DOI: 10.21917/ijct.2022.0420

SECURITY AND PRIVACY CONCERNS OF INTERNET OF THINGS (IOT) IN THE CLOUD

M.R. Sheeba[1], G. Suganthi[2] and R. Jemila Rose[3]
[1]*Department of Computer Science, St. Xavier's College, India*
[2]*Department of Computer Science, Women's Christian College, India*
[3]*Department of Artificial Intelligence and Data Science, St. Xavier's Catholic College of Engineering, India*

Abstract

The term Internet of Things is used to describe a wide range of web-enabled services and products, including cutting-edge gadgetry. To put it simply, cloud computing is the method of making information and software normally housed on separate local servers available to consumers through the Internet on demand. Cloud services mediate between IoT devices and the applications that control them. Because of this, essential data may be easily accessed without the need for costly infrastructure. The cloud based IoT paradigm connects the virtual and real realms. Two devices need to check their identities against each other before they can exchange data. Creating a one-of-a-kind identifier for every piece of electrical equipment; this might be a number or a name A person's right to privacy has been violated because this data can be used to harm them. Therefore, the suggested system will only store essential information about the user. If you want to keep the exam's identifiers secret, you should choose a method that leaves no paper trail. Therefore, protecting the privacy of users is so crucial. Viruses and other malicious software pose a significant risk to your network and the data it contains. Many IoT applications necessitate the construction of a distributed, scalable, and geographically dispersed datacenter network to meet the demands of their users. The providers of the desired information services are the ones responsible for automating the extensive data classification, analysis, and processing. Protective measures should ideally be handled by the security service desk. Using current approaches exposes too much data and services to risk. The goal of this completely new layout is to create a framework that can't be harmed by environmental elements in any way.

Keywords:

Privacy, Internet of Things, Cloud, Security

1. INTRODUCTION

In the context of the Internet of Things, Internet Protocol (IP) serves as a mediator for the communication that takes place between the internet and the many sensors and endpoints that make up the IoT. As one illustration, the internet of things has the potential to be utilized in the field of healthcare to facilitate remote monitoring, early diagnosis, treatment, and prevention [1]. Furthermore, the Internet of Things made it possible to equip things or people with sensors and actuators, such as radio-frequency identification (RFID) tags, in order to monitor and record data. Internet of Things applications make it possible to read, identify, recognize, and operate RFID tags that are attached to patient personal medical devices. These capabilities were not previously available.

The degree to which machines, humans, dynamic systems, and intelligent devices are all ingeniously connected to one another is directly related to the degree to which a healthcare system is efficient. The Internet of Things may be broken down into three primary layers, which are the network layer, the perception layer, and the application layer. Each of these layers is responsible for a different function within the overall system. The perception layer mission is to compile information regarding the state of the patient health from a wide variety of diverse sources. The network layer is in charge of processing and transmitting the input that was obtained from the perception layer. This layer is made up of wired, wireless, and middleware systems. If they are constructed properly, transport protocols have the potential to lessen the pressure placed on the network, cut the amount of electricity that is consumed, and protect the personal information of users [2].

The application layer is in charge of integrating a wide range of medical data sources and delivering tailored medical care to the end user. In addition, this layer is accountable for maintaining the security of the data. When working with the Internet of Things (IoT), the most important thing to keep in mind is protecting the privacy of patient information and ensuring that it is secure [3]. If data is stored and sent in a secure manner, all of its attributes, including its authenticity, integrity, and validity, can be preserved. This safeguards the data in all three of its dimensions. When only those individuals who are permitted to view the data are able to do so, the data confidentiality is preserved.

It is possible to establish appropriate safety precautions if the essentials, the goals, and the requirements are taken into consideration. It is crucial that sensitive personal data be kept private, even when widespread usage of Internet of Things devices has the potential to improve patient care [4]. As the number of attacks on next-generation systems has increased, the gadgets that make up the Internet of Things are increasingly vunerable to dangers that are both unidentified and already well-established.

As data travels from the Internet of Things to the cloud and the visualization domains, it goes through a process of transformation at several levels of the structural hierarchy of the cloud. Traditional security solutions, such as those that rely on signature or machine-learning approaches, would have a difficult time keeping up with the current situation because of the enormous number of attacks that are being launched that are unknown to the system.

Deep neural networks (DNNs), also known as convolutional neural networks, are a type of artificial neural network. DNNs may be able to detect flaws in virtualized communication networks with more accuracy. Getting to this point requires first gaining the ability to detect the regular data flow, and then recreating it.

2. RELATED WORKS

When developing the model that is currently being used to protect the privacy of cloud users, the authors of [5] made use of

the most cutting-edge AI techniques available to do so. This methodology places a high value on the process of cleaning the data as well as the procedure of restoring it, therefore both of these steps are regarded to be key components. During the sanitization process, a hybrid metaheuristic called as Jaya-based shark smell optimization (often abbreviated as J-SSO) is used. This is done in order to obtain an acceptable key. In order to generate the best key feasible, a multi-objective function was utilized. This function took into account a variety of characteristics, including the percentage of the information that was hidden, the degree to which it was altered, and the percentage of the information that was preserved.

We take note of the development of a biometric-based user authentication system (SAB-UAS) in [6], which protects the confidentiality of healthcare communications without invading the user right to personal privacy. The research revealed that a fraudulent user does not behave in the same manner that a genuine user does while accessing or canceling a portable smart card. This was shown to be the case by the findings. The findings substantiated this assertion. An innovative approach to protecting patient privacy inside healthcare systems that are based on the Internet of Things is detailed in the article [4]. If an adversary were to only use the client public key, it would be difficult for them to determine the valid status counter of the record because of the trapdoor permutations that were introduced. This is a result of the utilization of the trapdoor permutations that were implemented.

In order to increase the performance of the model, the authors of the paper [7] created a deep residual network and made a few modifications to it. In addition to this, the authors of the study offered a technique for identifying human behaviors within the IoT cloud. Users will be able to construct scenarios based on the activities that make up their usual day with this feature. The group came to the conclusion that the best approach would be to build an architecture known as function as a service (FaaS), which meant that each function would execute in its very own container. The scalability issue was addressed by doing this in order to resolve it.

In order to find a technique to securely keep the medical records of patients on a cloud server for the purpose of further analysis, the authors of the study [8] devised the technology that is currently referred to as privacy-preserving disease prediction (PPDP). The single-layer perceptron learning method was utilized in order to bring about an improvement in the accuracy of the prediction models.

In reference, an intelligent Internet of Things (IoT) model for healthcare diagnostics is presented. This model is supported by an optimal deep learning-based secure blockchain (ODLSB). This architecture was essentially made up of three essential parts: medical diagnostics, encrypted hash value transactions, and secured finance transactions.

In [9], it was hypothesized that fractional-order chaotic systems with fluctuating order may be synchronized with one another. In order to realize synchronization between the response system and the fractional-order drive system, the Lyapunov stability theory was put into practice. With the assistance of N-shift encryption, crucial data signals can be encrypted as well as decrypted. This encryption method is utilized in both processes. Through the utilization of simulation, the practicability of the theoretical method was demonstrated and confirmed.

We gain knowledge of a mechanism for the transmission of data in the industrial IoT that makes use of Fabri-C block chains to safeguard the data integrity and privacy in reference. This information is made available to us by [10]. This strategy makes use of the technology known as a decentralized ledger, which makes it possible for participants to engage in an information exchange in a more fluid manner. Because of this method, there is an increase of 13% in both the rate at which packets are transmitted and the rate at which they are received, making the respective increases a total of 12%. The use of this method could be extremely beneficial in a number of different areas, including decentralized administration and sharing.

Utilizing a crypto-deep neural network increased the efficiency of a decentralized outsourcing technique that was previously used by [2]. This strategy requires the deployment of a web server, as well as cloud and data center agents, in addition to a cloud server. defense against attacks that involve impersonalization that is based in the cloud, cryptography, and neural networks (CDNNCS). The results of CDNNCS showed an improvement of approximately 5% in response time when compared to the method that is currently being used, as well as a reduction of approximately 10% in the amount of packets that were lost. Both of these improvements were achieved in comparison to the method that is currently being used.

A hierarchical fuzzy neural network was trained with the help of a two-stage optimization strategy in [5], and the network low-level parameters were learned with the help of a model based on the well-known method of alternating-direction multipliers. Both of these methods conceal the local data from any other agents who may access them. Utilizing a technique that is faster and more convergent in its optimization is done so in order to create greater coordination at higher levels of the hierarchy. Problems with the gradient vanishing, such as those found in backpropagation models, do not have an impact on scalability or runtime. The application of classification and regression strategies, both of which were found to be effective through simulation, was done with the intention of demonstrating the effectiveness of the proposed strategy.

The authors in [1] has suggested a data analytics and privacy protection system for the Internet of Things (IoT)-enabled healthcare industry. At the core of this system is deep learning, which is designed to safeguard patient personal information. The user is the one who collects the raw data, and the user private information is stored in a different location, completely out of the public eye. To undertake analyses of data relevant to a variety of health-related topics, convolutional neural networks (CNNs) are deployed on the cloud, where sensitive user information and security issues are not a worry. Using experiments, it was possible to demonstrate both the efficiency and the robustness of the system. To solve the problem of finding an optimal strategy for sending packets with varying buffer sizes over multiple channels while maintaining high throughput, a novel Q-learning-based transmission process for scheduling was developed. This was done in response to the challenge of finding an optimal strategy. Deep learning applied to the Internet of Things was important in this task successful completion. In order to characterize the transitions in state that the system experiences, a computational

method that is utilized is one that is founded on the Markov decision process. This method use is the reason that it is employed. This new method of packet transmission consumes less energy than the previous method did and, as a result, there is no loss of packets.

Users can have faith in the approach that is offered to them in [24] for the intelligent administration of clouds. This strategy is presented to us in the article. The trust approach of an open wireless medium required the development of a technique for updating the trust cloud so that it could be handled in a manner that was both flexible and intelligent. A trust cloud was utilized in order to successfully complete this task. The fact that detection accuracy for counterfeit devices was effectively increased is evidence of the efficacy of this method in bringing uncertainty into trust concerns. This is evidenced by the fact that there are now less trust worries. It is feasible, with the assistance of a convolutional neural network, to identify whether a fastener has become damaged or has just fallen loose (CNN). Extensive experimental testing has shown that this method is both successful and efficient, which supports the conclusion that it should be used. When compared to the physical operation, this method achieves an average precision and recall that is 95.38% and 98.62%, respectively, thanks to the utilization of a speedy detecting mechanism.

3. PROPOSED WORK

Intruder detection systems, or IDSs, are security systems that automatically monitor and defend a host or network by finding and analyzing any activity that may be malicious or suspicious. Continuously monitoring and defending against threats is something they do. The security flaw was discovered by the use of an easy method of intrusion detection. In particular situations, it specifies the kinds of evidence that must be submitted, in addition to the procedures that must be followed in order to acquire it. An anomaly that exists within a computer network or system and poses a threat of data theft or corruption is referred to as an incursion. An irregularity, also known as an anomaly, is any deviation from the norm that takes place inside the system. In today society, it is normal practice to send and preserve secret information through the use of the Internet and other networks. According to the information that is shown in the intrusion detection systems are a type of cybersecurity application that are utilized by firewall and antivirus software.

In addition, the firewall will only perform a superficial analysis of the websites that you go to in its monitoring of your activity. IDSs are able to regulate, monitor, and maintain all traffic on networks; yet, they will nonetheless raise an alarm if they detect any suspicious activity or an attempt to attack the networks. This is because IDSs are able to maintain and regulate all traffic on networks. Even if intrusion detection systems (IDSs) are able to manage, monitor, and maintain all traffic on networks, this will still be the case.

These three aspects of IDSs are the primary components that can be dissected individually. In the second part of the procedure, the first thing that has to be done in order to evaluate and identify cyberattacks is to collect evidence data from the input data, and then process it. This must be done in order to go on to the next step of the procedure. In the third and last portion, the attacks, taken by themselves, are dissected in some detail.

When it comes to working with extremely large datasets, the performance of approaches based on deep learning is superior to that of approaches based on machine learning. Since they were first made available to the public, deep learning intrusion detection systems have moved quickly to the forefront of the industry, where they have fast established themselves as the gold standard. Deep learning, which is a subfield of machine learning, is employed in the subject of cybersecurity to an enormous degree. This is due to the fact that deep learning has the capability of uncovering hidden patterns even in data that has not been processed. It achieves this goal by repeatedly undertaking refinement, which ultimately leads to the identification of traits on a higher level.

All of the difficulties that are often connected with pattern recognition on enormous databases can be conquered through the application of deep learning. It accomplishes this by automatically picking the information that is most necessary for pattern recognition by employing a large number of hidden layers. This allows for greater accuracy. In contrast to the typical order in which feature extraction, training, and testing are carried out within the context of conventional machine learning, deep learning mandates that all of these processes be carried out simultaneously.

The structure of a feed-forward neural network serves as the basis for the development of models for use in deep learning. An input layer, a hidden layer or layers, and an output layer are the standard components that make up a deep learning architecture. Typically, a deep learning architecture will have all three of these components. It is possible to deduce some characteristics of the image by utilizing particular layers, which are typically referred to as hidden layers. The property vector that represents the input item is given to the input layer when it is processed. The word item is shortened to input. The generation of the class vector that will be utilized for the input vector is the responsibility of the output layer.

Backpropagation is a technique that is used in deep learning to adjust the weight values in order to reduce the cost function that is associated with learning. In order to facilitate the learning process, this step needs to be taken. The system begins by providing an input vector and weights, which are later utilized to evaluate the level of similarity between the actual output and the ideal output. This makes it possible to proceed to the next step of the procedure, which is to determine the error rate.

4. DATASET

The Information Security Center of Excellence came up with the idea for the DATASET ISCX IDS dataset in 2012. This was done with the intention of developing and researching various network intrusion and attack detection techniques. This was carried out with the purpose of preventing similar breaches in the future. It contains information regarding HTTP, FTP, SMTP, IMAP, SSH, and POP3 network traffic, in addition to the typical and abnormal behavior of these protocols (Inside attacks, DoS, DDoS, and Brute Force SSH).

The data are compiled over the course of one week. The datasets contain a total of 151,2 thousand tagged packets, each of

which has 19 characteristics and 17 attributes. In total, the datasets contain 151,2 thousand tagged packets. Researchers at the Lawrence Berkeley National Laboratory (LBNL) utilized uPMU to collect data on the incoming and outgoing traffic of two routers so that they could compile a dataset. This allowed the researchers to better understand the network. One hundred twenty hertz was the output frequency of the micro-phasor measurement device, which produced a total of twelve streams (Hz).

This sample of 79,000 transactions did not contain any unique flows of any kind. There were no surprises. Because labels solely describe application-level communication, there is no indication as to whether or not the traffic flow is normal or irregular. [13]. The Cyber Range Lab at the University of New South Wales in Canberra is in the process of developing a new Bot-IoT dataset with the intention of incorporating it into Internet of Things (IoT) networks.

The nearly 72,000,000 entries contain many kinds of attacks, such as denial of service, distributed denial of service, operating system, service scanning, data exfiltration, and keylogging. This category encompasses both regular traffic and traffic from botnets as well. In order to facilitate machine-to-machine (M2M) communication, the lightweight MQTT network protocol is deployed. In addition to that, the Node-RED tool is applied so that a simulation of the activities that are occurring within the network may be created.

5. RESULTS AND DISCUSSION

There has been a comparable increase in the relevance of network security as the number of programs and individuals that utilize networks continues to expand. Damage to the physical layer, device failure, and power limits are just a few examples of potential issues that could occur at the physical layer. Other potential issues include the failure of other devices. Denial-of-service attacks, sniffer attacks, gateway attacks, and unlawful access are a few examples of the types of issues that might arise at the network layer.

Other issues can also arise at this level. Even though a substantial number of devices connected to the Internet of Things have built-in self-defense mechanisms, these devices are nevertheless susceptible to a wide variety of dangers. The primary challenges that need to be surmounted by an Internet of Things system are the authentication issues that arise and the potential dangers that may be encountered.

At the network layer, there is a necessity for stronger privacy safeguards between the devices that make up the Internet of Things and the gateways that connect them. This requirement is in place because of the General Data Protection Regulation (GDPR), which went into effect in May 2018. The privacy of the information that is transmitted from one app or service to another is the topic of the next category of security concerns that should be addressed.

As soon as a network system is vulnerable to attempts at spoofing or noise, the integrity of the data begins to be jeopardized. Infrastructure and services related to the Internet of Things are susceptible to being penetrated by attacks that do not adhere to a recognized pattern. Denial-of-service attacks (DoS), distributed denial-of-service attacks (DDoS), and probing attacks are all included in this category. We are now going through the fourth set of factors to take into account when it comes to protecting the personal privacy of persons. The protection of user personal information is a crucial aspect of the security of the Internet of Things (IoT). An individual identifier is assigned to each device that is a part of the Internet of Things (IoT). This identifier is responsible for storing information regarding the thing owner as well as its present position and its prior locations [59, 60].

Using metrics such as accuracy, precision, recall, F measure, FAR, classification, and misclassification rate, this section provides a comprehensive analysis of deep learning algorithms for the detection and prevention of intrusions in preexisting systems and networks. These algorithms were evaluated for their ability to detect and prevent intrusions in preexisting systems and networks which is shown in Figure 1.

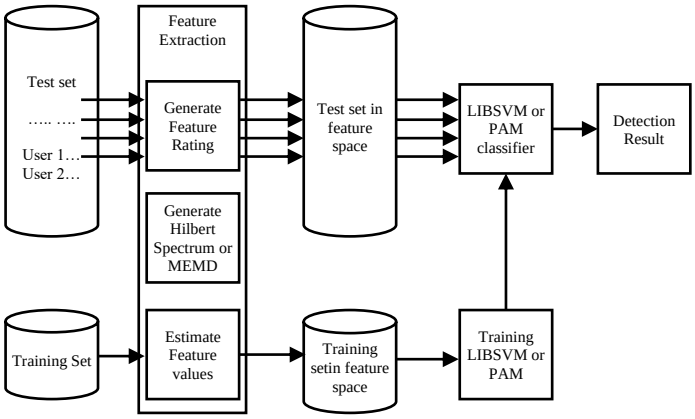

Fig.1. Proposed Model

In order to counteract the complex nature of today security-related networks and the rapid increase of threats, a new intrusion detection system (IDS) that is based on a deep neural network has been developed. The creation of the IDS allowed for the successful completion of this task. The strategy that has been outlined will make a direct attack on the problem of overfitting at some point in the future. IDS is in charge of organizing the dissemination of information regarding normal and abnormal behavior on the network. This is one of its primary responsibilities. The data that had been collected from KDD99 had been cleaned up and normalized with the assistance of the mean and the standard deviation.

Rectified linear unit (ReLU) and softmax are the activation functions that are utilized for the hidden layer and the final layer, respectively, because of the complex nature of the classification process. These activation functions are used for the hidden layer. The loss function that was produced through computing using the stochastic Adam optimizer was subjected to backpropagation when it was finished being created. After putting a variety of classifiers to the test, it was established that Softmax was the most effective in separating normal attacks from those that were not typical.

This conclusion was reached after testing a large number of classifiers. During the process of conducting the experimental assessment, it was discovered that the loss function was 0.005%, and that the correctness of the numerical data was 99.91%. The findings indicated that the accuracy and loss function for the mix data type were 99.78% and 0.015%, respectively. This work

evaluated the suggested method by applying various feature extraction strategies, with the goals of enhancing the system efficiency and maintaining its consistency.

The goal of this study was to establish the most effective method of putting the strategy into action. It was hypothesized that one of the tasks for deep image learning based on DCNN could be the detection, classification, and characterisation of anomalies. A mix of feature selection and model stacking was utilized to compile and present the results of this research. We compute the datasets with the help of CICFlowMeter to extract a total of 80 characteristics. Following the construction of a forest tree and the ranking of qualities that are used as CNN input, the top features are selected to produce two-dimensional grayscale images. A vector with the index 99 was produced in the model layers.

Changing attack patterns required for the development of a brand-new method, which led to the design of TSDL in response to those issues (two-stage deep learning) (two-stage deep learning). The strategy that is applied for NIDS is known as stacking autoencoders in conjunction with a softmax classifier. There are two different systems at play here. The value of the likelihood score is utilized in two different ways: first, it is used to determine if a record is normal or abnormal, and second, it is used as a secondary characteristic for recognizing both typical attacks and those that go beyond the typical range. This method learns feature representations from unlabeled data obtained at scale in an effective and efficient manner.

Evaluation on two datasets that are available to the public, which were used in the experimental inquiry, demonstrated a higher efficiency and recognition rate. The accuracy of the KDD99 dataset was proven to be 99.996%, whereas the accuracy of the UNSW-NB15 dataset was demonstrated to be 89.134%. According to the detailed assessment of the KDD99 dataset, out of the full number of records, 87785 have been accurately labeled as normal, while 53 have been wrongly categorized as abnormal. The total amount of records that were analyzed revealed that 57701 of them contained odd information, while 47 of them contained inaccurate classification.

There are a total of 145,586 records that might have been categorized, but only 145,486 were. Additionally, it was said that the two-class model had a precision of 99.93%, a recall of 99.93%, an F-measure of 99.93%, and a FAR (false alarm rate) of 0.0007%. These percentages were stated in that order. When the KDD99 dataset was tested using multi-class identification methods, 145,580 out of a total of 145,586 records were able to be correctly classified (including normal, DoS, U2R, Probe, and R2L) (including normal, DoS, U2R, Probe, and R2L). It was reported that the precision, recall, F-measure, and false alarm rate (FAR) for multi-classes were 99.99%, 99.99%, and 0.000015%, respectively. Precision was also reported to be 99.99%.

It was discovered that 108540 records were appropriately assigned to the normal class, whereas 15874 entries were mistakenly assigned to the abnormal class. This was discovered because of the research findingsset, it was discovered that 108540 records were appropriately assigned to the normal class, whereas 15874 entries were mistakenly assigned to the abnormal class. This was discovered because of the research findings.

A total of 103467 files were identified as potentially malicious, while another 8442 had the wrong label assigned to them. There was a total of 236.8 million files, but only 212,007 were able to be properly categorized. The purpose of this research was to develop and analyze multitasking and reinforcement learning strategies for DL in the hopes of improving the NIDS that were developed. A dynamic network security system that is both autonomous and intelligent has been designed in order to identify zero-day threats. This system was built specifically for this purpose.

The goal of the approach that has been suggested is to cut down on the quantity of work that must be done by hand. A convolutional neural network, a recurrent neural network, and a gated recurrent unit are some of the components that make up this hybrid approach (random forest) (random forest). The network packets generated by a single connection are stored, analyzed, and then features are extracted using software such as Snort and Bro IDS. Multiple classifiers, such as RNN, GRU, CNN, and RF, were used on the features, and their votes as well as the logic they generated were pooled to decide whether the traits were malicious.

The findings provide evidence that demonstrates how their method may automatically learn to recognize new harmful threats. On the other hand, in the future, the problem of incorrect attack classification will be solved through automatic learning. Experiments are carried out on the NSL-KDD dataset, and KDDTest+ and KDDTest- claim accuracy of 87.28% and 76.61%, respectively. While the training time and accuracy have both been increased, the scope of this research is still limited to non-real-time networks and attack types. This is even though training time and accuracy have both improved.

It was proposed that a fresh approach based on deep learning may be employed to cut down on the number of mistakes that are caused by the training process. The solution that has been recommended has two primary components: first, in the preprocessing step, redundant or unneeded data is deleted using a threshold-based ranking algorithm, which ultimately results in greater efficiency.

The Adam method fared better than the other optimization strategies that were evaluated. This research makes use of many approaches from the field of artificial intelligence to learn about sophisticated forms of attack and how to fight against them.

Table.1. Results

Attack	Accuracy	Precision	Recall	F-Measure
Random	0.69	0.74	0.78	0.81
Average	0.74	0.78	0.83	0.85
Bandwagon	0.79	0.82	0.87	0.88
Segment	0.83	0.86	0.895	0.905
Love/hate	0.865	0.89	0.91	0.92
Reverse bandwagon	0.89	0.905	0.92	0.935

6. CONCLUSION

Intrusion detection systems have progressed to address the challenge posed by the proliferation of expansive, high-dimensional Internet of Things (IoT) and network infrastructures. It is now very easy to use the various network apps that have been

developed and are readily available. It faces a great deal of difficulty in terms of dependability, privacy, secrecy, and protection of sensitive data. In this paper, a wide variety of different systems for detecting intrusions are dissected and analyzed. We have also conducted extensive research on deep learning-based intrusion detection systems (IDS) for network issues.

In this paper, we undertake a comprehensive study of the research on IDS methodology, sorts, and technologies. We analyze the advantages and disadvantages of these methodologies and technologies, as well as publicly available datasets that are based on networks. Accuracy, precision, recall, f-measure, false alarm rate, classification, and misclassification rate are just a few of the many performance metrics that are used to assess the efficacy of deep learning methods for intrusion detection and prevention in both traditional and networked settings. Other performance metrics include accuracy, which stands for false alarm rate, and classification, which measures how well a method classifies false positives and false negatives.

REFERENCES

[1] L.R. Waitman, X. Song and A.M. Davis, "Enhancing PCORnet Clinical Research Network Data Completeness by Integrating Multistate Insurance Claims with Electronic Health Records in a Cloud Environment Aligned with CMS Security and Privacy Requirements", *Journal of the American Medical Informatics Association*, Vol. 29, No. 4, pp. 660-670, 2022.

[2] U. Selvi and S. Puspha, "A Review of Big Data an Anonymization Algorithms", *International Journal of Applied Engineering Research*, Vol. 10, No, 17, pp. 13125-13130, 2015

[3] A. Ometov, "A Survey of Security in Cloud, Edge, and Fog Computing", *Sensors*, Vol. 22, No. 3, pp. 927-935, 2022.

[4] N. Li, T. Li and S. Venkatasubramanian, "T-Closeness: Privacy Beyond k-Anonymity and '-Diversity", *Proceedings of International Conference on Data Engineering*, pp. 106-115, 2007

[5] S. Carlin and K. Curran, "Cloud Computing Technologies", *International Journal of Cloud Computing and Services Science*, Vol. 1, No. 2, pp. 59-65, 2012.

[6] M. Ahmad, M. Chong and A. Hamid, "Enhancing Trust Management in Cloud Environment", *Proceedings of International Conference on Innovation, Management and Technology Research*, pp. 314-321, 2014.

[7] G.S. Sriram, "Resolving Security and Data Concerns in Cloud Computing by Utilizing a Decentralized Cloud Computing Option", *International Research Journal of Modernization in Engineering Technology and Science*, Vol. 4, No. 1, pp. 1269-1273, 2022.

[8] E.S. Hajji and T. Maha, "From Single to Multi-Clouds Computing Privacy and Fault Tolerance", *Proceedings of International Conference on Future Information Engineering*, pp. 112-118, 2014.

[9] J. Gong and N.J. Navimipour, "An In-Depth and Systematic Literature Review on the Blockchain-Based Approaches for Cloud Computing", *Cluster Computing*, Vol. 25, No. 1, pp. 383-400. 2022.

[10] C. Chandravathy, V. Kumar and G. Murugaboopathi, "Study on Cloud Computing and Security Approaches", *International Journal of Soft Computing and Engineering*, Vol. 3, No. 1, pp. 2231-2307, 2013.