is first calculated in PCA. The connections between various characteristics are captured by the covariance matrix. The covariance between two characteristics is represented by each member of the matrix, which is calculated using the previously stated procedure. A useful tool for understanding how variables are related to one another is the covariance matrix. Compute the standardized data's covariance matrix σ. The following represents the covariance of two characteristics, i and j as expressed in (3):

$$cov(X_i, X_j) = \frac{1}{n-1}\sum_{k=1}^{n}(X_{ki} - \bar{X}_i)(X_{kj} - \bar{X}_j) \qquad (3)$$

Where, the means of features i and j are denoted by $\bar{X}_i$ and $\bar{X}_j$, respectively.

3) Eigendecomposition

The covariance matrix's eigenvalues and eigenvectors must be determined in the next stage. The directions with the greatest variation in the data are represented by eigenvectors, and the amount of variation along each eigenvector is quantified by eigenvalues. The primary components can be found by sorting the eigenvectors according to the associated eigenvalues in descending order. The covariance matrix σ has eigenvalues λ and eigenvectors v. The directions of highest variance are represented by the eigenvectors, and the quantity of variation along those directions is shown by the associated eigenvalues in (4):

$$\sum v = \lambda v \qquad (4)$$

4) Select Principal Components

The top v eigenvectors are chosen in order to minimize dimensionality, creating a new matrix called the projection matrix W. The greatest variation in the data is captured by these eigenvectors. The dimensionality of the reduced feature space is determined by the user-defined parameter k, which is the number of main components. To create the matrix W, arrange the eigenvalues in decreasing order and choose the top k eigenvectors. The primary components are represented by these eigenvectors.

5) Projection

The subspace defined by the chosen main components is where the original data should be projected. Multiplying the original data matrix X by the projection matrix W yields the transformed dataset, which is designated as X_{PCA} in (5):

$$X_{PCA} = X \cdot W \qquad (5)$$

6) Explained Variance

Explained variance is used to evaluate how each primary component contributes to the overall variation. The ratio of the eigenvalue of the i^{th} principal component to the total of all eigenvalues determines the explained variance of the component is expressed in (6):

$$Explained\ Variance\% = \frac{\lambda_j}{\sum_{j=1}^{d}\lambda_j} \times 100 \qquad (6)$$

7) Choosing the Number of Components

Selecting how many of the main components to keep is an important choice. The lowest k that captures a large enough proportion of the overall variation is one such requirement. This guarantees that there won't be a noticeable loss of information as a result of the dimensionality reduction. Based on the intended level of explained variance, ascertain the number of main components k. Selecting k such that a sizable percentage of the total variance is maintained is a frequent method.

PCA is a potent dimensionality reduction method that strikes a compromise between preserving data integrity and cutting down on computing complexity. Because there are so many sensors and characteristics in IoT applications, the datasets frequently have high dimensionality. This makes it very useful. PCA can improve the effectiveness and comprehensibility of later machine learning models used with Internet of Things data.

C. Convolutional Neural Networks for Image-Based Anomaly Detection

CNN's capacity to automatically learn structures of authority and patterns directly from images has shown to be extremely useful in image-based anomaly detection jobs. CNNs are a kind of neural network architecture that use convolutional layers which are capable of capturing local patterns and spatial hierarchies to analyze organized grid input, like pictures. Convolutional layers are used by CNNs to apply tiny filters or kernels to methodically examine input pictures. These filters go across the picture, picking up little details and producing feature maps. In order to learn more complicated patterns in deeper layers, the network must first learn simpler patterns in the early layers thanks to the convolutional process [14]. These acquired patterns may stand in for typical picture textures or structures in the context of image-based anomaly detection. CNNs instantly pick up feature hierarchy representations. Simple elements like corners and edges are captured by lower layers, and more complicated structures are represented by higher layers combining these features. Since anomalies frequently take the form of departures from the anticipated patterns, this hierarchical representation is essential for identifying abnormalities. In encoder-decoder layouts, where the encoder learns a simplified version of the input pictures and the decoder reconstructs the input from this representation, CNNs are frequently employed for anomaly detection.

The reconstruction loss is minimized and the model is exposed to normal data during training. Reconstruction errors tend to be larger in test images that contain anomalies, indicating the presence of anomalies. A prominent technique in CNN-based anomaly identification is transfer learning. CNNs that have already been trained on big picture datasets (like ImageNet) can be adjusted for anomaly detection on the target dataset. This enables the model to take use of the information gathered from a variety of photos and modify it to fit the particular requirements of the anomaly detection task. Frequently, one-class classification problems are used to create image-based anomaly detection, in which the model is trained exclusively on normal data. The model becomes sensitive to deviations suggestive of anomalies throughout testing as it gains the ability to capture the typical variances in the data. CNNs are used in a variety of domains for image-based anomaly detection, including monitoring security camera feeds for anomalous activity or intrusions, detecting defects or anomalies in manufactured products based on images from production lines, and identifying anomalies in medical images, such as X-rays or MRIs, to aid in disease diagnosis. In image-based anomaly detection, CNNs have become highly successful tools, showcasing their ability to extract intricate patterns and representations straight from pictures. With the use of encoder-decoder architectures, convolutional layers, and hierarchical learning, CNNs are highly effective in differentiating abnormal from normal patterns in a wide range of applications. However, to guarantee the resilience and adaptability of the anomaly detection system, close attention to data properties, model architectures, and assessment metrics is necessary.

V. RESULTS AND DISCUSSION

The data pre-processing pipeline involves Min-Max normalization for standardizing position coordinates, enhancing the network's efficiency. Principal Component Analysis (PCA) then reduces high-dimensional IoT data, preserving essential information. Subsequently, Convolutional Neural Networks (CNNs) excel in image-based anomaly detection, automatically learning hierarchical representations. Leveraging encoder-decoder architectures and transfer learning, CNNs demonstrate robust anomaly identification, with minimized reconstruction loss during training and heightened sensitivity to anomalies in test images. The integration of Min-Max normalization, PCA, and CNNs forms a comprehensive framework, enhancing the adaptability and effectiveness of anomaly detection in diverse IoT applications.

A. CNN based Accuracy in Training and Validation

The proposed strategy called for utilising 20% of the data for validation and 80% of the data for training. FIg.s 2 and 3 provide the accuracy level and loss rate fluctuation graphs for the full CNN for image based anomaly detection method. By stabilizing at trained intervals of 100, the precision ratio and loss ratio overall graph, it is clear that the CNN fits data more rapidly.

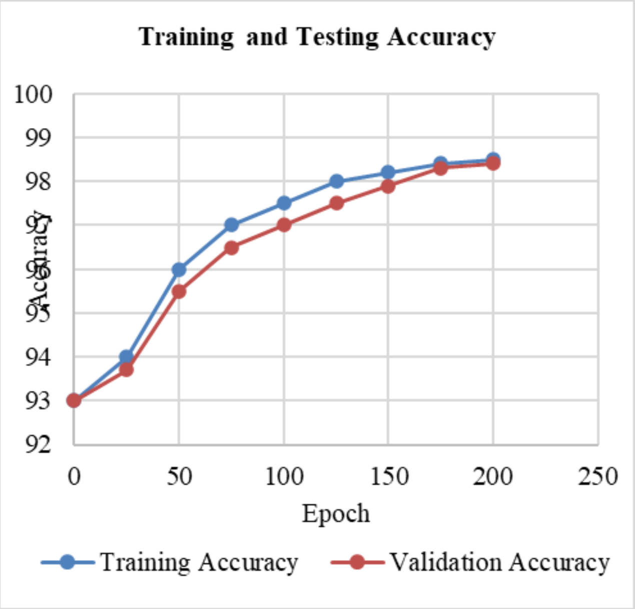

Fig. 2. Training and Testing Accuracy Curve of CNN

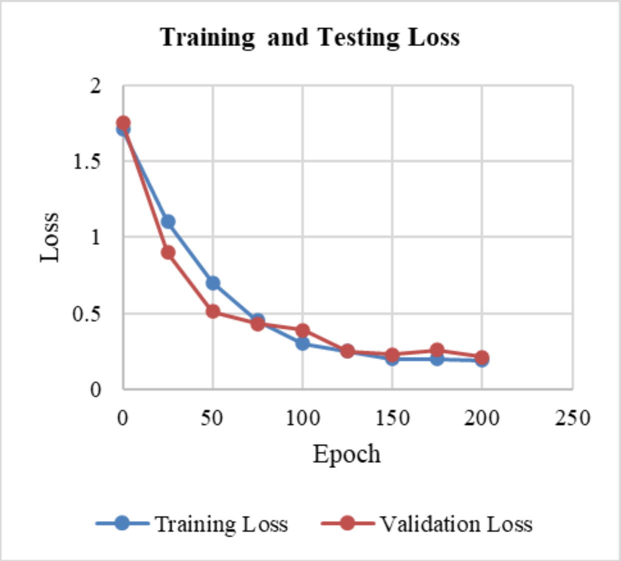

Fig. 3. Training and Testing Loss Curve of CNN

B. Performance Evaluation

For comparison, the following evaluation criteria were used: recall, F1-score, precision and accuracy. These parameters were used to assess the model. These are depicted below:

Accuracy: The prediction accuracy shown in (7) that is most frequently employed to assess classification performances is used to assess the classifier's overall effectiveness.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (7)$$

Precision: The term precision is used to describe how well a group of outcomes agree with one another. Precision is usually defined as the difference between a set of outcomes and the set's arithmetic mean. It is shown in (8).

$$Precision = \frac{TP}{TP+FP} \tag{8}$$

Recall: The purpose of recall analysis shown in (9) is to ascertain, under a certain set of assumptions, how several values of an autonomous variable influence a specific dependent variable. This procedure is applied within prearranged bounds that are dependent on one or more input data variables.

$$Recall = \frac{TP}{TP+FN} \tag{9}$$

Where FP represents false positive pixels, FN signifies false negative pixels, TP symbolizes true positive pixels, and TN describes true negative pixels.

F1-score: In the categorization task, recall and accuracy relate to one another. Although a high value for both is ideal, the reality is generally great accuracy with low recall, or high recall with low accuracy. To account for both recollection and accuracy, the F1-score, which is a mean of recall and accuracy, can be employed. Equation (10) shows the definition of F1-score.

$$F1 - score = 2 * \frac{Pr\ ecision*Recall}{Pr\ ecision+Re\ call} \tag{10}$$

Table I. Performance Metrics of Proposed Method

Proposed CNN for Detection	
Metrics	**Values (%)**
Precision	90.91
Recall	87.9
F1-Score	90.3
ROC	95

Table I proposed Convolutional Neural Network (CNN) for anomaly detection exhibits strong performance, with precision at 90.91%, ensuring accurate identification of anomalies among predicted instances. The recall value of 87.9% underscores the model's effectiveness in capturing a significant proportion of actual anomalies. Furthermore, the high F1-score of 90.3% indicates a balanced trade-off between precision and recall. The Receiver Operating Characteristic (ROC) value of 95% highlights the model's robust discriminatory ability in distinguishing between normal and anomalous instances. Fig. 4 Performance Assessment of Proposed CNN.

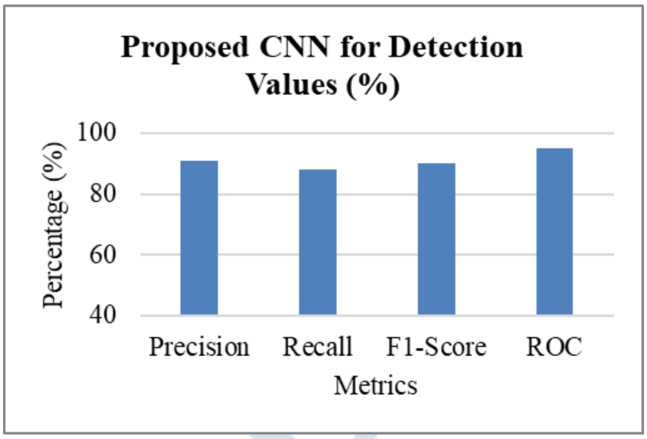

Fig. 4. Performance Assessment of Proposed CNN

Using Eqn. (11), the Area Under the Curve (AUC) has been calculated to estimate overall performance. Fig. 5 shows ROC curve for the Hybrid MLP-CNN TSO model, and it can be seen that the ROC area is nearly close to 1, confirming the model's good stability and potential for usage as classification model for anomaly detection.

$$AUC = \frac{1}{2}\left(\frac{TP}{TP+FN} + \frac{TN}{TN+FP}\right) \tag{11}$$

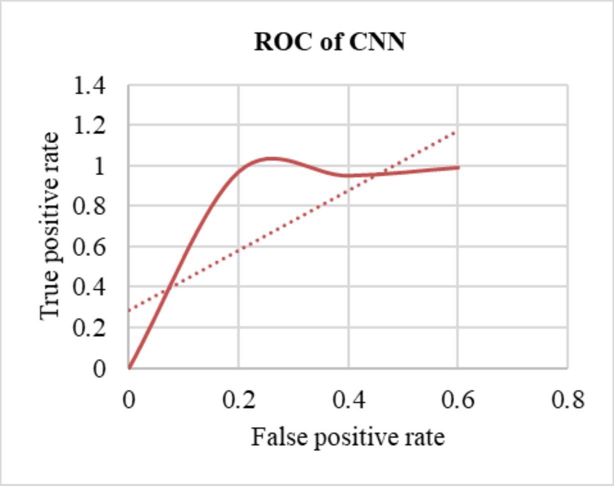

Fig. 5. ROC Curve for CNN

Fig.5 displays the ROC curve for the suggested model. The finding that the dimensions of ROC area are almost one indicates the model's significant degree of stability and its potential for usage as the framework for anomaly detection.

VI. CONCLUSION

The proposed anomaly detection framework, incorporating Min-Max normalization, Principal Component Analysis (PCA), and Convolutional Neural Networks (CNNs), showcases a comprehensive approach for enhancing the accuracy and efficiency of anomaly detection in IoT-enabled systems. The application of Min-Max normalization optimizes data preprocessing, PCA effectively reduces dimensionality while retaining essential information, and CNNs exhibit strong performance metrics, including high precision, recall, and F1-score values. This integrated methodology ensures adaptability and robust anomaly detection across diverse IoT applications, validating its effectiveness in handling complex and high-dimensional datasets. The future scope lies in advancing anomaly detection techniques by exploring novel data preprocessing methods and enhancing CNN architectures for improved adaptability to evolving IoT scenarios. Additionally, incorporating reinforcement learning and ensemble approaches could further elevate the accuracy and resilience of anomaly detection systems in dynamic and complex environments.

REFERENCES

[1] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, "Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," Int. J. Commun. Syst., vol. 33, no. 12, p. e4443, 2020.

[2] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, 2014.

[3] M. Mohsin, Z. Anwar, F. Zaman, and E. Al-Shaer, "IoTChecker: A data-driven framework for security analytics of Internet of Things configurations," Comput. Secur., vol. 70, pp. 199–223, 2017.

[4] D. Settembre-Blundo, R. González-Sánchez, S. Medina-Salgado, and F. E. García-Muiña, "Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times," Glob. J. Flex. Syst. Manag., vol. 22, no. Suppl 2, pp. 107–132, 2021.

[5] S. Ahmad and S. Purdy, "Real-time anomaly detection for streaming analytics," ArXiv Prepr. ArXiv160702480, 2016.

[6] K. Ring Burbeck, "Adaptive real-time anomaly detection for safeguarding critical networks," PhD Thesis, Institutionen för datavetenskap, 2006.

[7] P. P. Ray, "A survey on Internet of Things architectures," J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[8] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, p. e9324035, Jan. 2017, doi: 10.1155/2017/9324035.

[9] S.-Y. Lee, R. B. Chinnam, E. Dalkiran, S. Krupp, and M. Nauss, "Prediction of emergency department patient disposition decision for proactive resource allocation for admission," Health Care Manag. Sci., vol. 23, no. 3, pp. 339–359, Sep. 2020, doi: 10.1007/s10729-019-09496-y.

[10] K. N. Keya, R. Islam, S. Pan, I. Stockwell, and J. Foulds, "Equitable allocation of healthcare resources with fair survival models," in Proceedings of the 2021 siam international conference on data mining (sdm), SIAM, 2021, pp. 190–198.

[11] S. Wang and X. Zhu, "Predictive Modeling of Hospital Readmission: Challenges and Solutions." arXiv, Jun. 15, 2021. Accessed: Dec. 29, 2023. [Online]. Available: http://arxiv.org/abs/2106.08488

[12] H. Henderi, T. Wahyuningsih, and E. Rahwanto, "Comparison of Min-Max normalization and Z-Score Normalization in the K-nearest neighbor (kNN) Algorithm to Test the Accuracy of Types of Breast Cancer," Int. J. Inform. Inf. Syst., vol. 4, no. 1, pp. 13–20, 2021.

[13] G. T. Reddy et al., "Analysis of dimensionality reduction techniques on big data," Ieee Access, vol. 8, pp. 54776–54788, 2020.

[14] S. Xu, H. Wu, and R. Bie, "CXNet-m1: Anomaly detection on chest X-rays with image-based deep learning," IEEE Access, vol. 7, pp. 4466–4477, 2018.