Journal of Information Systems Engineering and Management
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Towards Securing IoT: A Deep Autoencoder-Based Anomaly Detection System

Zainab Abbas Shamsullah [1], Amir Lakizadeh[2] , Yaghoub Farjami[3]
[1,2,3] *Department of Computer and Information Technology, Faculty of Engineering, University of Qom*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 14 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

This research introduces three NIDS systems, named new Parallel Deep Auto-Encoder (NEW PDAE), as opposed to APAE, and DFE that has been proposed, with the goal of reducing processing load while enhancing or maintaining detection accuracy. Each of these models leverages different deep learning techniques to create an optimized structure. The proposed models were trained and evaluated on three datasets—CICIDS2017, UNSW-NB15, and KDDCup99—and then compared to the NDAE and MemAE algorithms. For multi-class classification, the NEW PDAE model achieved accuracies of 99.43%, 99.84%, and 99.92% on CICIDS2017, UNSW-NB15, and KDDCup99 datasets, respectively. The APAE model yielded accuracies of 99.50%, 99.89%, and 99.94%, while the DFE model achieved 99.31%, 99.96%, and 99.92% on these datasets. These results demonstrate that the proposed models provide sufficient accuracy and outstanding performance on these benchmark datasets for NIDS applications.

Conclusions: In this study, we presented three architectures, NEW PDAE, APAE, and DFE, for use in NIDSs. These architectures have demonstrated higher performance compared to simple encoder methods. The NEW PDAE method employs a parallel auto encoder technique with the ability to extract representations in different views. Due to the parallel feature extraction operations, NEW PDAE incurs less computational overhead, time, and fewer parameters compared to traditional methods for feature extraction. Another method, the APAE model, is based on an asymmetric auto encoder utilizing convolutional layers. This approach excels in extracting the best features in the encoder section by virtue of utilizing its modules effectively. Lastly, we introduced a very lightweight and powerful method called DFE, capable of using minimal processing and memory due to feature structuring while maintaining a very high detection accuracy.

For model implementation and testing, we utilized three datasets: CICIDS2017, UNSW-NB15, and KDDCup99, comparing our architectures with MemAE and NDAE models. As observed from the results presented in Section Four, our models NEW PDAE, APAE, and DFE exhibit higher accuracy compared to other models while offering fewer parameters. Therefore, it can be concluded that our proposed models are more suitable choices for devices like Internet of Things, where computational time and cost are critical, providing a much more viable option. Considering the hardware and computational constraints of Internet of Things devices, and bearing in mind the mentioned limitations, the aim is to substitute conventional layers in the presented methods with novel, extremely lightweight, and efficient convolutional layers in the future..

Keywords: Security, IoT, cloud, fog, intrusion detection system, deep learning

INTRODUCTION

In recent years, the deployment of IoT devices has raised significant security concerns, making network intrusion detection a crucial area of research. Chaabouni et al. [1] highlighted the importance of learning-based techniques in IoT security, emphasizing the role of adaptive models. Dhand and Tyagi [2] reviewed data aggregation techniques, a core requirement for efficiently managing IoT data. Pawar and Ghumbre [3] discussed IoT's vast applications and associated security challenges, while Vishwakarma and Jain [4] addressed the vulnerability of IoT networks to DDoS attacks, underscoring the need for robust defenses. Hassija et al. [5] explored various IoT security threats, identifying

potential solution architectures that can be applied to intrusion detection systems. Frustaci et al. [6] further analyzed critical IoT security issues, suggesting future directions for addressing evolving threats.Yang et al. [7] introduced IoT-based systems for remote health monitoring, showcasing the application of IoT in sensitive data environments, which emphasizes the need for security. Shah and Mishra [8] examined IoT in environmental monitoring, underscoring its role in smart cities where data security is critical. Smys [9] provided a comprehensive survey on smart IoT systems, detailing various applications and associated threats, while Saif et al. [10] addressed the vulnerability of home networks to unauthorized access. Kour et al. [11] analyzed IoT's dual impact on industries, focusing on its extensive applications but also highlighting inherent security risks.Lee et al. [12] discussed future IoT network requirements, pointing to security as a foundational aspect, whereas Matharu et al. [13] presented IoT security challenges, reinforcing the importance of robust defense mechanisms. Kumar et al. [14] proposed enhancements to IoT security at the hardware level, while Liao et al. [15] focused on preventing eavesdropping in heterogeneous IoT systems, which is crucial for data privacy. Kolias et al. [16] reviewed DDoS attacks in IoT, stressing the need for specific defenses like botnet mitigation. Choudhary and Kesswani [17] explored routing attack prevention in IoT, a vital area for maintaining secure network communication.Bandyopadhyay et al. [18] and Razzaque et al. [21] reviewed middleware solutions that facilitate secure communication in IoT, and Zhang and Wang [19] examined SQL injection vulnerabilities, highlighting the importance of secure back-end systems. Dorai and Kannan [20] further analyzed SQL injection threats, which are prevalent in IoT-connected databases. Swamy et al. [24] examined application-layer threats, emphasizing the need for comprehensive security models.For deep learning, Deng [25] provided an extensive overview of architectures and algorithms, relevant to intrusion detection systems, while Sadiq and Shyu [26] highlighted the importance of handling imbalanced data in IoT, a common issue in NIDS. Shyu et al. [27] extended this to multimedia data, emphasizing deep learning's role in complex classification tasks. Matharu et al. [28] and Nakov et al. [29] discussed algorithm optimization for anomaly detection, relevant to maintaining high accuracy in IoT. Pouyanfar et al. [30] reviewed deep learning applications for data-rich environments like IoT, while Paul and Singh [31] discussed recent advances, relevant for selecting optimal algorithms.Liu et al. [32] highlighted deep learning's effectiveness in general image classification, a technique that parallels feature extraction in NIDS. Sainath et al. [33] introduced bottleneck features with deep belief networks, beneficial for IoT due to reduced computational load. Krizhevsky et al. [34] demonstrated convolutional networks' power in complex data processing, crucial for intrusion detection. Fu et al. [35] discussed attention networks for data segmentation, which can enhance anomaly detection.Dai et al. [37] and Hochreiter and Schmidhuber [38] presented feature extraction and memory networks, respectively, providing architectures suited for capturing IoT data dependencies. Sainath et al. [39] and Sak et al. [40] demonstrated LSTM applications in handling sequential data, a common characteristic in network intrusion datasets. Benabdessalem et al. [41] and Li et al. [42] surveyed IoT security models, emphasizing the need for dynamic, multi-layered approaches to combat IoT-specific threats. Islam and Rahman [43] and Oliveira et al. [44] explored wireless security systems and IPv6 networks, both critical for scalable, secure IoT implementations. Jyothsna et al. [45] reviewed anomaly-based intrusion detection, a key approach for real-time IoT security, and Singh and Singh [46] compared host- and network-based intrusion detection systems, supporting the need for hybrid solutions in complex IoT environments. Karatas et al. [47] provided insights into deep learning applications in IDS, supporting the effectiveness of deep learning approaches, like those used in NEW PDAE, APAE, and DFE models.Xiao et al. [48] introduced a CNN-based model for intrusion detection that leverages feature reduction for improved efficiency, while Yu et al. [49] used convolutional autoencoders to enhance detection accuracy. Similarly, Yin et al. [50] demonstrated the utility of RNNs in intrusion detection, capturing temporal dependencies in network data. Shone et al. [51] presented a deep learning approach integrating feature extraction with neural networks to improve detection rates.For unsupervised anomaly detection, Gong et al. [52] used a memory-augmented autoencoder to recognize deviations from normal network behavior. Basati and Faghih [53] introduced APAE, an IoT-focused intrusion detection model using asymmetric autoencoders, which balances computational efficiency with high accuracy.[54] proposed a recalibration mechanism for fully convolutional networks using spatial and channel "squeeze and excitation" blocks to enhance feature learning, particularly in medical imaging. Similarly, [55] explored the feasibility of deep learning deployment on IoT devices, highlighting challenges such as computational constraints and energy efficiency. To address security concerns in IoT networks, [56] introduced the UNSW-NB15 dataset for network intrusion detection, providing a benchmark for evaluating anomaly detection models. Building on this, [57] proposed an autoencoder-based botnet detection framework to enhance IoT security, demonstrating its efficacy in detecting malicious activities. A similar approach was adopted by [58], where a deep autoencoder-based anomaly detection model was developed for identifying electricity theft cyberattacks in smart grids. Further extending autoencoder

applications, [59] employed a denoising autoencoder for intrusion detection in IoT systems, showing improved detection performance in noisy environments. [60] investigated trust management in deep autoencoder-based anomaly detection, aiming to enhance reliability in Social IoT. Meanwhile, [61] introduced a quantized autoencoder (QAE) for intrusion detection, designed to optimize anomaly detection in resource-constrained IoT devices using the RT-IoT2022 dataset. In terms of feature construction, [62] leveraged an autoencoder-based technique for clustering IoT attack patterns, enhancing threat categorization. However, [63] presented a transfer learning-based autoencoder for detecting DDoS attacks in IoT networks, though the study was later retracted, raising concerns about its validity. Our focus in this paper is on a type of intrusion detection systems that utilize deep learning techniques.

Problem statement

In this section of the research, considering the constraints of processing power, memory, and energy in Internet of Things devices, we will present NIDS systems. Therefore, we will employ three proposed methods for NIDS systems, including the NEW PDAE method, the APAE [51] model, and DFE mentioned. In all three mentioned methods, the emphasis lies on reducing processing and computational loads by decreasing the number of learnable parameters in the presented models. As one of the major challenges in deep learning-based architectures is reducing model parameters without compromising accuracy, the aim of each of these three methods is to reduce computational complexity while maintaining model accuracy and efficiency. Hence, in the following section, we will observe that our three proposed architectures will outperform the benchmark models NDAE [51] and MemAe [52] in terms of accuracy and classification while having significantly fewer parameters.Initially, we must outline various general aspects of implementing the aforementioned methods. Based on this, we will articulate the data preparation and normalization process. Subsequently, we will explain the construction of two-dimensional features from one-dimensional features and also discuss the advantages of transforming features into a two-dimensional structure.

Proposed method

3.1 The Presented Methods

3.1.1 Parallel Deep Auto-Encoder (NEW PDAE)

Using an encoder-decoder structure, a deep autoencoder can help reduce the dimensionality of input vectors. This process allows irrelevant information, which could lower classification accuracy, to be discarded, while the most influential features for classification are preserved. However, traditional deep autoencoders have drawbacks when applied to an NIDS system. They typically use standard convolutional filters, focusing only on a specific type of feature representation, and often overlook features that arise from interactions between more distant elements. This limitation results in reduced model efficiency and, conversely, increases computational load and the number of parameters, making it less feasible for IoT devices.To address this, the proposed method introduces an advanced model called the Parallel Deep Autoencoder (NEW PDAE). NEW PDAE integrates two types of autoencoders: one with a regular convolutional filter and another with an extended convolutional filter. This dual approach in NEW PDAE facilitates capturing different types of feature representations from varied feature spaces. As shown in Fig. 5, the NEW PDAE receives a 2D vector as input, produced through the preprocessing technique. In Fig. 1, the input dimensions are represented as 8x8, specific to the KDDCup99 dataset, while for the CICIDS2017 dataset, they are represented as 9x9.

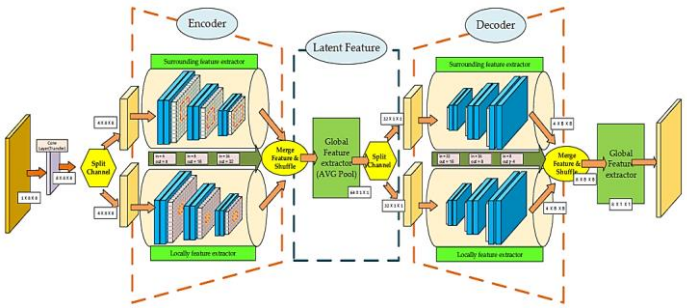


Fig. 1: Parallel Auto Encoder Model for the KDDCup99 Dataset

The NEW PDAE structure includes a feature transformer layer and three main components: the encoder, latent feature layer (or code layer), and decoder. The feature transformer layer contains eight standard convolutional filters,

which convert the input from a single-channel to an eight-channel format. These channels are then split into two groups, with each group prepared for input into the encoder. The encoder consists of two processing pipelines, called Tubes: the Surrounding feature extractor and the Local feature extractor. The Surrounding extractor pipeline utilizes a deep autoencoder with expanded convolution filters of size 3x3, while the Local extractor employs a deep autoencoder with standard 3x3 convolution filters.

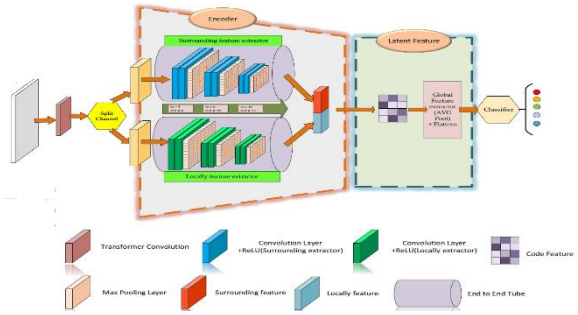


Fig. 2: Proposed NIDS Model using NEW PDAE and a Classifier

3.1.3 Architecture of the Asymmetric Parallel Auto-Encoder (APAE)

On standard encoder-decoder architectures, conventional deep autoencoders in NIDS face limitations due to their reliance on convolutional layer filters. For accurate feature extraction, these architectures require stacking numerous layers, which increases network complexity and makes them impractical for IoT applications. Moreover, as shown in Fig. 3, standard autoencoder encoders are symmetric—each layer in the decoder mirrors and reverses the function of its corresponding layer in the encoder. However, having fewer encoder layers with a higher number of processing units and a greater number of decoder layers can enhance data reconstruction in an autoencoder. This approach allows the encoder to develop a more robust abstract representation with fewer layers, while additional layers in the decoder improve the model's ability to reconstruct the input data. Based on this insight, our proposed approach leverages an advanced autoencoder, termed the Asymmetric Parallel Autoencoder (APAE), to optimize feature extraction and reconstruction for NIDS.

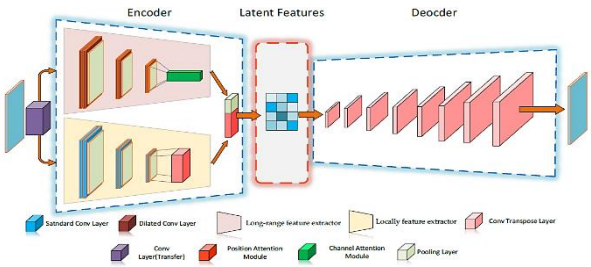


Fig. 3: The proposed model of Asymmetric Parallel Auto-Encoder (APAE)

3.1.4 Architecture of the deep Feature Extraction (DFE)

As outlined in our prior work [53], we converted the model's input data from a one-dimensional (1D) to a two-dimensional (2D) format before inputting it into the model. This transformation aggregates more cells/parameters, which simplifies the model's complexity. However, some parameters remain relatively far apart, posing challenges for 2D filters to capture meaningful correlations. Alternatively, by arranging individual parameters closer together within a three-dimensional (3D) space, we can simplify the network structure even further.Fig. 4 shows the complete structure of the proposed model. The model's input is a 2D version of the input vector, generated through a preprocessing step. The approach begins with a transfer layer comprising four standard 1x1 convolutional filters that transform the single-channel input into a four-channel representation (illustrated in blue). These channels are then split into two branches, each applying a different permutation type (as previously described) to capture the most relevant correlated information.Following the permutation step, each branch applies a convolutional layer with 8x2x2 filters and a stride of 2. In the first branch, this operation produces an output of 2x1x4, while in the second branch, the output size is 4x1x2. After this initial convolution and permutation stage, a second permutation is

performed in each branch to generate a new feature representation, ensuring that the outputs from both branches can be connected seamlessly. Once the branches are recombined, a Booster module further refines these features to create more sophisticated representations. Finally, a classifier is placed at the end of the model to identify and categorize different types of attacks.

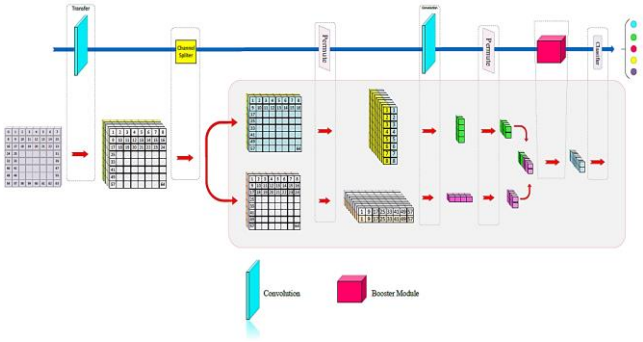


Fig.4: General structure of the proposed architecture.

RESULTS AND ANALYSIS

4.1 Simulation

In this section, the results of the APAE, NEW PDAE, and DFE models are presented using measurable parameters and metrics, followed by a comparison with the NDAE and MemAE models. It is important to note that for comparing the presented methods APAE, NEW PDAE, and DFE with the NDAE and MemAE models, more information on the algorithms and additional outputs on the datasets were required, which the authors of those papers did not provide. However, the source codes for NDAE and MemAE have been made publicly available. By utilizing their codes on all three datasets, we obtained the necessary outputs for analysis. For implementing the presented methods APAE, NEW PDAE, and DFE, we also used the Python programming language based on the Pytorch framework. All models were trained using the Adam optimizer and batch sizes of 128 for 40 iterations.

4.2 Datasets

For implementation, training, and assessing model performance, we have utilized public datasets in the domain of CICIDS2017, UNSW-NB15: NIDS, and KDDCup99 as the foundation. The assessment of models is conducted in two ways on these datasets, involving binary classification where one class represents normal and the other represents attack instances. However, in multi-class classification scenarios where one class represents normal and multiple classes represent different types of attacks, a detailed examination of model performance is undertaken. Multi-class evaluations are performed to scrutinize the performance of models across the classes within the dataset.

4.4 Model Evaluation

4.4.1 Binary Classification Analysis

4.4.1.1KDDCup99

In this section, the performance and efficiency of the proposed models NEW PDAE, APAE, and DFE are assessed alongside other models, NDAE and MemAE, on the KDDCup99 dataset concerning binary classification. Based on the results obtained from the models, as seen in Table 1, it can be inferred that our proposed models (NEW PDAE, APAE, and DFE) exhibit better performance compared to other models, providing higher accuracy.As observed from the presented results, in terms of accuracy and efficiency, the NEW PDAE model shows a 1.1% improvement, the APAE model shows an 1.11% improvement, and ultimately the DFE model demonstrates a 1.09% enhancement over the NDAE model. Additionally, the NEW PDAE model shows a 0.09% improvement, the APAE model 0.1%, and finally, the DFE model exhibits an 0.08% enhancement over the MemAE model. In terms of the number of learnable parameters in the models, we observe that the parameter count for the NEW PDAE model is 63.5%, while for the APAE model, it is approximately equal. Ultimately, the DFE model shows a 92% reduction in parameter count compared to the NDAE model, indicating a significant improvement in the proposed models over the NDAE.

Table 1: Presented results for binary classification on the KDDCup'99 dataset.

	ecision (%)				Recall (%)				-Score (%)			
	V E	E		AE E	V E	E	E	AE E	V E	E		AE E
Normal	76	36	8	.3	37	9	ł		86	84	36	78	.9	09
Attack	97	98	ɔ	.98	72	5	7	ɜ	ɜ	5	7	5	7	7
	V E	E		AE E										
Accuracy (%)	ɜ	ł	²	ł	ɜ									
Parameter														

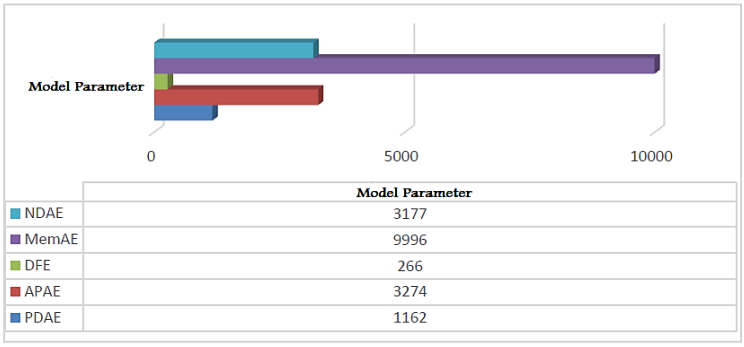


Fig.5: Comparison of parameter count in models on the KDDCup'99 dataset.

4.4.1.2 CICIDS2017

In this section, the performance and efficiency of our proposed models, NEW PDAE, APAE, and DFE, are compared and examined against other models, MemAE and NDAE, on the CICIDS2017 dataset for binary classification. As depicted in the results in Table 2, concerning accuracy and efficiency, the NEW PDAE model achieved 4.73%, the APAE model reached 4.09%, and ultimately, the DFE model exhibited a 4.34% improvement over the NDAE model. Furthermore, the NEW PDAE model showed an 1.18% improvement, the APAE model demonstrated a 0.54% improvement, and ultimately, the DFE model showcased a 0.79% enhancement over the MemAE model. However, in terms of the number of learnable parameters in the models, we observe that the NEW PDAE model had a 68% reduction, the APAE model a nearly 12% reduction, and ultimately, the DFE model a 92% decrease compared to the number of parameters in the NDAE model, indicating significant improvements in the proposed models over NDAE. Additionally, we find that the parameter counts for the NEW PDAE model reduced by 92%, the APAE model by 77%, and finally, the DFE model by approximately 98.5% compared to the parameter count in the MemAE model, showcasing either a reduction or enhancement in parameter numbers.

Table 2: Presented results for binary classification on the CICIDS2017 dataset.

	Precision (%)					Recall (%)					F-Score (%)				
	NEW PDAE	APAE	DFE	MemAE	NDAE	NEW PDAE	APAE	DFE	MemAE	NDAE	NEW PDAE	APAE	DFE	MemAE	NDAE
Normal	99.24	99.38	99.3	98.91	97.17	99.49	98.04	98.63	97.39	91.8672	99.37	98.96	98.96	98.15	94.37
Attack	99.51	99.13	98.69	97.9852	92.42	99.27	99.41	99.32	98.97	97.43	99.39	98.77	99	98.24	94.86

	NEW PDAE	APAE	DFE	MemAE	NDAE
Accuracy (%)	99.37	98.73	98.98	98.19	94.64
Parameter	1162	3278	282	14621	3732

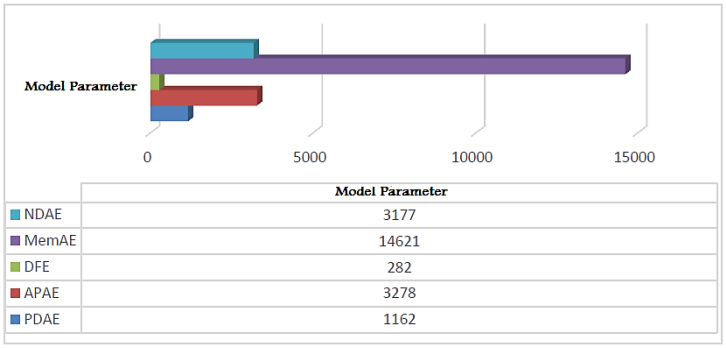


Fig. 6: Comparison of the number of parameters in models on the CICIDS2017 dataset.

4.4.1.3 UNSW-NB15

In this section, the proposed model NEW PDAE is evaluated alongside other models on the UNSW-NB15 dataset. As indicated in Table 3, all models perform well in the binary classification task on the UNSW-NB15 dataset. Further examination reveals that in terms of accuracy and efficiency, the NEW PDAE model, APAE model, and ultimately the DFE model show an improvement of 0.08% compared to the NDAE model. Additionally, the APAE, NEW PDAE, and DFE models exhibit similar accuracy to the MemAE model.

Table 3: Presented results for binary classification on the UNSW-NB15 dataset.

	Precision (%)					Recall (%)					F-Score (%)				
	NEW PDAE	APAE	DFE	MemAE	NDAE	NEW PDAE	APAE	DFE	MemAE	NDAE	NEW PDAE	APAE	DFE	MemAE	NDAE
Normal	100	100	100	99.99	99.92	100	100	100	100	100	99.92	100	100	100	99.99
Attack	100	100	100	100	99.94	100	100	100	100	99.99	99.94	100	100	100	100

	NEW PDAE	APAE	DFE	MemAE	NDAE
Accuracy (%)	100	100	100	99.99	99.92
Parameter	1162	1162	266	11621	3732

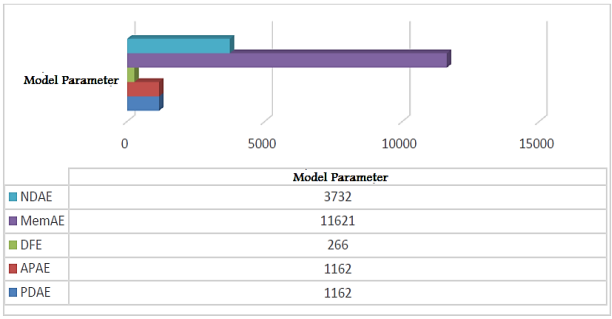


Fig. 7: Comparison of model parameters on the UNSW-NB15 dataset.

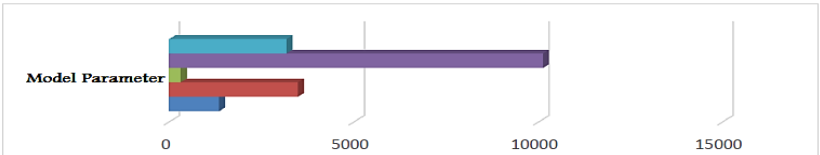
4.4.2 Multi-class Classification Analysis on KDDCup99.

4.4.2.1 KDDCup99

In this section, the proposed models NEW PDAE, APAE, and DFE are compared with other models MemAE and NDAE on the KDDCup99 dataset concerning multi-class (5-class) classification. This dataset comprises 5 classes, including 1 normal class and 4 classes of various attacks. However, the U2R class in this dataset has the fewest records, only 52 in total, making different models weaker on this class. As shown in Table 4 results, models NEW PDAE and DFE show similar accuracies of 1.79%, and also the APAE model provides an improvement of 1.81% in accuracy compared to the NDAE model. On the other hand, compared to MemAE, models NEW PDAE and DFE offer improvements of 0.09% and APAE 0.11% in accuracy.

Table 4: Results presented for multi-class classification on the KDDCup'99 dataset.

	Precision (%)					**Recall (%)**					**F-Score (%)**				
	NEW PDAE	**APAE**	**DFE**	**MemAE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**MemAE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**MemAE**	**NDAE**
U2R	99.85	99.82	99.74	99.66	94.36	99.81	99.91	99.88	99.51	99.02	99.83	99.86	99.81	99.58	96.63
DoS	80	64.71	90.91	0	0	75	62.5	62.5	0	0	77.42	66.67	74.07	0	0
R2L	99.99	100	100	99.99	99.19	100	100	100	100	99.18	99.99	100	100	100	99.19
Probe	95.1	96.73	94.85	70	62.77	91.89	89.86	87.16	89.86	19.93	93.47	93.17	90.85	78.7	30.26
U2R	97.74	98.95	99.32	99.9	40.24	98.67	98.95	97.81	96.48	3.14	98.2	98.95	98.56	98.16	5.83
	NEW PDAE	**APAE**	**DFE**	**MemAE**	**NDAE**										
Accuracy (%)	99.92	99.94	99.92	99.83	98.13										
Parameter	1357	3469	317	11621	3177										



	Model Parameter
NDAE	3177
MemAE	10122
DFE	317
APAE	3489
PDAE	1357

Fig. 8: Comparison of the number of parameters in models on the KDDCup'99 multi-class dataset.

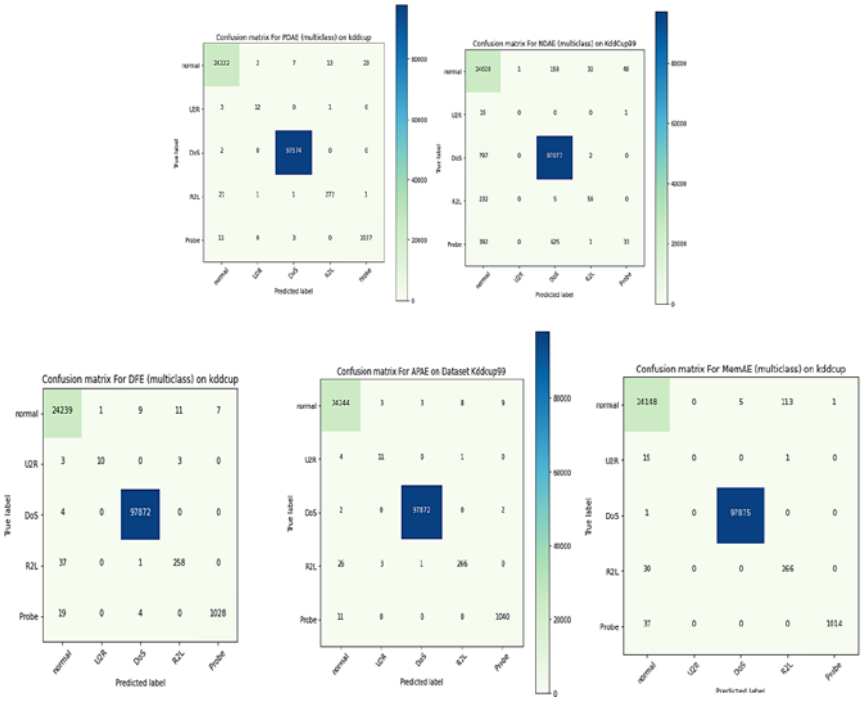
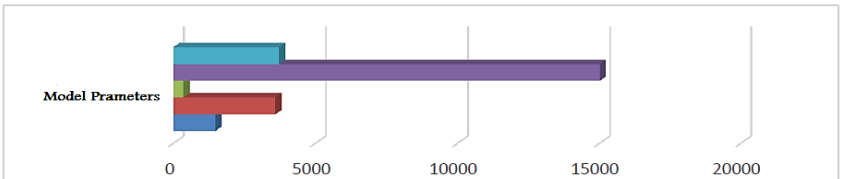


Fig. 9: Confusion matrix for models on the KDDCup'99 dataset.

4.4.2.2 CICIDS2017

In this section, the proposed models NEW PDAE, APAE, and DFE are evaluated and compared with other models NDAE and MemAE in terms of multi-class classification for the CICIDS2017 dataset. This dataset, for multi-class classification, consists of one normal class and six attack classes, encompassing a wide spectrum of novel network attacks. However, this dataset is highly imbalanced and complex in terms of record distribution. For instance, the Infiltration class has only 36 records while the Portscan class has 158,930 records.



	Model Prameters
NDAE	3732
MemAE	15016
DFE	367
APAE	3599
PDAE	1487

Fig. 10: Comparison of the number of parameters of models on the CICIDS2017 multi-class dataset.

Table 5: Presented Results for Multi-Class Classification on the CICIDS2017 Dataset.

	Precision (%)					Recall (%)					F-Score (%)				
	NEW PDAE	**APAE**	**DFE**	**MemAE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**MemAE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**MemAE**	**NDAE**
Benign	99.58	99.81	99.47	99.39	98.48	99.29	99.21	99.17	97.23	99.02	99.44	99.51	99.32	98.3	97.52
DoS	99.16	99.47	99.06	98.9	98.4	99.83	99.84	99.76	99.77	99.25	995.5	99.65	99.41	99.34	98.82
PortScan	99.66	99.58	99.7	93.99	93.42	99.86	99.88	99.81	99.83	98.03	99.76	99.73	99.75	96.82	95.67
Infiltration	60	38.89	100	0	0	75	58.33	41.67	0	0	66.67	46.46	58.82	0	0
Web Attack	92.22	64.37	95.63	88.24	56.74	88.37	96.84	83.06	9.48	53.73	90.25	77.33	88.9	17.12	55.19
Bot	97.63	82	77.75	83.89	83.14	36.98	85.93	51.8	60.03	64.22	53.64	83.92	62.17	69.98	72.47
Brute Force	99.59	99.38	98.16	91.85	97.56	99.38	99.75	95.75	99.4	96.72	99.48	99.57	97.04	95.48	97.14
	NEW PDAE	**APAE**	**DFE**	**MemAE**	**NDAE**										
Accuracy (%)	99.43	99.5	99.31	98. 26	97. 56										
Parameter	1487	3599	367	15016	3732										

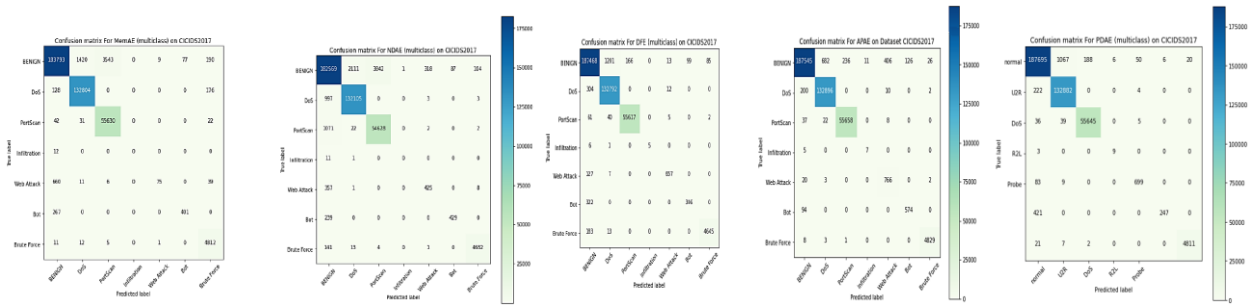


Fig.11: Confusion matrix for models on the CICIDS2017 dataset.

4.4.2.3 UNSW-NB15

In this section, the proposed models NEW PDAE, APAE, and DFE are compared and evaluated against other models like MemAE and NDAE on the UNSW-NB15 dataset for multi-class classification. This dataset consists of 1 normal class and 9 attack classes, covering a wide spectrum of network attacks. In terms of the distribution of class records in the UNSW-NB15 dataset, it is highly complex and asymmetric. For example: The Worms class has 130 records in the training set and only 44 records in the test set. Similarly, the Shellcode class has 1133 records in the training set and 378 records in the test set. These two classes are minority classes compared to others. From the analysis and

results in Table 6, it is observed that in terms of accuracy and performance, the NEW PDAE model achieved 33.11%, the APAE model achieved 33.16%, and ultimately, the DFE model showed a 33.23% improvement over the NDAE model.

Table 6: Presented results for multi-class classification on the UNSW-NB15 dataset.

	Precision (%)					Recall (%)					F-Score (%)				
	NEW PDAE	**APAE**	**DFE**	**Mem AE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**Mem AE**	**NDAE**	**NEW PDAE**	**APAE**	**DFE**	**Mem AE**	**NDAE**
Normal	99.99	99.96	100	99.81	68.78.	99.99	100	100	100	94.91	99.99	99.98	100	99.91	76.76
Reconnaissance	99.97	100	100	100	17.64	99.91	99.8	99.97	96.28	3.03	99.94	99.99	100	98.11	5.17
Backdoor	98.64	98.531	100	88.08	12.66	99.83	100	100	91.25	8.23	99.23	99.15	100	89.64	9.98
Dos	97.96	99.46	99.42	85.84	15	99.85	99.56	99.98	98.26	12.74	98.9	99.51	99.7	91.63	13.78
Exploit	99.99	100	100	98.91	2.21	99.25	99.53	99.78	93.7	0.04	99.62	99.77	99.89	96.24	0.07
Analysis	99.84	96.98	99.85	90.35	3.13	99.7	99.56	100	99.56	5.47	98.25	98.25	99.93	94.73	
Fuzzers	100	99.69	100	99.77	16.07	99.59	99.84	99.98	98.14	16.58	99.79	99.76	100	98.94	
Worms	93.62	91.67	100	8.19	0	100	100	100	84.09	0	967.7	95.65	100	14.92	0
Shellcode	99.73	100	99.74	52.78	0	99.21	100	100	5.03	0	99.47	100	99.87	9.18	0
Generic	99.98	100	100	99.89	98.84	99.99	100	100	99.88	95.95	99.99	100	100	99.89	97.37
	NEW PDAE	**APAE**	**DFE**	**Mem AE**	**NDAE**										
Accuracy (%)	99.84	99.89	99.96	98.23	66.73										
Parameter	1682	3794	402	12061	3372										

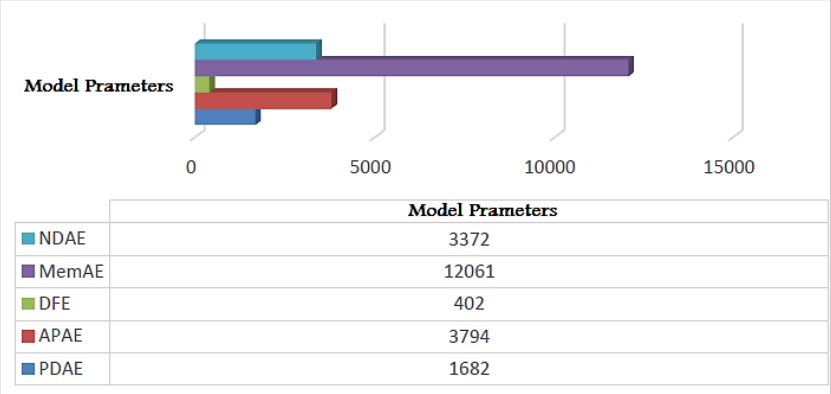


Fig. 12: Comparison of the number of parameters of the models on the UNSW-NB15 dataset for multi-class classification.

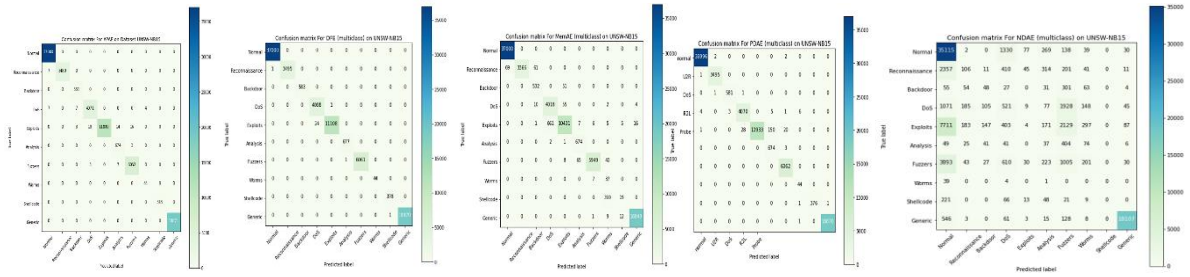


Fig. 13: Confusion matrix for the models on the UNSW-NB15 dataset.

CONCLUSION

In this study, we presented three architectures, NEW PDAE, APAE, and DFE, for use in NIDSs. These architectures have demonstrated higher performance compared to simple encoder methods. The NEW PDAE method employs a parallel auto encoder technique with the ability to extract representations in different views. Due to the parallel feature extraction operations, NEW PDAE incurs less computational overhead, time, and fewer parameters compared to traditional methods for feature extraction. Another method, the APAE model, is based on an asymmetric auto encoder utilizing convolutional layers. This approach excels in extracting the best features in the encoder section by virtue of utilizing its modules effectively. Lastly, we introduced a very lightweight and powerful method called DFE, capable of using minimal processing and memory due to feature structuring while maintaining a very high detection accuracy.

For model implementation and testing, we utilized three datasets: CICIDS2017, UNSW-NB15, and KDDCup99, comparing our architectures with MemAE and NDAE models. As observed from the results presented in Section Four, our models NEW PDAE, APAE, and DFE exhibit higher accuracy compared to other models while offering fewer parameters. Therefore, it can be concluded that our proposed models are more suitable choices for devices like Internet of Things, where computational time and cost are critical, providing a much more viable option.Considering the hardware and computational constraints of Internet of Things devices, and bearing in mind the mentioned limitations, the aim is to substitute conventional layers in the presented methods with novel, extremely lightweight, and efficient convolutional layers in the future.

REFRENCES

[1] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security based on Learning Techniques," IEEE Communications Surveys & Tutorials, pp. 2671 - 2701, 2019.

[2] G. Dhand and S. Tyagi, "Data aggregation techniques in WSN: Survey," Procedia Computer Science, pp. 378-384, 2016.

[3] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," in 2016 International Conference on Computing, Analytics and Security Trends (CAST), India, 2016, pp. 294-299.

[4] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommunication Systems, pp. 3-25, 2020.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal ,and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access, pp. 82721-82743, 2019.

[6] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," IEEE Internet of Things Journal, pp. 2483-2495, 2017.

[7] G. Yang et al., "IoT-based remote pain monitoring system: From device to cloud platform," IEEE journal of biomedical and health informatics, pp. 1711-1719, 2017.

[8] J .Shah and B. Mishra, "IoT enabled environmental monitoring system for smart cities," in 2016 international conference on internet of things and applications (IOTA), India, 2016, pp. 383-388.

[9] S. Smys, "A Survey on Internet of Things (IoT) based Smart Systems," Journal of ISMAC, pp. 181-189, 2020.

[10] U. Saif, D. Gordon, and D. Greaves, "Internet access to a home area network," IEEE Internet computing, pp. 54-63, 2001.

[11] K. Kour, D. Gupta, K. Gupta, and M. S. Bali, "IoT: Systematic Review, Architecture, Applications and Dual Impact on Industries," IOP Conference Series: Materials Science and Engineering, p. 012053, 2021.

[12] S. K. Lee, M. Bae, and H. Kim, "Future of IoT networks: A survey," Applied Sciences, p. 1072, 2017.
[13] G. S. Matharu, P. Upadhyay, and L. Chaudhary, "The Internet of Things: Challenges & security issues," in 2014 International Conference on Emerging Technologies (ICET), Pakistan, 2014, pp. 54-59.
[14] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. Mahapatra, "Security Enhancements to System on Chip Devices for IoT Perception Layer," in 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), India, 2017, pp. 151-156.
[15] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in 2018 15th IEEE Annual Consumer Communications & Networking Conf. (CCNC), USA, 2018, pp. 1-2.
[16] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, pp. 80-84, 2017.
[17] S. Choudhary and N. Kesswani, "Detection and prevention of routing attacks in internet of things," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), USA, 2018, pp. 1537-1540.
[18] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," in Recent trends in wireless and mobile networks, 2011 ,pp. 288-296.
[19] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in 2009 International Symposium on Computer Network and Multimedia Technology, China, 2009, pp. 1-4.
[20] R. Dorai and V. Kannan, "SQL injection-database attack revolution and prevention," J. Int'l Com. L. & Tech., p. 224, 2011.
[21] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," IEEE Internet of things journal, pp. 70-95, 2015.
[22] S. Hidano, S. Kiyomoto, Y. Murakami, P. Vlacheas, and K. Moessner, "Design of a security gateway for iKaaS platform," in International Conference on Cloud Computing, South Korea, 2015, pp. 323-333.
[23] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," IEEE Access, pp. 24639-24649, 2018.
[24] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), India, 2017, pp. 477-480.
[25] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," APSIPA Transactions on Signal and Information Processing, pp. 1–29, 2014.
[26] Y. Y. S .Sadiq and M. C. M.-L. Shyu, "Efficient Imbalanced Multimedia Concept Retrieval by Deep Learning on Spark Clusters," Deep Learning and Neural Networks: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, p ,2019.274.
[27] M. C. Yilin Yan, Mei-Ling Shyu, and Shu-Ching Chen, "Deep learning for imbalanced multimedia data classification," In The IEEE International Symposium on Multimedia. IEEE, pp. 483–488, 2015.
[28] N. D. a. B. Triggs., "Histograms of oriented gradients for human detection," presented at the IEEE Conference on Computer Vision and Pattern Recognition, USA, 2005.
[29] P. Nakov, A. Ritter, S. Rosenthal, F. Sebastiani, and V. Stoyanov, "SemEval-2016 task 4: Sentiment analysis in Twitter," arXiv preprint arXiv:1912.01973, p. 0, 2019.
[30] S. Pouyanfaret al., "A survey on deep learning: Algorithms, techniques, and applications," ACM Computing Surveys (CSUR), p. 92, 2019.
[31] S. Paul and L. Singh, "A review on advances in deep learning," in 2015 IEEE Workshop on Computational Intelligence: Theories, Applications and Future Directions (WCI), India, 2015, pp. 1-6.
[32] P.-H. Liu, S.-F. Su, M.-C. Chen, and C.-C. Hsiao, "Deep learning and its application to general image classification," in 2015 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS), China, 2015, pp. 7-10.
[33] T. N. Sainath, B. Kingsbury, and B. Ramabhadran, "Auto-encoder bottleneck features using deep belief networks," in 2012 IEEE international conference on acoustics, speech and signal processing (ICASSP), Japan, 2012, pp. 4153-4156.
[34] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," ACM, pp. 1097-1105, 2012.

[35] J. Fu et al., "Dual Attention Network for Scene Segmentation," in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), USA, 2019, pp. 3141-3149.
[36] G. E. Hinton, "A practical guide to training restricted Boltzmann machines," in Neural networks: Tricks of the trade: Springer, 2012, pp. 599-619.
[37] X. Dai et al., "Deep Belief Network for Feature Extraction of Urban Artificial Targets," Mathematical Problems in Engineering, p. 0, 2020.
[38] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural computation, pp. 1735-1780, 1997.
[39] T. N. Sainath, O. Vinyals, A. Senior, and H. Sak, "Convolutional, long short-term memory, fully connected deep neural networks," in 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Australia, 2015, pp. 4580-4584.
[40] H. Sak, A. Senior, and F. Beaufays, "Long short-term memory recurrent neural network architectures for large scale acoustic modeling," in Fifteenth annual conference of the international speech communication association, USA, 2014.
[41] R. Benabdessalem, M. Hamdi, and T.-H. Kim, "A survey on security models, techniques, and tools for the internet of things," in 2014 7th International Conference on Advanced Software Engineering and Its Applications, China, 2014, pp. 44-48.
[42] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Information Systems Frontiers, pp. 243-259, 2015.
[43] M. S. Islam and S. A. Rahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches," International Journal of Advanced Science and Technology, pp. 1-8, 2011.
[44] L. M. Oliveira, J. P. Amaral, J. M. Caldeira, J. J. Rodrigues, and L. Zhou, "Management system for IPv6-enabled wireless sensor networks," in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, China, 2011, pp. 195-200.
[45] V. Jyothsna, V. R. Prasad, and K. M. Prasad, "A review of anomaly-based intrusion detection systems," International Journal of Computer Applications, pp. 26-35, 2011.
[46] A. P. Singh and M. D. Singh, "Analysis of host-based and network-based intrusion detection system," IJ Computer Network and Information Security, pp. 41-47, 2014.
[47] G. Karatas, O. Demir, and O. K. Sahingoz, "Deep Learning in Intrusion Detection Systems," in 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), india, 2018, pp. 113-116.
[48] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao" ,An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," IEEE Access, pp. 42210-42219, 2019.
[49] Y. Yu, J. Long, and Z. Cai, "Network intrusion detection through stacking dilated convolutional autoencoders," Security and Communication Networks, p. 1, 2017.
[50] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, pp. 21954-21961, 2017.
[51] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, pp. 41-50, 2018.
[52] D. Gong et al., "Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection," in Proceedings of the IEEE/CVF International Conference on Computer Vision, USA, 2019, pp. 1705-1714.
[53] A. Basati and M. M. Faghih, "APAE: an IoT intrusion detection system using asymmetric parallel auto-encoder," Neural Computing and Applications, p. 1, 2021.
[54] A. G. Roy, N. Navab, and C. Wachinger, "Recalibrating fully convolutional networks with spatial and channel “squeeze and excitation” blocks," IEEE transactions on medical imaging, pp. 540-549, 2018.
[55] J. Tang, D. Sun, S. Liu, and J.-L. Gaudiot, "Enabling deep learning on IoT devices," Computer, pp. 92-96, 2017.
[56] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in 2015 military communications and information systems conference (MilCIS), Australia, 2015, pp. 1-6.
[57] Mahajan, Radhika, and Manoj Kumar. "Autoencoder-Based Botnet Detection for Enhanced IoT Security." In International Conference on Sustainable Development through Machine Learning, AI and IoT, pp. 162-175. Cham: Springer Nature Switzerland, 2023.

[58]]Takiddin, Abdulrahman, Muhammad Ismail, Usman Zafar, and ErchinSerpedin. "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids." IEEE Systems Journal 16, no. 3, 2022, 4106-4117.
[59] Alrayes, Fatma S., Mohammed Zakariah, Syed Umar Amin, Zafar Iqbal Khan, and MahaHelal. "Intrusion detection in IoT systems using denoising autoencoder." IEEE Access, 2024.
[60] Rashmi, M. R., and C. Vidya Raj. "Trust Management for Deep Autoencoder based Anomaly Detection in Social IoT." International Journal of Advanced Computer Science and Applications 14, no. 1, 2023.
[61] Sharmila, B. S., and Rohini Nagapadma. "Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset." Cybersecurity 6, no. 1, 2023, 41.
[62] Haseeb, Junaid, Masood Mansoori, Yuichi Hirose, Harith Al-Sahaf, and Ian Welch. "Autoencoder-based feature construction for IoT attacks clustering." Future Generation Computer Systems 127, 2022, 487-502.
[63] Shafiq, Unsub, Muhammad Khuram Shahzad, Muhammad Anwar, Qaisar Shaheen, Muhammad Shiraz, and Abdullah Gani. "[Retracted] Transfer Learning Auto-Encoder Neural Networks for Anomaly Detection of DDoS Generating IoT Devices." Security and Communication Networks 2022, no. 1, 2022, 8221351.