Revue d'Intelligence Artificielle
Vol. 38, No. 3, June, 2024, pp. 893-900
Journal homepage: http://iieta.org/journals/ria

Deep Learning Methods to Prevent Various Cyberattacks in Cloud Environment

Qusay Kanaan Kadhim*, Ohood Fadil Alwan, Inteasar Yaseen Khudhair

Department of Computer Science, University of Diyala, Baqubah 32001, Diyala, Iraq

Corresponding Author Email: dr.qusay.kanaan@uodiyala.edu.iq

https://doi.org/10.18280/ria.380316

Received: 24 November 2023
Revised: 3 January 2024
Accepted: 9 January 2024
Available online: 21 June 2024

Keywords:
deep learning, cloud computing, cyberattacks, principal component analysis (PCA), Fuzzy C-Means (FCM), AutoEncoder (AE), CE-CIC-2018 dataset

ABSTRACT

Cloud computing offers many benefits, but it also presents new cybersecurity challenges that must be addressed to ensure data protection in the cloud environment. Governments and organizations face increasing and ongoing cyberattacks by state-sponsored hackers to wage cyberwars. A successful cyberattack on vital infrastructure, such communications or electricity networks, might have disastrous effects. These attacks vary in their forms and patterns, which makes understanding and confronting them necessary. An essential function of artificial intelligence is the detection of intrusions. To prevent various cyberattacks in the cloud environment and is widely considered the best method. The Deep Learning (DL) method efficiently trained on datasets to improve performance based on statistical features can accurately detect various attacks. In this paper, we use the CE-CIC-2018 dataset that contains seven distinct attack scenarios, updated for cybersecurity: Brute-force, Heartbleed, Botnet, DoS, DDoS, and Web Attacks. This paper contributes, to improving the precision of identifying different types of threats in a cloud environment and improving additional performance indicators. The proposed using DL method dimensionality reduction using Principal Component Analysis (PCA), the Fuzzy C-Means (FCM) technique to create clusters, and the deep learning-based AutoEncoder (AE) method combined to identify the attack and non-attack. PCA + FCM + AE method prevents different cyberattacks in a cloud environment. The results showed that the best accuracy was 97.70 %, which is the highest accuracy compared to those results reported in the relevant literature.

1. INTRODUCTION

In a cloud computing environment, pooled resources, software, and data are made available to computers and other devices on demand [1]. In addition to providing a lot of storage space, the cloud also has a ton of computer power, which it may use to support various web-based applications [2]. Virtual Machines (VMs) that handle a variety of multiuser applications are available from Cloud Service Providers (CSPs). Utilizing virtual machines in cloud computing has been extremely beneficial for providing a wide range of end users with a flexible, affordable, extensible, interoperable, and uniform interface [3]. Popular cloud computing services include Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) [4]. Deep Learning (DL) deep learning is used to analyses large amounts of unstructured data such as images and audio files in of cloud computing [5]. Cloud computing has become famous for providing distinctive services that facilitated its users' work, reduced its cost, and made it easy for institutions and individuals to start their work by relying entirely on cloud computing.

The COVID-19 pandemic has accelerated the transition to work-from-home policies worldwide [6]. An enormous rise in IT multipliers has been caused by the growing use of cloud collaboration platforms and virtual meeting systems. The unplanned implementation of remote work infrastructure was accompanied by insufficient and non-comprehensive policies for tools such as cloud server access. The cloud computing market is booming in the Middle East and Africa region, with expectations that it will achieve annual growth of 23.82%, CAGR, by Kosmopoulos et al. [7]. In this context, experts confirm that the region needs this type of service with the increasing rate of tests annually for research and development.

In turn, small and medium-sized companies use a larger volume of data, which they transfer to the cloud and work on processing and analyzing it while adopting a smart solutions strategy. Figure 1 shows growth expectations for the adoption of cloud computing services in the Middle East and Africa region.

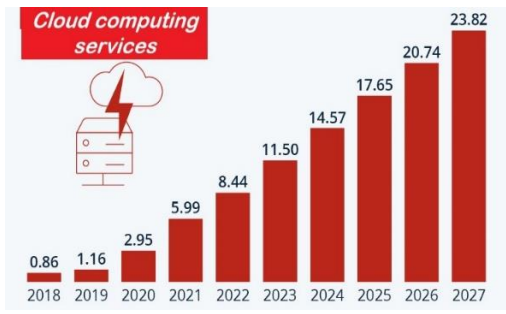

Figure 1. Growth of cloud computing services in the Middle East and Africa region [8]

According to studies, 70 % of customers' requirements for cloud-native capabilities will be provided by cloud-native, ultra-fast service provider ecosystems, rather than focusing on the edge cloud. In 2026, spending on cloud computing could exceed $1 trillion worldwide, surpassing all IT markets [9]. Utilizing virtual machines in cloud computing has been extremely beneficial for providing a wide range of end users with a flexible, affordable, extensible, interoperable, and uniform interface [10]. The IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) are popular cloud computing services [11]. Intrusion Detection Systems (IDSs) are reliable defenses against these attackers and can stop them from happening [12]. The behaviors of end users, changes to network traffic, system configuration, log files, and IDS monitoring can all be used to spot suspicious activity [13].

Growing dangers Cloud attacks have the potential to significantly impact a company by resulting in data loss, financial loss, and reputational harm. Organizations must have robust cloud security measures in place to guard against assaults on the cloud. These measures should include intrusion detection and prevention, data encryption, and access control. The recommended approach uses an algorithm based on deep learning concepts to process traffic-based raw data before moving on to a clustering mechanism to separate attack data. The deep learning method is then used to the attack cluster data to categorize the attack [14]. Finally, a greater accuracy will be used to demonstrate the classified attack's accuracy along with other metrics like accuracy, recall, and precision.

Cyber threats range from malicious activities to the cloud and cloud, such as hacking, phishing, malware attacks, and ransomware incidents. These threats exploit weaknesses in networks, systems, and software to gain unauthorized access, steal sensitive information, or disrupt operations. In line with this, businesses are seeking security solutions that help protect their networks and prevent financial losses, reputational damage, and legal repercussions. Artificial Intelligence technology offers great opportunities to advance the field of cybersecurity and protect sensitive data. These technologies must be used proactively and sustainably to address the increasing threats of our modern age.

Organization of this paper, Cyberattacks on cloud environment, Related works, Methodology, CE-CIC-2018 dataset, Modules for cluster formation, Module for attack classification, Result and analysis, Evaluation method and finally Conclusions and future work.

2. CYBERATTACKS ON CLOUD ENVIRONMENT

Used by companies in a variety of industries, including manufacturing, transportation, energy, and retail, to operate more profitably and efficiently with regard to customer service [15]. Organizations need to safeguard their digital assets and prevent unauthorized access to their systems in the same way that they do with their physical assets [16]. When someone intentionally hacks into a computer system, network, or related facility, it is referred to as a “cyber-attack”. A successful cyber-attack results in confidential data being exposed, stolen, deleted or altered, Cybersecurity measures defend against cyberattacks [17].

Information security experts and specialists advise various public sectors and government institutions and learn about the best practices and relevant international experiences in the field of cybersecurity [18]. The importance of planning and thinking about the issue of security and cyber vigilance before moving to cloud computing services to study potential cyber-attacks and draw up scenarios for confronting them, in order to meet security needs and raise their readiness regarding cyber risks on all cloud computing services.

The methods and mechanisms of cyber-attacks have developed recently of these methods is expected to witness a noticeable increase in the coming period is Cyber Attacks as a Service, which will provide cyber-attack mechanisms through cloud computing services, which can During which cyber-attacks are carried out by people who do not have the resources, whether the experience or the technical systems necessary to carry out such attacks. Figure 2 shows results of the most common types of cyber-attacks in cloud computing in 2023.

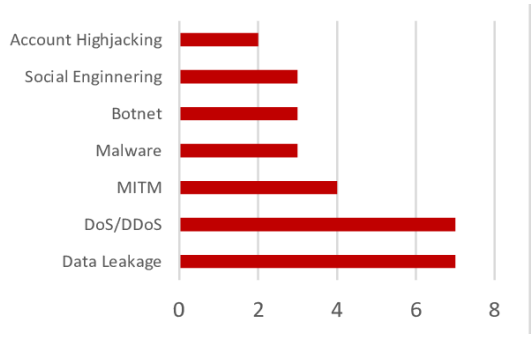

Figure 2. Cyber-attacks combination on a cloud environment [19]

Attack actors continue to evolve their techniques, and our strategies to defend against these attacks must evolve in parallel. Enhanced cybersecurity measures, information sharing, and early threat detection are now essential to protecting financial systems and mitigating tensions [20]. Learn about the best practices and relevant international experiences in the field of cybersecurity. In the cyber field based on artificial intelligence technologies, its advanced solutions and platforms, contribute to improving the capabilities of detecting threats and responding to them accurately, and reducing the time needed to neutralize cyber threats [21]. Governments work through their institutions to provide solutions to institutions in various sectors such as financial services, healthcare and the public sector. To classify unknown data sets as harmful or benign using machine learning techniques. Figure 3 shows Artificial intelligence (AI) and machine learning (ML), particularly deep learning (DL), regarding the potential and current applications of AI for intelligent data analysis and automation in cyber security.

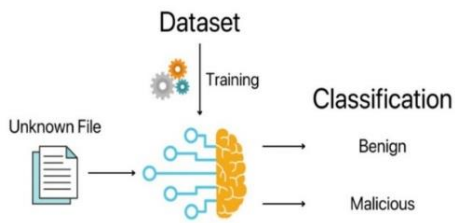

Figure 3. Using intelligence in the field of cyber-attacks [22]

Using AI knowledge, especially deep learning and machine learning technology, is essential to provide an improved security system through analysis of security data. In the

context of cyber security, machine learning is considered a subfield of artificial intelligence, which is a more general word; Artificial intelligence is also substituted with the term machine learning with an emphasis on how it is used for intelligent data analysis and automation in cybersecurity through its ability to extract valuable insights from cyber data [23].

Decision-making, automation, and data-driven intelligence allow government institutions and organizations to protect and proactively mitigate. Using deep learning technology in the field of cybersecurity exploring the state of machine learning and its approaches today the method is combined to determine the attack and non-attack to achieve future cyberattack breakthroughs [24].

Deep learning approach in our modern era has become more prominent in providing security and support against malicious activities, and with the development of digital technologies and the increase in cyber threats at the same time. It is necessary to develop defense mechanisms in the face of risks facing the important data of institutions and individuals, and to protect against cyber-attacks that aim to blackmail, steal money, and destroy businesses.

3. RELATED WORKS

Today's trend is quickly shifting to cloud computing, where processing, storage, and networking resources are all located online. As a result, several businesses, including AWS, Azure, Google, and Oracle, now offer IaaS, PaaS, and SaaS services to their clients through their own cloud services [25]. The number of people using cloud provider services increased dramatically, particularly during the COVID-19 period. Due to router-based attacks, cyber security is a concern as the cloud expands so quickly [26]. According to a recent analysis from insight, there has been a significant migration of businesses to the cloud environment, but some concerns have persisted, prompting other businesses to review their security [27]. This section will address relevant literature for this investigation, which makes use of the CSE-CIC-IDS2018 dataset.To improve the robustness and efficiency of cloud environments by increasing the accuracy, recall, and precision of the model in the cloud environment through deep learning for intrusion prevention and detection [28].

In 2019, Lin et al. [29], they presented a proposed anomaly detection system using LSTM and attention mechanism (AM) to increase the network training performance. The (LSTM+AM) cyber dataset CIC-IDS 2018 was used to train the proposed mouthed the analysis of the results reported an accuracy of 96.00%, a detection rate of 15%, and a recall rate of 95%.

In 2020, Gamage and Samarabandu [30], they presented the use of deep learning models with (AE + ANN) for intrusion detection and classification. Deep learning models are able to learn intrusion patterns from large data sets in a cloud-computing environment. Attacks against the cloud-computing environment are a growing threat, and intrusion detection systems are essential to detect them and alert to protect teams. The AE+ANN models showed that the model accuracy was 76.88%.

In 2021, Kunang et al. [31], employing a pre-training strategy that combines Deep Neural Network (DNN) and Deep AutoEncoder (PTDAE). In the period prior to training, they examined the outcomes of using our strategy with three feature extraction techniques: Deep AutoEncoder (DAE), and Stacked AutoEncoder (SAE). To increase detection performance, the automated hyperparameter optimization procedure assists in determining the hyper parameter value and the optimal class configuration of hyperparameters. Datasets from CSE-CIC-ID2018 were used to test the suggested model. The (PTDAE+DNN) method showed that the model accuracy was 95.79%, recall was 95.15, and precision was 95.19.

In 2022, Srinivas et al. [32], The Sail Fish Dolphin optimization-based deep recurrent neural network (SFDO-based Deep RNN) presents an efficient intrusion detection method, it is employed in the cloud environment to detect anomalies. The Sail Fish Optimizer (SFO) and Dolphin Echolocation (DE) algorithms are integrated to generate the developed SFDO. Fuzzy C-Means (FCM) clustering is used to group certain attribute features that are gathered from the cloud model. Using the suggested method (SFDO-RNN+FCM), the results for intrusion detection on the CSE-CIC-IDS-2018 dataset were accuracy of 95.22%, precision of 98.82%, and recall of 96.82%.

In 2023, Balajee and Jayanthi Kannan [33], The suggested model combines a deep learning algorithm with a hybrid method. It combines the centroid optimization approach, the fuzzy C-Means (FCM) procedure for ensemble generation, the Spider Monkey Optimization (SMO) algorithm for affecting ensembles, and the dimensionality reduction technique (PCA), using the AutoEncoder (AE) technique based on deep learning for the classification of attacks (only from data packages provided in the attack set). When compared to the CSE-CIC-IDS-2018 dataset, which is the most popular combination of contemporary cyber-attacks on a cloud computing environment, the recommended technique (PCA + SMO-FCM + AE) yielded 95% results for intrusion detection. Against 11 other current approaches, this is compared.

The cybersecurity landscape is constantly evolving, driven by emerging industry trends and the ever-changing tactics of cybercriminals. To effectively address cybersecurity challenges, it is essential that government and enterprise organizations stay on top of the latest trends and understand the evolving threat landscape. To combat adversarial attacks, cybersecurity professionals must constantly update and improve AI methods, incorporate robust security measures that improve the accuracy of detecting various attacks and enhance other performance metrics.

Table 1 provides a summary of the work results related to the methods in the CE-CIC-2018 dataset, and an analysis of previous work compared to other methods for five methods. The critical analysis and comparisons between the proposed method and the methods in Table 1 are presented. This led to six comparisons, five in previous work in this paper + one proposed. It is the highest accuracy compared to those results reported in related literature to identify attack and non-attack of various cyber-attacks in cloud environment.

Table 1. Provides a summary of the work results related to the five methods for the CE-CIC-2018 dataset

Authors	Methods	Accuracy	Recall	Precision
[29]	LSTM+AM	96.00 %	95.00 %	75.00 %
[30]	AE + ANN	76.88 %	75.74 %	80.22 %
[31]	PTDAE+DNN	95.79 %	95.15 %	95.19 %
[32]	SFDO-RNN+FCM	95.22 %	95.42 %	96.82 %
[33]	PCA+SMO-FCM + AE	95.00 %	95.00 %	94.00 %

4. METHODOLOGY

The proposed approach uses a deep learning algorithm and a hybrid method. Dimensionality reduction using PCA, using the Fuzzy C-Means (FCM) technique to create clusters, and the deep learning-based AutoEncoder (AE) method are combined to identify an attack (utilizing just the packet data that the attack cluster contains). PCA + FCM + AE are the name of the suggested model. Prior to pre-processing, the raw data is checked for any missing data, and the output is then used to normalize the numbers so that they may be handled effectively in the succeeding steps. The clustering algorithm will struggle with a dimensionality issue because the normalized data include many fields. Clustering gets challenging when the number of dimensions is big. Therefore, there strategies to deal with the dimensionality problem: either only selecting the most crucial features, or extracting all the features into reduced amount of fields. Here, the proposed model has taken the approach PCA + FCM + AE in order to take into account each field's values. The deep learning-based (AE) will generally produce accurate results, but processing a result in the cloud environment will take longer. After that taking into account extreme conditions, attack discovery should happen faster and categorization should be accurate in a cloud environment. The (AE) classifies the traffic data using only the attacked traffic data after the attack detection is separated out more quickly using the Fuzzy C-Means (FCM) procedure. Because we are feeding the AutoEncoder with fewer rows, the application will result in a quicker classification with more accuracy, as presented in Figure 4.

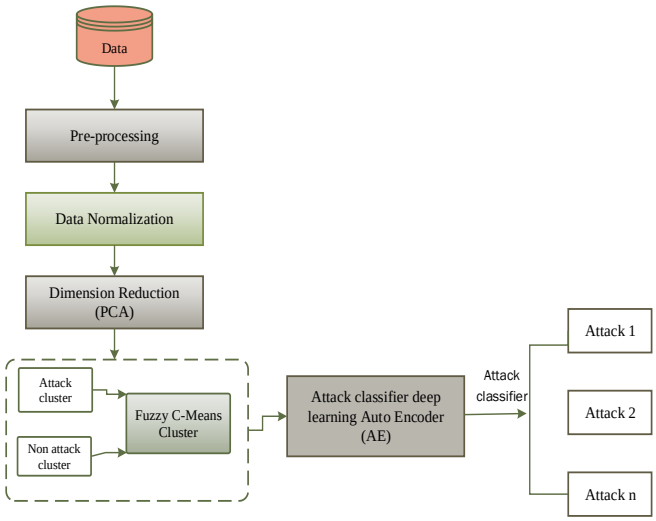

Figure 4. Proposed architecture for PCA + FCM + AE attack classifications

4.1 Dataset

The Canadian Institute for Cybersecurity (CIC) (91) and the Communications Security Enterprise (CSE) collaborated to build the CSE-CIC-IDS2018 dataset in order to overcome deficiencies in previously available datasets. The datasets provided by CIC are used worldwide for security testing and malware prevention in cloud cyberattacks [34]. The data includes various types of attacks including Heart bleed, Botnet, DoS, DDoS, Web Attacks, Botnet almost more than 92 % of the attacks are on the mentioned dataset, under license.

License: http://www.unb.ca/cic/datasets/ids-2018.html

4.2 Pre-processing of data

The first stage in the process is to train the algorithm to take into account the desired samples or the characteristics of both users and Distributed Denial of Service (DDoS) attackers. Pre-processing's goal is to give the incoming data traffic a meaningful shape so that the classifier can use it laterite relevant features are first extracted from the raw data, and those with symbolic values are then transformed into numeric values with ranges 0, 1.

4.3 Normalizing features

Now that we have examined the data, we can see that the values in the various fields fall within various min and max ranges. When this is analyses, the complexity increases. Therefore, a transformation is necessary set the minimum and maximum ranges in the pre-processed data table. The term "normalization" refers to the development of transforming data within a predetermined array based on its novelty. Here, for performing the normalization, the minimum value is 1 and the maximum value is 1. As inputs for a dimensionality reduction, these normalized data are provided.

4.4 Reduction in dimension

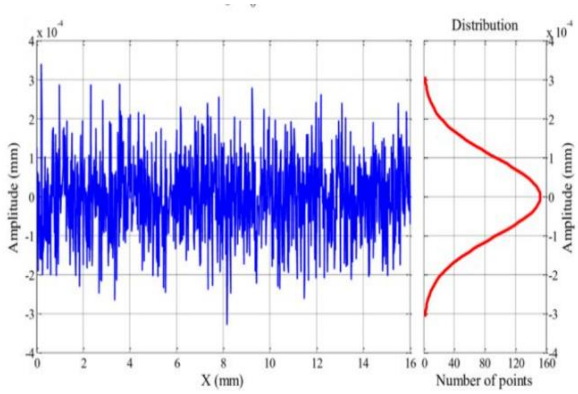

Figure 5. Gaussian noise

An examination of principal components Being able to show the internal structure of data and provide an explanation for variation in the data makes it a well-established machine learning technique that is often employed in exploratory data analysis. PCA analyzes data that has several variables in it. It searches for relationships between variables and ascertains which range of values best reflects the variations in outcomes. Principal components are a more condensed form of feature space that is created using these combined feature values. Every new input is examined to look for irregularities. Along with the normalized reconstruction error, the anomaly detection algorithm computes its projection onto the eigenvectors. The abnormality score is calculated using the standard error. The instance is more abnormal the larger the fault. Reducing the dimensions of a dataset may also be suitable in cases where its variables are noisy. A data set containing independent and identically distributed Gaussian noise in each of its columns (Figure 5) will also contain similar Gaussian noise in those columns, which may have a similar form. The first few components achieve the highest signal-to-noise ratio, so PCA can have the effect of focusing much of the signal into the first few principal components, which can

be usefully captured by dimensionality reduction. However, as the total variance in the first few principal components increases relative to the same variance in the noise, the relative influence of the noise is smaller. However, later important components might be overpowered by noise and removed with little loss.

Principal Components Analysis (PCA) is a helpful exploratory data analysis technique that enhances the display of variation in a multivariate data collection. A reduced set of main components is obtained by converting a set of covariates to get this improved visualization. The principal component can be considered the direction in which there is the greatest amount of variance.

5. MODULES FOR CLUSTER FORMATION

Each packet's feature's degree of fuzzy was used as the basis for the Fuzzy C-Means cluster that was created from the dimensionality-reduced data. A comparable cluster will be created using a similar fuzzy degree. The suggested method in this article uses various learning percentages from 75% to 95%, with a step value of 25%. The cluster's overall learning rate is represented by this learning percentage. The number of clusters is set to two, with one cluster being an attack cluster and the other the non-attack cluster. A first packet will be put in one of the clusters if it is being received.

5.1 Fuzzy C-Means (FCM)

One such fuzzy clustering method that allows data points to belong to many groups is the Fuzzy Clustering Method (FCM)] [35]. Its objective is to reduce the objective function, which is calculable utilizing Eq. (1):

$$\text{Jm}=\sum_{a=1}^{n}\sum_{b=1}^{c}\ \mu ab\ \ pd2 \qquad (1)$$

where, p determines how much overlap there is between clusters. Smaller values of p indicate less overlap, and it is typically greater than 1. In this study, p equals 2, where μab is the percentage of the *ath* multi-dimension measured data that is included.

The n and c are the number of pixels and classes in a particular image, respectively; dab is the distance between the *ath* measured data and the *bth* cluster center *cb*; and p is the position of the pixel in the *bth* cluster.

$$\mu\text{ab}=\frac{1}{\sum_{m=1}^{c}(dab/dam)^{\frac{2}{p-1}}} \qquad \text{cb}=\frac{\sum_{a}^{n}\mu ab\ xa}{\sum_{a=1}^{n}\mu ab} \qquad (2)$$

where, *ath* measurement data are *xa.* The iteration will end when the difference in the objective function between two successive iterations is not substantial. This value in the study was set to 1e-5. The maximum iteration period was predefined at 100 to prevent the iterative death loop and to reduce computational time [36].

6. MODULE FOR ATTACK CLASSIFICATION

A deep learning-based classifier called the AutoEncoder has been given the one of the cluster's data points for the reduced dimensionality assault. While data is presented in a clustered manner, this AutoEncoder gives reliable results and works well with data that has fewer dimensions [37].

An essential component of Deep Learning (DL) techniques is the autoencoder, which is a tool for taking inputs and transforming them into a new representation. Unsupervised machine learning is a topic in which autoencoders are highly helpful. They can be applied to decrease the dimensionality and compress data.

Reconstructing the input from the encoding serves to validate and improve the encoding. AutoEncoder is an unsupervised learning method. It learns the effective data representation (encoding) by training the neural network to ignore the "noise" signal. Figure 6 provides a diagrammatic representation of how the Denoising AutoEncoder is works.

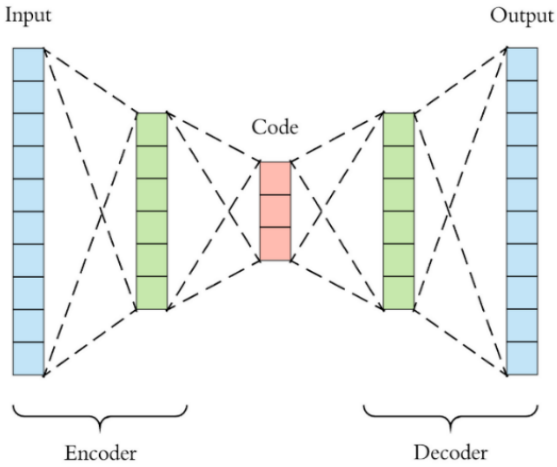

Figure 6. AutoEncoder workflow

AutoEncoder noise reduction the working principle of this aim is to understand how to restore the original, undistorted input by using a partially damaged input. An effective tool for data analysis and compression is AutoEncoder. They can be utilized to find hidden patterns in your data, which you can then utilize to condense the original data into a smaller form. This can be useful when working with data sets that are inconveniently large or when you want to check the distribution of different classes within your data. PCA is used to identify important features in a data set that are more suitable for displaying data with maximum variance than high-dimensional data. AutoEncoder are useful for compressing data and reducing its dimensionality.

7. RESULT AND DISCUSSION

Using the CE-CIC-2018 dataset, which contains seven distinct attack scenarios, the suggested solution (PCA + FCM + AE) is integrated into a deep learning-based attack identification system: to achieve the best accuracy, use brute-force, heartbleed, botnet, doS, DDoS, and web attacks. Using Principal Component Analysis (PCA), the Fuzzy C-Means (FCM) technique to create clusters, and the deep learning-based AutoEncoder (AE) method combined to identify the attack and non-attack. PCA + FCM + AE method prevents different cyberattacks. The result and analysis led to the creation of six comparisons, five existing + one proposed.

The results of our proposal method as shown in Figure 7 the results for accuracy of 97.70%, a recall rate of 96.26%, and a Precision of 97.00%. It is the highest accuracy compared to those results associated with the five methods.

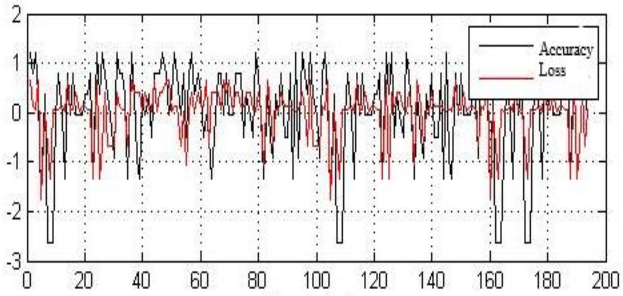

Figure 7. Accuracy of the proposed method

8. EVALUATION METHOD

This study evaluated the accuracy of the suggested strategy by looking at four factors: the number of correct and wrong findings. True positive (TP) refers to the quantity of benign samples that are accurately categorized; False positive (FP): the quantity of false positives that will outweigh the quantity of samples thought to be benign; Attack samples that are successfully identified as true negatives (TN) and false positives (FN), on the other hand, are the number of false positives that are anticipated to be attack samples.

With these four components, three indicators can be computed to assess the accuracy, recall, and accuracy performance of the recommended approach. The percentage of correctly identified data from various electronic threats in a cloud environment is known as accuracy.

$$\text{Accuracy (attack classification)}=\frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$\text{Recall (attack classification)}=\frac{TP}{TP+FN} \quad (4)$$

$$\text{Precision (attack classification)}=\frac{TP}{TP+FP} \quad (5)$$

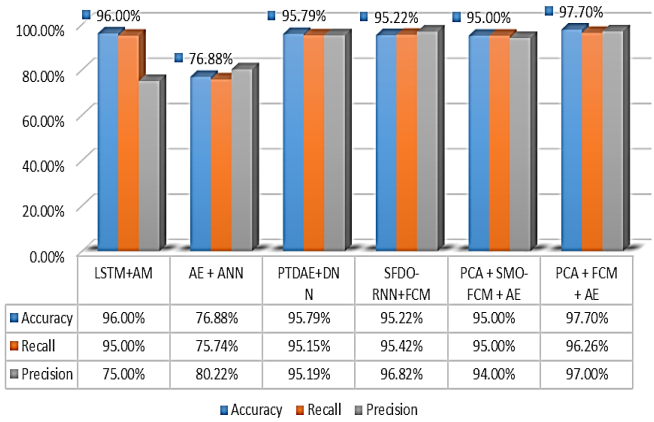

Figure 8. Compare five methods with our proposed method

In Figure 8 the critical evaluation and analysis for six methods, LSTM+AM, AE + ANN, PTDAE+DNN, SFDO-RNN+FCM, PCA+SMO-FCM + AE and our PCA+FCM+AE proposed method and the result was accuracy of 97.70%, a recall rate of 96.26%, and an precision of 97.00%. It is the highest accuracy compared to the results of the six methods. These results and analysis contribute to improving the precision of improving contemporary performance measurements and identifying different types of threats in a cloud environment.

9. CONCLUSIONS

The Cyberattacks are becoming more complex and frequent; this increases the importance of governments, cybersecurity institutions, and even users in their homes adopting advanced solutions. Here comes the role of artificial intelligence, which has changed the way we defend ourselves against cyberattacks. Machine learning methods excel at behavioral analysis, identifying patterns and bugs, and enabling governments and security organizations to analyses massive amounts of data to detect previously unknown threats or potential attacks. Machine learning algorithms learn from old data and adapt to new attack indicators, which suggest that their accuracy will improve over time as artificial intelligence models continue to develop to strengthen their security defenses and anticipate evolving threats. The valuable proposed PCA+FCM+AE method achieved the highest accuracy in positive parameters, such as 97.70% accuracy, 96.26% recall rate, and 97.00% accuracy for the work results related to DL methods of CSE-CIC-IDS2018 dataset.

REFERENCES

[1] Achbarou, O., El kiram, M., El Bouanani, S. (2017). Securing cloud computing from different attacks using intrusion detection systems. International Journal of Interactive Multimedia and Artificial Intelligence, 4(3): 61-64. https://doi.org/10.9781/ijimai.2017.439

[2] Nazeeh, I., Hadi, T.H., Mohammed, Z.Q., Ahmed, S.T., Kadhim, Q.K. (2023). Optimizing blockchain technology using a data sharing model. Indonesian Journal of Electrical Engineering and Computer Science, 29(1): 431-440. https://doi.org/10.11591/ijeecs.v29.i1.pp431-440

[3] Saran, M., Yadav, R.K., Tripathi, U.N. (2022). Machine learning based security for cloud computing: A survey. International Journal of Applied Engineering Research, 17(4): 332-337. https://doi.org///dx.doi.org/10.37622/IJAER/17.4.2022.332-337

[4] Bo, P., Fenzhen, S., Yunshan, M. (2020). A cloud and cloud shadow detection method based on fuzzy c-means algorithm. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 13: 1714-1727. https://doi.org/10.1109/JSTARS.2020.2987844

[5] Nassif, A.B., Talib, M.A., Nasir, Q., Albadani, H., Dakalbab, F.M. (2021). Machine learning for cloud security: A systematic review. IEEE Access, 9: 20717-20735. https://doi.org/10.1109/ACCESS.2021.3054129

[6] Khadhim, B.J., Kadhim, Q.K., Shams, W.K., Ahmed, S.T., Alsiadi, W.W. (2023). Diagnose COVID-19 by using hybrid CNN-RNN for chest X-ray. Indonesian Journal of Electrical Engineering and Computer Science, 29(2): 852-860. https://doi.org/10.11591/ijeecs.v29.i2.pp852-860

[7] Kosmopoulos, P., Dhake, H., Melita, N., Tagarakis, K., Georgakis, A., Stefas, A., Vaggelis, O., Korre, V., Kashyap, Y. (2024). Multi-layer cloud motion vector forecasting for solar energy applications. Applied Energy, 353(PB): 122144.

https://doi.org/10.1016/j.apenergy.2023.122144
[8] Temitope, O., Awodiji, T., Ayoola, F., Aderonke, D., Tosin-Amos, A., Owoyemi, J. (2023). Stop cyber attacks before they happen: Harnessing the power of predictive analytics in cybersecurity. Journal of Multidisciplinary Engineering Science and Technology, 10(April): 15863-15874. https://www.researchgate.net/publication/370414664
[9] Lata, S., Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. International Journal of Information Management Data Insights, 2(2): 1-14. https://doi.org/10.1016/j.jjimei.2022.100134
[10] Farahzadi, A., Shams, P., Rezazadeh, J., Farahbakhsh, R. (2018). Middleware technologies for cloud of things: A survey. Digital Communications and Networks, 4(3): 176–188. https://doi.org/10.1016/j.dcan.2017.04.005
[11] Nizamudeen, S.M.T. (2023). Intelligent intrusion detection framework for multi-clouds–IoT environment using swarm-based deep learning classifier. Journal of Cloud Computing, 12(1): 134. https://doi.org/10.1186/s13677-023-00509-4
[12] Belal, M.M., Sundaram, D.M. (2022). Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. Journal of King Saud University - Computer and Information Sciences, 34(10): 9102–9131. https://doi.org/10.1016/j.jksuci.2022.08.035
[13] Alata, M., Molhim, M., Ramini, A. (2008). Optimizing of Fuzzy C-Means clustering. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2(3): 670-675.
[14] Ahmed, S.T., Kadhem, S.M. (2022). Early Alzheimer' s disease detection using different techniques based on microarray data: A review. International Journal of Online & Biomedical Engineering, 18(4): 106-126. https://doi.org/10.3991/ijoe.v18i04.27133
[15] Ahmed, H.A.S., Ali, M.H., Kadhum, L.M., Bin Zolkipli, M.F., Alsariera, Y.A. (2017). A review of challenges and security risks of cloud computing. Journal of Telecommunication, Electronic and Computer Engineering, 9(1-2): 87-91.
[16] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Ali Al-shami, S.S., Selamat, S.R. (2018). A review study on cloud computing issues. In Journal of Physics: Conference Series, 1018: 012006. https://doi.org/10.1088/1742-6596/1018/1/012006
[17] Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6): 1-42. https://doi.org/10.3390/electronics12061333
[18] Dunn Cavelty, M., Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. Journal of European Public Policy, 30(7), 1330-1352. https://doi.org/10.1080/13501763.2023.2173274
[19] Alqahtani, K.S., Albalawi, A.M., Frikha, M. (2023). Reviewing of cybersecurity threats, attacks, and mitigation techniques in cloud computing environment. Journal of Theoretical and Applied Information Technology, 101(6): 2058-2066.
[20] Cartwright, A., Cartwright, E., Edun, E.S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers and Security, 131(10): 1-15. https://doi.org/10.1016/j.cose.2023.103288
[21] Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization, 12(June): 100268. https://doi.org/10.1016/j.rico.2023.100268
[22] Mijwil, M.M., Salem, I.E., Ismaeel, M.M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal for Computer Science and Mathematics, 4(1): 87-101. https://doi.org/10.52866/ijcsm.2023.01.01.008
[23] Dai, D., Boroomand, S. (2022). A review of artificial intelligence to enhance the security of big data systems: State-of-art, methodologies, applications, and challenges. Archives of Computational Methods in Engineering, 29(2): 1291-1309. https://doi.org/10.1007/s11831-021-09628-0
[24] Wu, Y., Wei, D., Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020: 8872923. https://doi.org/10.1155/2020/8872923
[25] Rajput, A., Gupta, P., Ghodeshwar, P., Varma, S., Sharma, K.K., Singh, U. (2023). Study of cloud providers (Azure, Amazon, and Oracle) according to service availability and price. In 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), pp. 1177-1188. https://doi.org/10.1109/ICPCSN58827.2023.00200
[26] Safaei Pour, M., Nader, C., Friday, K., Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. Computers and Security, 128: 103123. https://doi.org/10.1016/j.cose.2023.103123
[27] Amjad, A., Alyas, T., Farooq, U., Tariq, M.A. (2019). EAI endorsed transactions detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems, 6(23): 1-8. https://doi.org/10.4108/eai.29-7-2019.159834
[28] Xin, R., Liu, H., Chen, P., Zhao, Z. (2023). Robust and accurate performance anomaly detection and prediction for cloud applications: A novel ensemble learning-based framework. Journal of Cloud Computing, 12(1): 7. https://doi.org/10.1186/s13677-022-00383-6
[29] Lin, P., Ye, K., Xu, C. Z. (2019). Dynamic network anomaly detection system by using deep learning techniques. In Cloud Computing–CLOUD 2019: 12th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, pp. 161-176. https://doi.org/10.1007/978-3-030-23502-4_12
[30] Gamage, S., Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 169(6): 10-27. https://doi.org/10.1016/j.jnca.2020.102767
[31] Kunang, Y.N., Nurmaini, S., Stiawan, D., Suprapto, B.Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. Journal of Information Security and Applications, 58: 102804.

https://doi.org/10.1016/j.jisa.2021.102804
[32] Srinivas, B.V., Mandal, I., Keshavarao, S. (2022). Virtual machine migration-based intrusion detection system in cloud environment using deep recurrent neural network. Cybernetics and Systems, 19(9): 1-21. https://doi.org/10.1080/01969722.2022.2122008
[33] Balajee, R.M., Jayanthi Kannan, M.K. (2023). Intrusion detection on AWS cloud through hybrid deep learning algorithm. Electronics, 12(6): 1-21. https://doi.org/10.3390/electronics12061423
[34] Dittakavi, R.S.S. (2022). Dimensionality reduction based intrusion detection system in cloud computing environment using machine. International Journal of Information and Cybersecurity, 6(1): 62-81.
[35] Yu, B., Zheng, Z., Cai, M., Pedrycz, W., Ding, W. (2024). FRCM: A fuzzy rough c-means clustering method. Fuzzy Sets and Systems, 480: 108860. https://doi.org/10.1016/j.fss.2024.108860
[36] Ben Braiek, H., Khomh, F. (2023). Testing feedforward neural networks training programs. ACM Transactions on Software Engineering and Methodology, 32(4): 1-16. https://doi.org/10.1145/3529318
[37] Priyatharishini, M., Devi, M.N. (2022). A deep learning based malicious module identification using stacked sparse autoencoder network for VLSI circuit reliability. Measurement, 194(5): 11-55. https://doi.org/10.1016/j.measurement.2022.111055