Improving the accuracy of Anomaly Detection in Multimodal Sensors using 1D-CNN

Muhammad Imad*
School of Computing, Ulster University, Belfast, U.K
imad-m@ulster.ac.uk

Ian Cleland
School of Computing, Ulster University, Belfast, U.K
i.cleland@ulster.ac.uk

Patrick McAllister
School of Computing, Ulster University, Belfast, U.K
p.mcallister@ulster.ac.uk

Chris Nugent
School of Computing, Ulster University, Belfast, U.K
cd.nugent@ulster.ac.uk

ABSTRACT

Unusual sensor data within intelligent built-up environments can indicate a range of concerns, including sensor inaccuracies, susceptibility to security breaches, and alterations in activity and behavioural patterns. This study aims to assess the effectiveness of 1D-CNN in detecting and improving the accuracy of anomalies in multimodal sensor data. This method effectively captures temporal patterns in lengthy data sequences collected over extended periods of time. Through comprehensive experiments utilising a public dataset for smart homes, we have empirically verified, after balancing the dataset, the proposed technique's efficacy, and a high accuracy of 0.96 in predicting anomalies.

KEYWORDS

Anomaly Detection, Deep Learning, Multimodal Sensor Data, HAR

ACM Reference Format:
Muhammad Imad, Ian Cleland, Patrick McAllister, and Chris Nugent. 2024. Improving the accuracy of Anomaly Detection in Multimodal Sensors using 1D-CNN. In *The PErvasive Technologies Related to Assistive Environments (PETRA) conference (PETRA '24), June 26–28, 2024, Crete, Greece*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3652037.3652052

1 INTRODUCTION

Identifying anomalies is a significant challenge in the contemporary landscape of data-driven environments. The process requires identifying patterns and occurrences within data that reveal substantial deviations from conventional behaviour. Anomalies, alternatively referred to as outliers, are data points that deviate from the expected patterns and distributions observed in most of the dataset. The significance of anomaly detection is considerable across various domains, such as cybersecurity and network analysis [1]. Anomaly detection algorithms are utilised by financial institutions, credit card companies, and e-commerce platforms to discern atypical patterns in transactions and account activities. By effectively identifying and promptly responding to instances of fraudulent transactions or activities, these systems can mitigate financial losses and safeguard customers' interests [2]. The significance of anomaly detection in Human Activity Recognition (HAR) and smart home environments is to identify deviations from normal behaviour. This enables early detection of potential emergencies or abnormal situations, facilitating swift responses to ensure the safety and well-being of occupants by leveraging the power of smart technology. Despite its critical importance, this area often remains under-explored, presenting a rich avenue for innovative research and application. The exponential increase in data complexity and volume across various domains has emerged as a significant driving force behind the demand for efficient anomaly detection methods. The continuous generation of vast amounts of data has become increasingly established with the emergence of the Internet of Things (IoT) and the widespread connectivity of various devices. The utilisation of traditional rule-based systems and manual analysis becomes unfeasible when confronted with extensive and heterogeneous datasets [3].

Machine learning algorithms that are designed to detect anomalies show the potential to provide a possible solution to tackle this particular challenge [7]. Through sophisticated algorithms, these methodologies can autonomously acquire knowledge of patterns and detect deviations in real time, thereby facilitating effective consideration and decision-making in complex and multi-dimensional datasets [8]. Anomaly detection techniques can be broadly classified into supervised, unsupervised, and semi-supervised approaches. In supervised anomaly detection, labelled data is used to identify and label anomalies. The algorithm is trained on this labelled data to learn the distinguishing features between anomalies and normal instances. During the evaluation phase, the algorithm applies its learned patterns to predict the anomalous nature of new instances. Supervised methods are effective when labelled data is readily available, however, they face challenges when dealing with limited and insufficient knowledge about anomalies during the training phase [9].

In contrast, unsupervised anomaly detection methods do not require the availability of labelled data [10]. These techniques rely on identifying inherent patterns and structures within the data. Their objective is to capture the intrinsic characteristics of typical data points and detect instances that deviate significantly from those characteristics. Unsupervised methods offer distinct advantages in scenarios where anomalies are rare and unfamiliar, as they can detect and classify previously unseen anomalies that were not encountered during training. Nevertheless, dealing with datasets presenting considerable fluctuations and intricate patterns can pose

*Corresponding Author

PETRA '24, June 26–28, 2024, Crete, Greece

ACM ISBN 979-8-4007-1760-4/24/06
https://doi.org/10.1145/3652037.3652052

challenges. Multimodal sensor data includes the data obtained from different sensor modalities, including but not limited to temperature sensors, pressure sensors, motion sensors, cameras, and microphones [4]. The main objective of anomaly detection in multimodal sensor data is to distinguish between common patterns and behaviours and atypical patterns that deviate from the anticipated behaviour [5]. Analysing aggregated data from multiple sensors enables the identification of anomalies that may not be readily visible when observing the data from each sensor. The concept of anomaly detection relies heavily on the understanding of normality. Normality refers to the expected behaviour and patterns observed in most data points within a given dataset. It is usually assumed that data points adhere to specific statistical distributions and present distinct patterns. On the other hand, anomalies deviate significantly from the expected patterns [6]. These anomalies can manifest in various forms, including extreme values, unexpected clusters, and sequences that diverge from established patterns.

On the other hand, semi-supervised anomaly detection is a hybrid approach that combines both supervised and unsupervised methods. This approach leverages a limited amount of labelled data and a larger set of unlabelled data. Using labelled data helps in acquiring knowledge about the distinguishing features of anomalies and normal instances. In contrast, the integration of unlabelled data assists in capturing the overall properties of the normal data. Semi-supervised approaches bridge the benefits of supervised and unsupervised methods, improving detection accuracy where labelled data availability is limited [11].

This paper explores the 1D-CNN technique for anomaly detection on the SIMADL dataset [12], particularly addressing the challenges of imbalanced datasets. The main contributions of this study are outlined below:

1. Efficient data preprocessing and feature engineering strategies were tailored for 1D CNN, which were pivotal for optimizing model performance before and after balancing the dataset.
2. The Synthetic Minority Over-Sampling Technique (SMOTE) was applied to address class imbalance, a common challenge in anomaly detection tasks, ensuring a more balanced and representative dataset for model training.
3. The parameters of the 1D-CNN were fine-tuned to enhance the accuracy of the high-dimensionality SIMADL dataset, reduce the false positive rate, and enhance recall.
4. A 1D-CNN model was designed, and its validation was conducted through Stratified k-fold cross-validation, demonstrating the model's consistency and reliability across the balanced dataset.

The remaining sections of the paper are organised as follows. The Literature Review section provides an overview of related work focusing on anomaly detection. The Methodology section presents the dataset description and the proposed framework for anomaly detection. In the Experimental Result section, the results from the experiments are showcased, and the discussion follows highlighting the implications of these results along with conclusions and future work.

2 LITERATURE REVIEW

Anomaly detection in high-dimensional data has developed as a critical research field with numerous real-world applications [13]. Agrawal [14] presented a detailed analysis of numerous anomaly detection strategies to provide a fundamental understanding of the various approaches used in anomaly detection. Chandola et al. [2] reviewed anomaly detection strategies used in various applications. Similarly, Hodge and Austin [15] conducted a survey that evaluated outlier detection strategies, highlighting their benefits and drawbacks. Patcha and Park [16] provided another significant addition by providing a comprehensive assessment of anomaly detection systems and hybrid intrusion detection systems, emphasising identifying open difficulties and unresolved concerns. Furthermore, Jakkula et al. [20] used data mining techniques to discover anomalies in smart home data. Angipuram et al. [21] used multiple machine-learning algorithms to detect anomalies in IoT devices. The DS2OS dataset was used which consists of various sensors, including light controls, thermometers, movement sensors, and smartphones. The Naive Bayes, BayesNet, ZeroR, J48, Random Forest, Decision Tree, DTNB, and Multilayer perceptron were used on test data. The performance of these approaches were assessed in terms of detecting malicious control, malicious operation, and Denial-of-Service (DoS) attacks [18].

Using statistical methodologies has efficiently identified and revealed atypical patterns within diverse fields. These methods have effectively identified deviations from anticipated patterns and detected anomalies in datasets from various application domains. Using statistical techniques and measures provides valuable insights into the atypical behaviours that occur in various domains. A dissimilarity-based approach has been created in the field of statistical methods [17, 22]. This concept uses an index to assess the degree of resemblance between normal and aberrant behaviour. Experiments were carried out on two distinct datasets with single residents at home. Dissimilarity measurements in the literature include Hamming distance, Manhattan distance, and cosine similarity. The selection of distance measures is critical and should be dependent on the data's qualities. Sensors in intelligent environments frequently communicate binary data on objects in functional or rest states. An effective distance metric for such binary data can be chosen from a list of 76 distances provided in [19, 23].

Several researchers have used deep learning techniques to identify unusual activities in video sequences. Notably, the work referenced in [24] implemented deep autoencoders to model normal patterns and applied reconstruction loss as a means for anomaly detection. Additionally, Luo et al. [25] proposed a method focusing on the temporal consistency of anomalies, leveraging sparse coding and the computational capabilities of a stacked RNN for enhanced detection. Luo et al. [26] utilized a CNN and a Convolutional Long Short-Term Memory (ConvLSTM) network to detect anomalies, focusing on the retention of motion features from all preceding frames. This approach was further enhanced by integrating an autoencoder with ConvLSTM to effectively capture the motion and appearance characteristics of objects in various scenarios. In a different technique, Huo et al. [27] developed an approach for detecting unusual events in video footage, employing multi-instance dictionary learning. This method proves particularly effective in contexts where it's

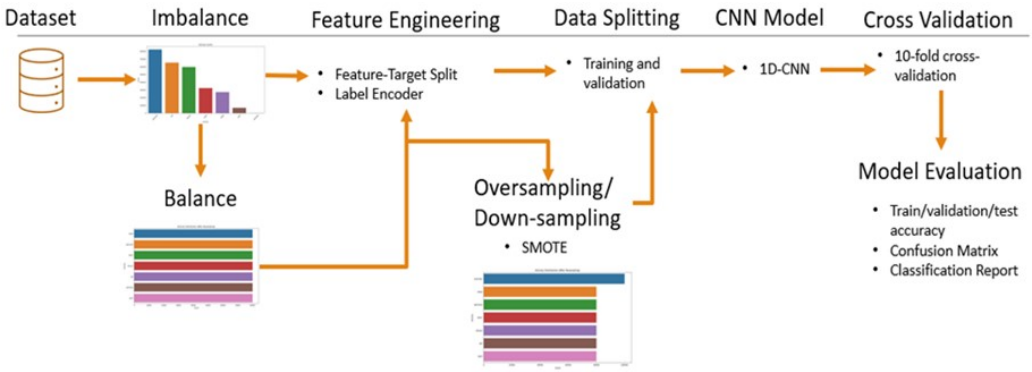

Figure 1: Depicts the proposed methodology framework highlighting the main steps in data balancing, feature extraction, model training and validation.

feasible to obtain labels for a collection of sub-events, even when the labels for individual sub-events remain ambiguous.

DeMedeiros [28] provides a comprehensive review of anomalies with a specific emphasis on the detection of anomalies in the IoT and sensor networks. The survey aims to elucidate the current approaches and methods employed for anomaly detection in these domains. In addition, this paper aims to identify gaps in existing research and delineate areas that necessitate further exploration within the domain of anomaly detection IoT and sensor networks.

As from the above literature studies, there is a lack of research in the field of activity recognition relating to the identification of anomalies in the activity data, improving the accuracy in high-dimensional data, reducing false positives and enhancing recall rate. While numerous studies have focused on recognizing and classifying activities, there has been limited investigation into effectively detecting and characterizing anomalous activities [31].

3 METHODOLOGY

Figure 1 illustrates the sequential workflow of the proposed methodology for detecting anomalies in the SIMADL dataset through the integration of deep learning techniques. This section provides a comprehensive analysis of the SIMADL dataset and thoroughly considers deep learning techniques.

3.1 General Description of SIMADL Dataset

The present study utilises the SIMADL dataset [12], as introduced by Open-SHS, an openly available simulation program. This tool was chosen due to its capacity to create data pertaining to the activities of daily living (ADLs) of individuals, which is crucial for the classification process. The Open-SHS framework was employed to produce multiple synthetic datasets comprising 29 columns of binary data, whereby each binary sensor exhibits two distinct states: on (1) and off (0). The sensors can be categorised into two different classes: passive and active. Passive sensors exhibit a response without requiring explicit interaction from the participants. In contrast, their responses are contingent upon the movements and placements of the participants. The participants employed the following labels: Personal, Sleep, Eat, Leisure, Work, Other, and Anomaly. Using a stratified approach, the dataset is strategically split into training/validation and testing subsets. The list of all activities with specific frequencies is presented in Figure 2, while Table 1 presented all recorded sensors mentioned in the SIMADL dataset.

3.2 Feature Engineering

The target variable undergoes label encoding, transforming categorical labels into a numerical format essential for deep learning. Finally, the feature set is reshaped to fit the requirements of a 1D CNN, adjusting its dimensions to ensure compatibility with the neural network architecture.

3.2.1 SMOTE. Figure 2 illustrates a pronounced disparity among recorded activities, with 'personal' activities being the most prevalent at over 800,000 instances. In comparison, categories such as 'eating' and 'leisure' shows large frequencies of data, but sleep, work and anomaly show smaller frequencies of daily activities. The disparity in the number of instances across activities suggests that resampling techniques need to balance the dataset before it is used for predictive modelling. SMOTE is an algorithm that aims to balance class distribution in a dataset. It does so by creating synthetic instances of the minority class, thereby avoiding the overfitting that can occur when simply duplicating minority class instances and improving the performance of the model by providing a more balanced representation of classes [29, 30].

A systematic approach is used to address class imbalance in a machine learning dataset, employing both oversampling and down-sampling techniques to ensure a more equitable representation of all classes. This preprocessing step is vital in preparing the data for subsequent analysis and modelling, ensuring that the models developed are both accurate and unbiased. Figure 3 presents the preprocessing from imbalance to balance the data.

3.3 1D Convolutional Neural Network (1D-CNN)

In Figure 4, the model is a sequential approach, integrating layers specifically suited for 1D data analysis. The convolutional layers

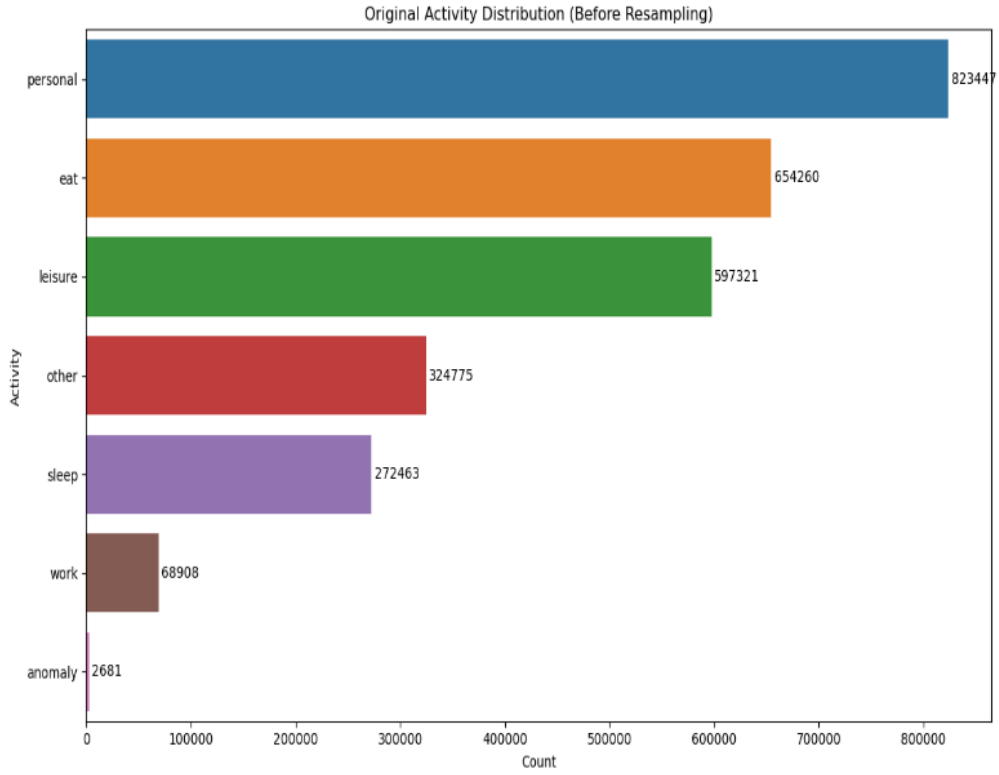

Figure 2: Count of the number of instances per class.

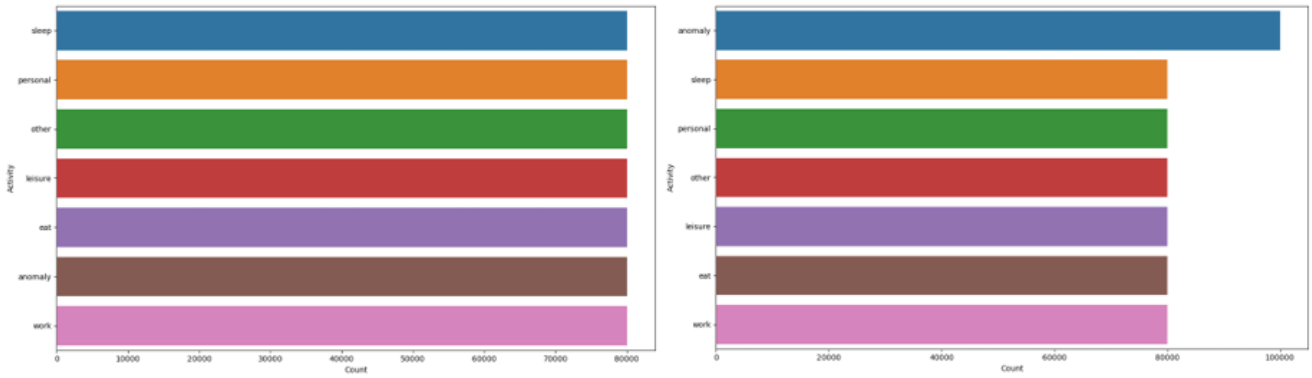

Figure 3: (a). Balance data after sampling, (b). Oversampling of the anomaly activities.

acquire spatial hierarchy in data through filters, followed by max-pooling layers for dimensionality reduction and feature emphasis. The network then flattens the output for dense layers, which are fully connected layers. The model incorporates two 1D convolutional layers, each designed to extract spatial hierarchies of features from the input data. The first layer consists of 64 filters, and the second comprises 128 filters, both using a kernel size of 3. The 'relu' activation function is employed in these layers for introducing non-linearity, enabling the model to learn more complex patterns in the data. Following each convolutional layer is a max pooling layer with a pool size of 2. These layers serve to reduce the dimensionality of the data, which helps in reducing the computational load and the risk of overfitting. They achieve this by retaining only the most significant information from the feature maps generated by the convolutional layers. The model includes a flattened layer that transforms the 2D feature maps into a 1D vector. This vector is then fed into dense (fully connected) layers. The first dense layer has 128 units, also with 'relu' activation, further processing the features. The final dense layer's units correspond to the number of classes in the classification task and utilize a 'SoftMax' activation

Table 1: List of sensors recorded in the SIMADL dataset [12].

#	Name	Type	Description	Active/Passive
1.	BathroomCarp	binary	Bathroom carpet sensor	Passive
2.	BathroomDoor	binary	Bathroom door sensor	Active
3.	BathroomDoorLock	binary	Bathroom door lock sensor	Active
4.	BathroomLight	binary	Bathroom ceiling light	Passive
5.	Bed	binary	Bed contact sensor	Active
6.	BedTableLamp	binary	Bedroom table lamp	Active
7.	BedroomCarp	binary	Bedroom carpet sensor	Passive
8.	BedroomDoor	binary	Bedroom door sensor	Active
9.	BedroomDoorLock	binary	Bedroom door lock sensor	Active
10.	BedroomLight	binary	Bedroom ceiling light	Passive
11.	Couch	binary	Living room couch	Active
12.	Fridge	binary	Kitchen fridge	Active
13.	HallwayLight	binary	Hallway ceiling light	Passive
14.	KitchenCarp	binary	Kitchen door sensor	Active
15.	KitchenDoor	binary	Kitchen door sensor	Active
16.	LivingDoorLock	binary	Kitchen door lock sensor	Active
17.	LivingCarp	binary	Living room carpet sensor	Passive
18.	LivingLight	binary	Living room ceiling light	Active
19.	KitchenLight	binary	Kitchen ceiling light	Active
20.	MainDoor	binary	Main door sensor	Active
21.	MainDoorLock	binary	Main door lock sensor	Active
22.	Office	binary	Office room desk sensor	Passive
23.	OfficeCarp	binary	Office room carpet sensor	Passive
24.	OfficeDoor	binary	Office door sensor	Active
25.	OfficeDoorLock	binary	Office door lock sensor	Active
26.	OfficeLight	binary	Office ceiling light	Active
27.	Oven	binary	Kitchen oven sensor	Active
28.	TV	binary	Living room TV sensor	Active
29.	Wardrobe	binary	Bedroom wardrobe sensor	Active
30.	Activity	String	Participant activity	
31.	Timestamp	String	Timestamp every second	

function, which is typical for multi-class classification problems. This layer outputs the probability distribution over the classes. The model is compiled using the Adam optimiser, a popular choice due to its effectiveness in handling sparse gradients and adapting the learning rate during training. The loss function used is 'sparse_categorical_crossentropy,' appropriate for multi-class classification tasks where the target classes are encoded as integers. The model's performance is evaluated based on classification and confusion matrix report.

4 EXPERIMENTAL RESULT

The experimental results involving imbalance and balance results and using deep learning technique, performance evaluation metrics, and comparing the result with previous work were highlighted.

4.1 Imbalanced Result using 1D-CNN

Figure 5 represents the performance of a model using a 10-fold cross-validation approach over a series of epochs during training. Each 'fold' represents a partition of the dataset where the model is trained on 9 parts and validated on the 10th, rotating until each part has been used for validation.

The confusion matrix visualises the performance of a classification model that predicts seven types of activities, as mentioned in Figure 6. labelled from 0 to 6. These activities include 'anomaly' (0), 'eat' (1), 'leisure' (2), 'other' (3), 'personal' (4), 'sleep' (5), and 'work' (6). The model's predictive performance is affected by class imbalances in the dataset. Such imbalances are evident in the disproportionate misclassification rates. For example, 'anomaly' (0) is frequently misclassified as 'personal' (4) and 'eat' (1), which could be due to a relatively small number of 'anomaly' samples compared to the other classes, leading the model to be less accurate in distinguishing this category. Similarly, a substantial number of 'eat' (1) instances are incorrectly predicted as 'personal' (4) and 'leisure' (2), suggesting that the model may be biased towards the more represented classes. The high misclassification between 'personal' (4) and 'sleep' (5), as well as 'work' (6) being mistaken for 'sleep' (5), could also be manifestations of such imbalance. These frequent errors between specific classes imply that the model struggles to differentiate between underrepresented activities in the dataset and

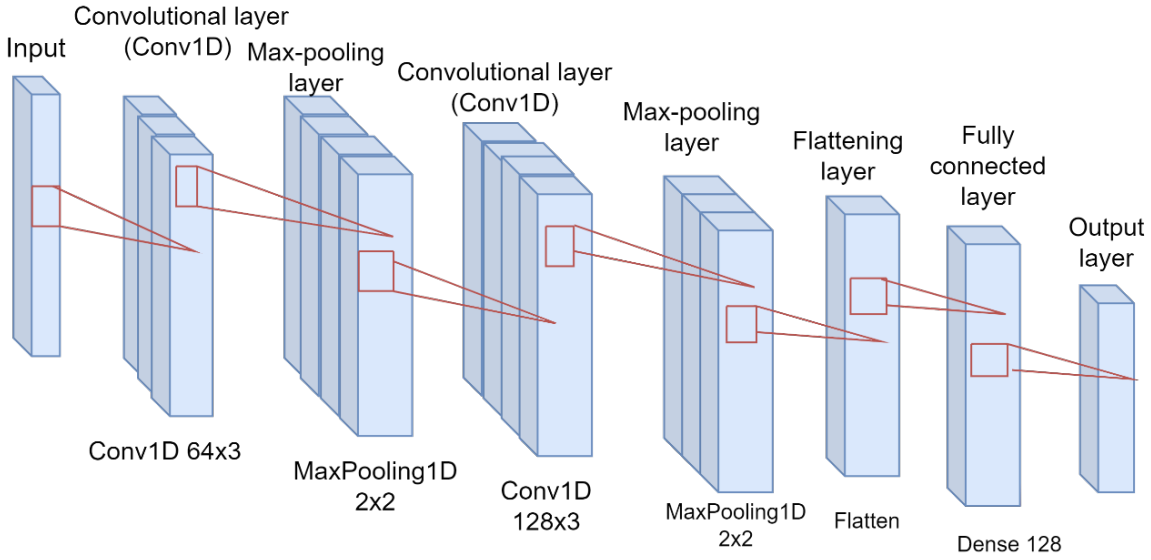

Figure 4: Proposed CNN model architecture.

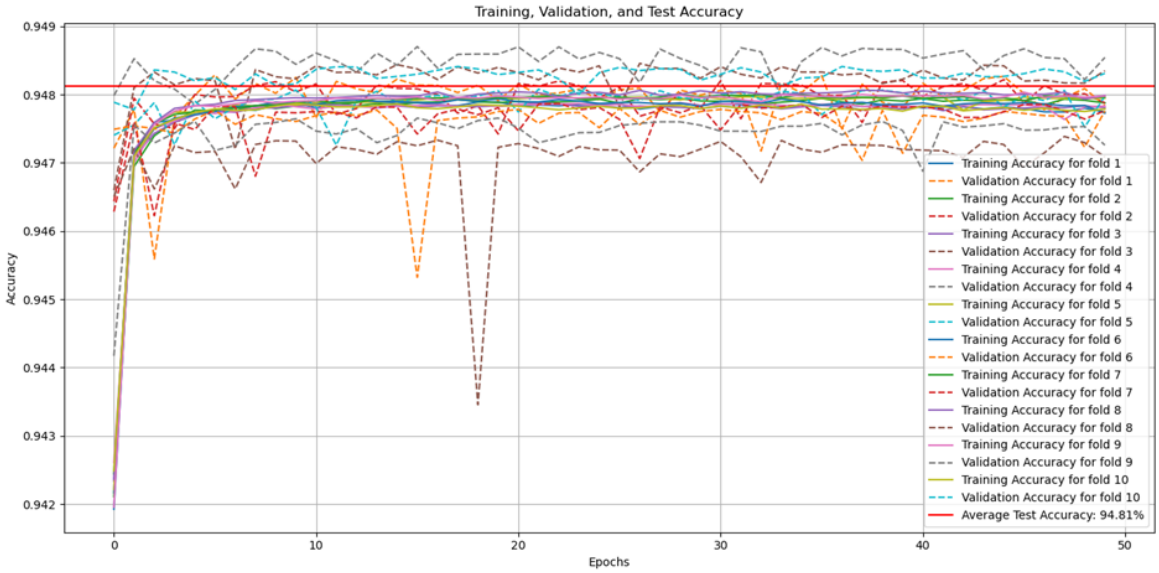

Figure 5: Training, validation, and test accuracy of imbalanced data.

more prevalent ones. This challenge is further compounded by the inherent similarities in features between certain activities, such as the low levels of motion in both 'personal' and 'sleep' activities. Adjusting the model to account for these imbalances through resampling techniques or class-weight adjustments could enhance its classification accuracy and reduce the misclassification rate.

The classification report in Table 2 delineates the performance metrics of a 1D-CNN evaluated through a rigorous 10-fold cross-validation mentioned in Table 2. This procedure enhances the robustness of the model assessment by ensuring comprehensive exposure to the dataset. Nevertheless, the recall for class '0', which corresponds to 'anomaly,' is markedly lower at 0.39 and F1-Score is 0.56, compared to the other classes, which maintain a recall and F1-Score is above 0.92. This suggests that while the model's predictions for 'anomaly' are accurate when they are made, it fails to identify a substantial number of true 'anomaly' instances, indicative of a high false negative rate for this class. Overall, the model exhibits a commendable accuracy of 0.95, indicating that most of

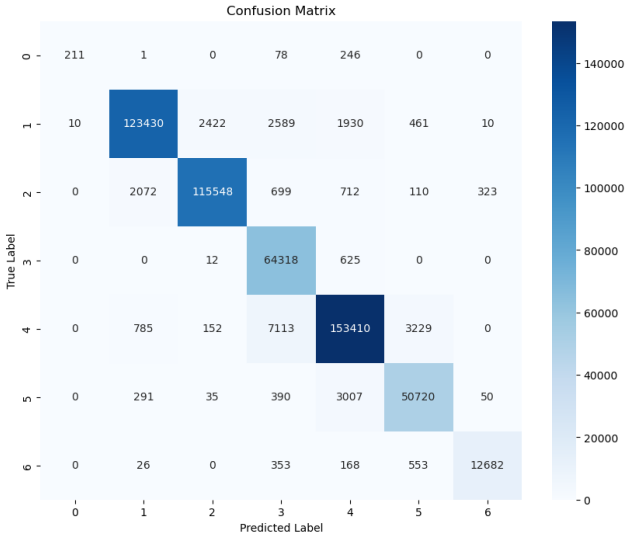

Figure 6: Confusion Matrix of imbalanced data. Note the poor performance in classifying the minority class of anomaly, 0-6 represents the different activities such as 'anomaly' (0), 'eat' (1), 'leisure' (2), 'other' (3), 'personal' (4), 'sleep' (5), and 'work' (6).

the predictions align with the true class labels. The class imbalance, particularly the underrepresentation of 'anomaly,' has a pronounced impact on the recall for this class. The precision, recall, and F1-Score for each activity are mentioned in Table 2.

4.2 Balanced result using 1D-CNN

Figure 7 presents the outcomes of a 1D-CNN evaluation using a 10-fold cross-validation method. Cross-validation is a statistical approach used to gauge the predictive performance of a model and to mitigate overfitting. In this instance, the graph shows ten pairs of lines, each representing a separate fold in the validation process. The x-axis quantifies the epochs—complete iterations over the training dataset—while the y-axis quantifies the accuracy, reflecting the ratio of correct predictions made by the model.

For each fold, there are two distinct lines: one signifies the training accuracy, and the other represents the validation accuracy. The consistency in the pattern of these lines across all folds indicates the stability of the model's predictive capability. Additionally, the proximity of the validation accuracy to the training accuracy suggests that the model generalises well to unseen data.

The graph also includes a horizontal line indicating the test accuracy, which is reported to be 0.95. This metric is derived post the cross-validation method, where the model is subjected to a separate test dataset to assess its predictive power. The uniformity in the model's performance across different folds and the high-test accuracy rate are indicative of the model's robustness and its potential to perform reliably on external data.

The confusion matrix presented the accuracy of a predictive model in classifying various activities as shown in Figure 8, labelled from 0 to 6, each corresponding to a unique activity: 'anomaly' (0), 'eat' (1), 'leisure' (2), 'other' (3), 'personal' (4), 'sleep' (5), and 'work' (6). The matrix is structured such that the true activity labels (True Labels) are arranged along the vertical axis, and the predicted labels (Predicted Labels) by the model are laid out along the horizontal axis. Each cell within the matrix represents the instances in which the model predicted a particular activity versus the true activity. The activities 'personal' (4), 'sleep' (5), and 'work' (6) show substantial correct predictions, as denoted by the darker cells on the diagonal, thus signifying a higher prediction accuracy for these activities.

The classification report under consideration gives a detailed evaluation of a multiclass classifier, with each class representing a specific activity, represented numerically as 'anomaly' (0), 'eat' (1), 'leisure' (2), 'other' (3), 'personal' (4), 'sleep' (5), and 'work' (6). The precision measure across these classes indicates that the model's predictions have a high level of specificity, with values such as 0.98 for both 'anomaly' and 'eat' meaning that 0.98 of the cases classified as these classes are correct. The recall metric indicates the model's sensitivity, with the 'anomaly' class having a 1.00 recall, meaning that the model effectively captured all actual instances of 'anomaly'.

In Table 3, The accuracy of 0.96 in the aggregated metrics reveals that the model accurately predicted 0.96 of all classes. The macro average, which treats all classes equally, has an accuracy, recall, and f1-score of 0.95, indicating uniform performance across classes regardless of their frequency in the dataset. The weighted average, which considers class imbalance by weighting each class's contribution to the average by its support, similarly returns a constant score of 0.96 across all three categories. This implies that the classifier

Table 2: 1D-CNN Classification report of imbalanced data.

Labels	Precision	Recall	F1-Score	No. of Samples
0 (anomaly)	0.95	0.39	0.56	536
1 (eat)	0.97	0.94	0.96	130852
2 (leisure)	0.98	0.97	0.97	119464
3 (other)	0.85	0.99	0.92	64955
4 (personal)	0.96	0.93	0.94	164689
5 (sleep)	0.92	0.93	0.93	54493
6 (work)	0.97	0.92	0.94	13782
Accuracy			0.95	548771
Macro avg	0.94	0.87	0.89	548771
Weighted avg	0.95	0.95	0.95	548771

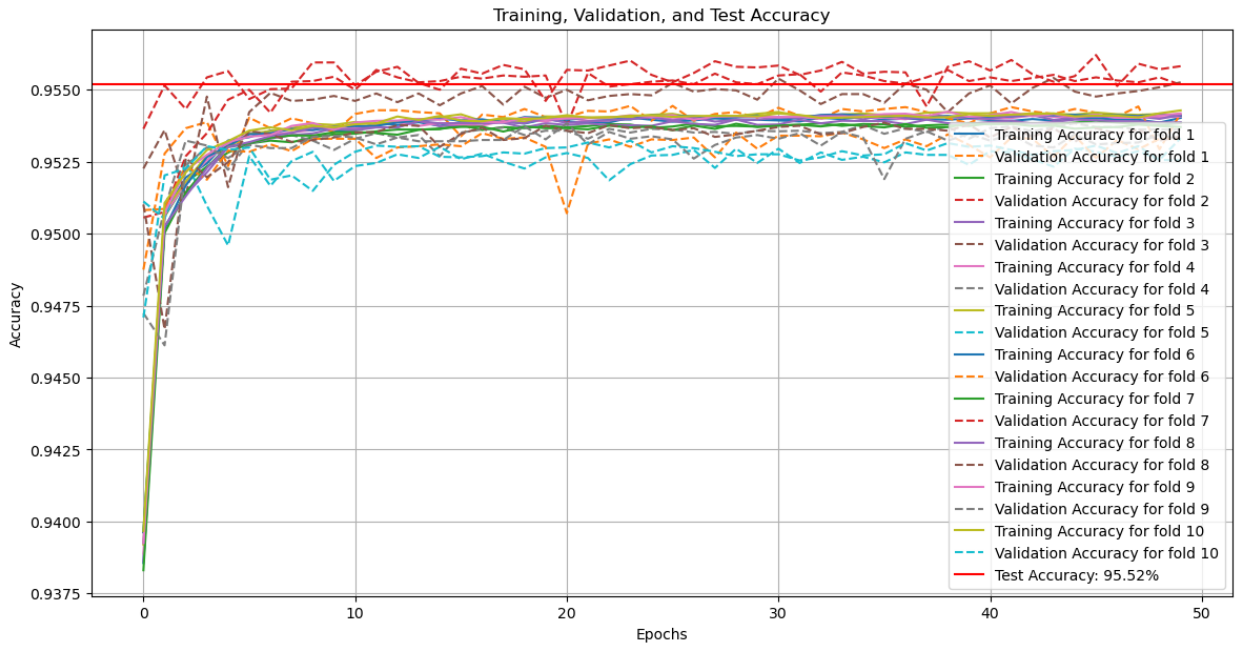

Figure 7: Training, validation, and test accuracy of balanced data.

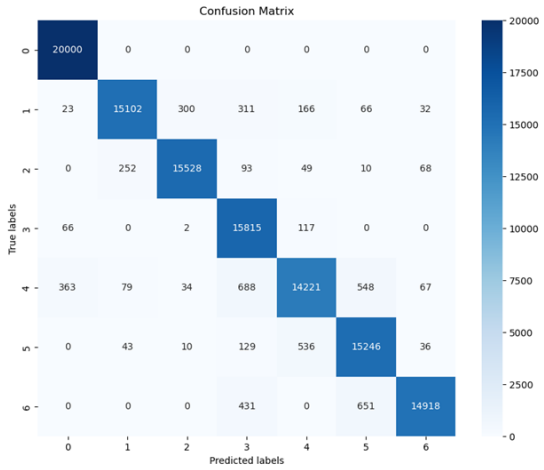

Figure 8: Confusion Matrix of balanced data. Note the performance in classifying the majority class of anomaly, 0-6 represent the different activities such as 'anomaly' (0), 'eat' (1), 'leisure' (2), 'other' (3), 'personal' (4), 'sleep' (5), and 'work' (6).

performs effectively even when adjusted for class size variation. Such findings highlight the classifier's effectiveness over a wide range of activity classifications within the given dataset.

4.3 Performance comparison of balance and imbalance results

The model reduced the false positive and enhanced recall rate achieved the highest accuracy of 0.96 and performed well in terms of Precision, Recall, and F1 score as compared with the imbalance result, as mentioned in Table 4.

4.4 Performance comparison with previous work

Zerkouk et al. [30] used LSTM, SVM, NB, KNN, and NN techniques for the SIMADL dataset for abnormal behaviour detection and showed that the LSTM +SMOTE achieved the best precision of 0.91, recall of 0.91, and f-score of 0.91 as compared to ML techniques. Our model achieved the highest accuracy of 0.96 and performed well in terms of Precision, Recall, and F1 score as mentioned in Table 5.

5 CONCLUSION

This research aims to detect anomalies in multimodal sensor data in smart homes. We effectively tackled the difficulty of improving the accuracy of anomaly detection by following the preprocessing, feature engineering, and then using the 1D-CNN approach. The model achieved a high accuracy of 0.96 after balancing the SIMADL dataset and oversampling the anomaly activity. The study's findings, demonstrating a robust accuracy of 0.96 and balanced class performance, are particularly impactful in the smart home domain, where precise activity recognition can revolutionise home automation, enhance security systems, and provide tailored assistance to residents, especially the elderly or those with disabilities. In the future, we aim to expand on this study by exploring multiple deep-learning algorithms for anomaly identification in smart homes which can potentially improve detection capabilities by collecting complex patterns and temporal relationships in sensor data.

Table 3: 1D-CNN Classification report of balance data.

Labels	Precision	Recall	F1-Score	No. of Samples
0 (anomaly)	0.98	1.00	0.99	20000
1 (eat)	0.98	0.94	0.96	16000
2 (leisure)	0.98	0.97	0.97	16000
3 (other)	0.91	0.99	0.95	16000
4 (personal)	0.94	0.89	0.91	16000
5 (sleep)	0.92	0.95	0.94	16000
6 (work)	0.99	0.93	0.96	16000
Accuracy			0.96	116000
Macro avg	0.96	0.95	0.95	116000
Weighted avg	0.96	0.96	0.96	116000

Table 4: Comparison of balance and imbalance data.

Name	Avg. Precision	Avg. Recall	Avg.F1-Score
Imbalanced result using 1D-CNN	0.94	0.87	0.89
Balanced result using 1D-CNN	0.96	0.95	0.95

Table 5: Comparison with previous work.

Name	Precision	Recall	F1-Score
Zerkouk et al. [30] (SMOTE+LSTM)	0.91	0.91	0.91
Proposed Model (SMOTE+1D-CNN)	0.96	0.95	0.95

ACKNOWLEDGMENTS

This research is supported by the ARC (Advanced Research Engineering Centre) project, funded by PwC[1] and Invest Northern Ireland.

REFERENCES

[1] Yao, D. D., Shu, X., Cheng, L., & Stolfo, S. J. (2018). Anomaly detection as a Service. Synthesis Lectures on Information Security, Privacy, and Trust. doi:10.1007/978-3-031-02354-5

[2] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection. ACM Computing Surveys, 41(3), 1–58. doi:10.1145/1541880.1541882

[3] Guo, Y., Ji, T., Wang, Q., Yu, L., Min, G., & Li, P. (2020). Unsupervised anomaly detection in IOT systems for Smart Cities. IEEE Transactions on Network Science and Engineering, 7(4), 2231–2242. doi:10.1109/tnse.2020.3027543

[4] Ehatisham-Ul-Haq, M., Javed, A., Azam, M. A., Malik, H. M., Irtaza, A., Lee, I. H., & Mahmood, M. T. (2019). Robust human activity recognition using multimodal feature-level fusion. IEEE Access, 7, 60736–60751. doi:10.1109/access.2019.2913393

[5] Cook, A. A., Misirli, G., & Fan, Z. (2020). Anomaly detection for IOT time-series data: A survey. IEEE Internet of Things Journal, 7(7), 6481–6494. doi:10.1109/jiot.2019.2958185

[6] Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of Network Anomaly Detection Techniques. Journal of Network and Computer Applications, 60, 19–31. doi:10.1016/j.jnca.2015.11.016

[7] Zoppi, T., Gharib, M., Atif, M., & Bondavalli, A. (2021). Meta-learning to improve unsupervised intrusion detection in cyber-physical systems. ACM Transactions on Cyber-Physical Systems, 5(4), 1–27. doi:10.1145/3467470

[8] Sun, H., He, Q., Liao, K., Sellis, T., Guo, L., Zhang, X., . . . Chen, F. (2019a). Fast anomaly detection in multiple multi-dimensional data streams. 2019 IEEE International Conference on Big Data (Big Data). doi:10.1109/bigdata47090.2019.9006354

[9] Goernitz, N., Kloft, M., Rieck, K., & Brefeld, U. (2013). Toward supervised anomaly detection. Journal of Artificial Intelligence Research, 46, 235–262. doi:10.1613/jair.3623

[10] Munir, M., Siddiqui, S. A., Dengel, A., & Ahmed, S. (2018). DeepAnT: A deep learning approach for unsupervised anomaly detection in time series. Ieee Access, 7, 1991-2005.

[11] Song, X., Wu, M., Jermaine, C., & Ranka, S. (2007). Conditional anomaly detection. IEEE Transactions on Knowledge and Data Engineering, 19(5), 631-645. doi:10.1109/TKDE.2007.1009

[12] Alshammari, T., Alshammari, N., Sedky, M., & Howard, C. (2018). SIMADL: Simulated activities of daily living dataset. Data (Basel), 3(2), 11. doi:10.3390/data3020011

[13] Suboh, S., Aziz, I. A., Shaharudin, S. M., Ismail, S. A., & Mahdin, H. (2023). A systematic review of anomaly detection within high dimensional and multivariate data. JOIV : International Journal on Informatics Visualization Online, 7(1), 122-130. doi:10.30630/joiv.7.1.1297

[14] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques. Procedia Computer Science, 60, 708-713. doi:10.1016/j.procs.2015.08.220

[15] Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. The Artificial Intelligence Review, 22(2), 85-126. doi:10.1023/B:AIRE.0000045502.10941.a9

[16] Patcha, A., & Park, J. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks (Amsterdam, Netherlands : 1999), 51(12), 3448-3470. doi:10.1016/j.comnet.2007.02.001

[17] Meng Jiang, Peng Cui, & Faloutsos, C. (2016). Suspicious behavior detection: Current trends and future directions. IEEE Intelligent Systems, 31(1), 31-39. doi:10.1109/MIS.2016.5

[18] Dahmen, J., & Cook, D. J. (2021). Indirectly supervised anomaly detection of clinically meaningful health events from smart home data. ACM Transactions on Intelligent Systems and Technology, 12(2), 1-18. doi:10.1145/3439870

[19] Dahmen, J., Cook, D. J., Wang, X., & Honglei, W. (2017). Smart secure homes: A survey of smart home technologies that sense, assess, and respond to security threats. Journal of Reliable Intelligent Environments, 3(2), 83-98. doi:10.1007/s40860-017-0035-0

[20] V. Jakkula, D. J. Cook D. J. Cook. (2008). Anomaly Detection Using Temporal Data Mining in a Smart Home Environment. Methods of information in medicine, 47(1), 70-75. doi:10.3414/ME9103

[21] Vangipuram, R., Gunupudi, R. K., Puligadda, V. K., & Vinjamuri, J. (2020). A machine learning approach for imputation and anomaly detection in IoT environment. Expert Systems, 37(5), n/a. doi:10.1111/exsy.12556
[22] Mahmoud, S., Lotfi, A., & Langensiepen, C. (May 25, 2011). Abnormal behaviours identification for an elder's life activities using dissimilarity measurements. Paper presented at the 1-5. doi:10.1145/2141622.2141653
[23] Muniswamaiah, M., Agerwala, T., & Tappert, C. (2023). Applications of binary similarity and distance measures. (). Ithaca: Cornell University Library, arXiv.org. doi:10.48550/arxiv.2307.00411
[24] Bin Zhao, Li Fei-Fei, & Xing, E. P. (Jun 2011). Online detection of unusual events in videos via dynamic sparse coding. Paper presented at the 3313-3320. doi:10.1109/CVPR.2011.5995524
[25] Weixin Luo, Wen Liu, & Shenghua Gao. (Oct 2017). A revisit of sparse coding based anomaly detection in stacked RNN framework. Paper presented at the 341-349. doi:10.1109/ICCV.2017.45
[26] Weixin Luo, Wen Liu, & Shenghua Gao. (Jul 2017). Remembering history with convolutional LSTM for anomaly detection. Paper presented at the 439-444. doi:10.1109/ICME.2017.8019325
[27] Huo, J., Gao, Y., Yang, W., & Yin, H. (2012). Abnormal event detection via multi-instance dictionary learning. Intelligent Data Engineering and Automated Learning - IDEAL 2012, 76–83. https://doi.org/10.1007/978-3-642-32639-4_10
[28] DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. Sensors (Basel, Switzerland), 23(3), 1352. doi:10.3390/s23031352
[29] Hengyu, Z. (2020). Improved SMOTE algorithm for imbalanced dataset. Paper presented at the 693-697. doi:10.1109/CAC51589.2020.9326603
[30] Zerkouk, M., & Chikhaoui, B. (2019). Long short term memory based model for abnormal behavior prediction in elderly persons. How AI Impacts Urban Living and Public Health, 36–45. https://doi.org/10.1007/978-3-030-32785-9_4
[31] Pang, G., Shen, C., Cao, L., & Hengel, A. V. (2021). Deep Learning for Anomaly Detection. ACM Computing Surveys, 54(2), 1–38. https://doi.org/10.1145/3439950