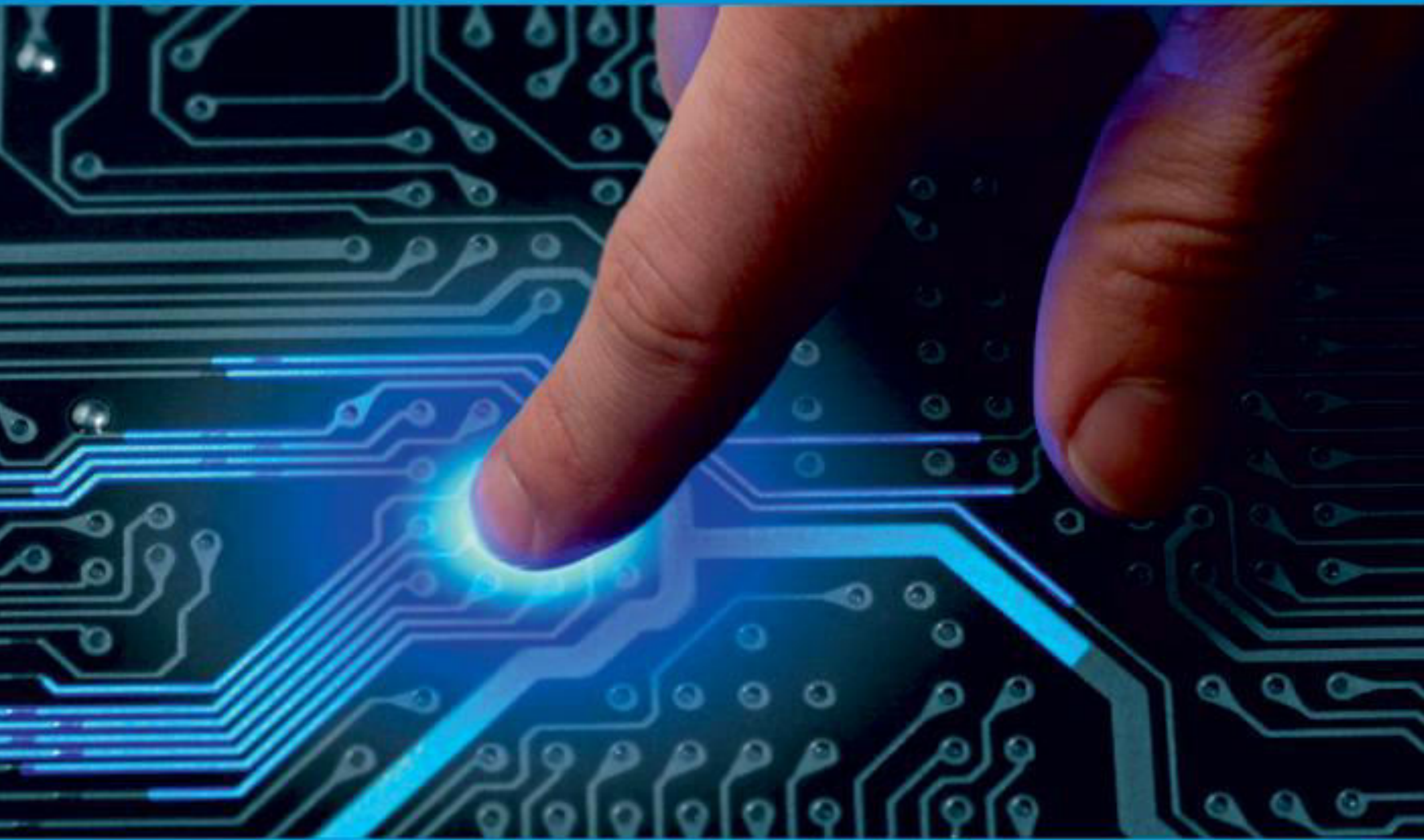
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 11, November 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

Intrusion Detection System in MCPS Using Artificial Neural Network

Alias Itten

Lecturer, Dept. of Computer Engineering, Govt. Polytechnic College, Kaduthuruthy, India

ABSTRACT: Medical Cyber Physical Systems (MCPS) is a digital medical device systems which integrate computationaland physical components effectively. MCPS is being used more and more in health sector settings in providing good quality care throughallowingactiveobserving and therapy. Security breaches, on the other hand, canthreatenthe privacy, security, and availabilityof healthcare devices while avoiding traditional measures like cryptography. In terms of damage and responsibility, this might have serious consequences for both the patient and the organization. Based on Artificial Neural Networks (ANN), we construct highly distributed, machine learning based Intrusion Detection System (IDS)in MCPS. In this study, an artificial neural lnetwork method is presented for effectively classifying the four main categories of network attack traffic identified in an efficiently pruned KDD dataset that develops through the elimination, classification, and prioritisation concentrating in the accuracy, space, and time. Theoutput shows that the proposed ANN technique has a greater detection rate and lesser false alarm rate. Finally, this technique has a precision rate and the recall rate is higher than the existing methods.

KEYWORDS: Machine learning, Artificial Neural Network(ANN), MCPS, Security, Intrusion Detection System (IDS).

I. INTRODUCTION

IDS have becomeextremelydifficultchallenge in the networking sector for several years (Wankhade and Jondhale, 2019). Intrusion detection is the observation of system events to identify behavior that breachesthesecurityprotocol ofthe system(Heckman, 2017).Anintrusiondetectionsystem(IDS)should evaluate massive amounts of data in real-time to identify and correlate events that reveal an attack is taking place. To identify malicious attacks, an intrusion detection system is essential. Data mining and machine learning approaches (Chauhan and Shukla, 2015) are critical in the identification of cyber-attacks.This technology (Bhuyan et al., 2014) can discover hidden patterns,detect intrusions, and provide a decision support system for intrusion detection systems (Denatious and John, 2012). Because of these factors, data mining and machine learning approaches are mainly significant in the field of IDS(Marchang et al., 2017).

Medical cyber-physical systems (MCPS) (Schneble and Thamilarasu, 2019) allow for the seamless integration of physical and computer components in life-serious, context-aware networked systems of medicinal equipment. MCPSis becoming increasingly popular in a variety of fields, including automobiles, aviation, and force systems, as well as manufacturing, human services, and discriminating foundations. (E.K. Wang, et al. 2010). On the other hand, as digital-physical systems become more prevalent and widely used in diverse and critical applications, they become increasingly vulnerable to security flaws and targets for digital-physical attacks. Systems (M. Alam et al. 2016) are long-promised technologies that seek to provide digital health care to patients by utilizing sensor data generated from Such body-worn devices. The information gathered by these devices could be kept in a private or public cloud and evaluated by medical officials later (O. Kocabas et al. 2016).

Classification of machine learning algorithm is prevalent while distinguishing between normal and abnormal. Deep learning approaches (J. P. Planquart 2001) such as Neural Network have recently been proved to be effective techniques for classifying different types of network attack risks. To produce promising results, neural networks are being integrated using clustering algorithms (W. Gang et al. 2010). In several research papers, variouspresent dataset is being utilizedin assessing the implementation of IDS utilizing neural networks. (S. K. Sahu et al. 2014). In this study, a neural network-based IDS is presented that evolves multi-class data to a 2-class issue afterclass prioritizing andclassification based data pruning to identify the four basic types of network attacks. We discuss some of the related works in Section 2 in detail. Section 3 defines the methodology of the proposed mechanism. In the Section 4 the result and performance evaluation are shown in detail. Finally, section 5, concludes with the conclusion.

II. RELATED WORKS

In this paper (Vigna and Kemmerer 1999) a new method to network intrusion detection that uses the State Transition

Analysis Technique (STAT) is described. State transition diagrams, which describe transitionsandstatesin a networked context, are used in model network-based invasions. A system based on hypergraphs is used to show the intended network environment. The method identifies that network measures must be observed and also where they're being examined using a formal system of both the network to be defended and the assaults to be spotted, giving provision for configurationautomaticallyand the assignment of intrusion detection elements.However, this method did not focus on the conclusion of the prototype and the improvement of its design.

According to this study, (Sharafaldin,etal.2018)since1998 over eleven public datasets, many data set is being out of service and undependablefor using. Certain datasets do not cover various attacks, and certain datasets lose volume and traffic diversity, where others anonymizeddata packets as well as payloads that could not replicatepresent trends and missing metadata andfeature sets. This study creates a trustworthy dataset with seven similar network attack flows that fit actual requirements that are available in public.The study compares the performancein a wide range of network machine learning methods as well astraffic metrics to determine which characteristics are effective for detecting specific attack types. However, the number of PCs must be increased in the future, and also more up-to-date attacks must be carried out.

The goal of this research (Hady, et al., 2020) is to demonstrate that integrating network and biometric measurements as characteristics outperform utilizing one of the two types of structures. We created anactual Enhanced Healthcare Monitoring System (EHMS) testbedwhich gathers metrics of the network flow as well as analyses patients' biometrics. Then the collected information is transferred into a distant server for more diagnosis as well as treatment. Cyber-attacks using man-in-the-middle techniques were deployed, and a dataset over sixteen thousand records of attack and normal healthcare informationis generated.After then, the method uses a variety of machine learning approaches to train and validate the dataset against such assaults. The findings show that skills have improved by 7% to 25% in some circumstances, demonstrating the suggested system's robustness in giving better intrusion detection. The findings, however, demonstrate that the system's efficiency isn't ideal, necessitating further examination.

This research (Siniosoglou, et al. 2021) offers a Federated Layered Architecture for use in MCPS Networks, which includes an establishment of various layers in aggregation to increase model training protection.Furthermore,twoDeepAdversarialNeuralNetworksisgivenforusingthedatafromtheMCPS surroundings.The networktrained in Federated system gets a higher capacity to notice possible intrusions in MCPSnetwork than generally trained networks, according to the assessment of the provided work. Our long-term goals in this area involve implementing a variety of Federated Training in DL modelsas well as supplementing them with the privacy-preserving strategies to make the process even safer.

In(You et al. 2018) lightweight specification-based misbehavior detection technique is proposed whichuses automatic model verification and formal verification to effectively and successfully detect misbehaviour of an IoT device fixed in a MCPS. With patient-controlled analgesia (PCA) device incorporated in a medical health monitoring system, the specification based misbehaviour detection method is being tested.The PCA device integrated with an MCPS where a peer PCA acts as a monitor node demonstrates the practicality of our suggested technique. The behavior instruction specification based misbehaviour detection method is situated as the only viable answer for protecting resource r eserved integrated IoT devices beside zero-day threats in terms of computation, run time, low memory, and communication overhead, as well as high misbehavior detection accuracyrate. This will be put to the test through experimental confirmation.

III. PROPOSED METHODOLOGY

While developing an effective Intrusion Detection System, there has always beena trade-off between accuracy, space, and time. If the total classes to be differentiated is increased, then the machine learning model's accuracy diminishes and the IDS gets slower. Again, ifthe total attributes is reduced, then the system's accuracy decreases where the IDS works quicker. Decreasing the amount of attributes isn't a smart planalways because different types of attacks could be categorized if it containsa large number of qualities to differentiate them from each other.Asystem is built whichis not only precise but alsoefficientintermsof spaceandtime,takingintoaccountall ofthesefactors.Asaresult,theadvantage of a two-class problem is used to resolve the different penalties to the strategies owing to large data handling, as it is time effective and improves the accuracy, as it is explored later.

The process space is efficient as theline goes downby using a logical elimination method. This phase helps us to make our process more effective in terms of space. However, all of the classes are included in the step by step classification process in attempting to maintain a two-class issue.The strategy is starting with the two simplest classes, called the attackas well as normal class. Firstly,delete the normal class cases as well as reconstruct the two-class issue from the later class using one class of attack as theselected attack as well as the other class as the other attack classtype after the information is discovered and not belonging to the normal class. And if the information doesn’t match our prioritized attack type, the instances of this attack class is eliminated, thenanoriginal two-class issue is created using the similar

prioritization technique.
The ANN mechanism is shown in Figure 1 functioning with the 3 primary processes of prioritization, elimination, and classification. The attacks are categorizedlikeR2L, U2R, Probe, and DoS, in that order.

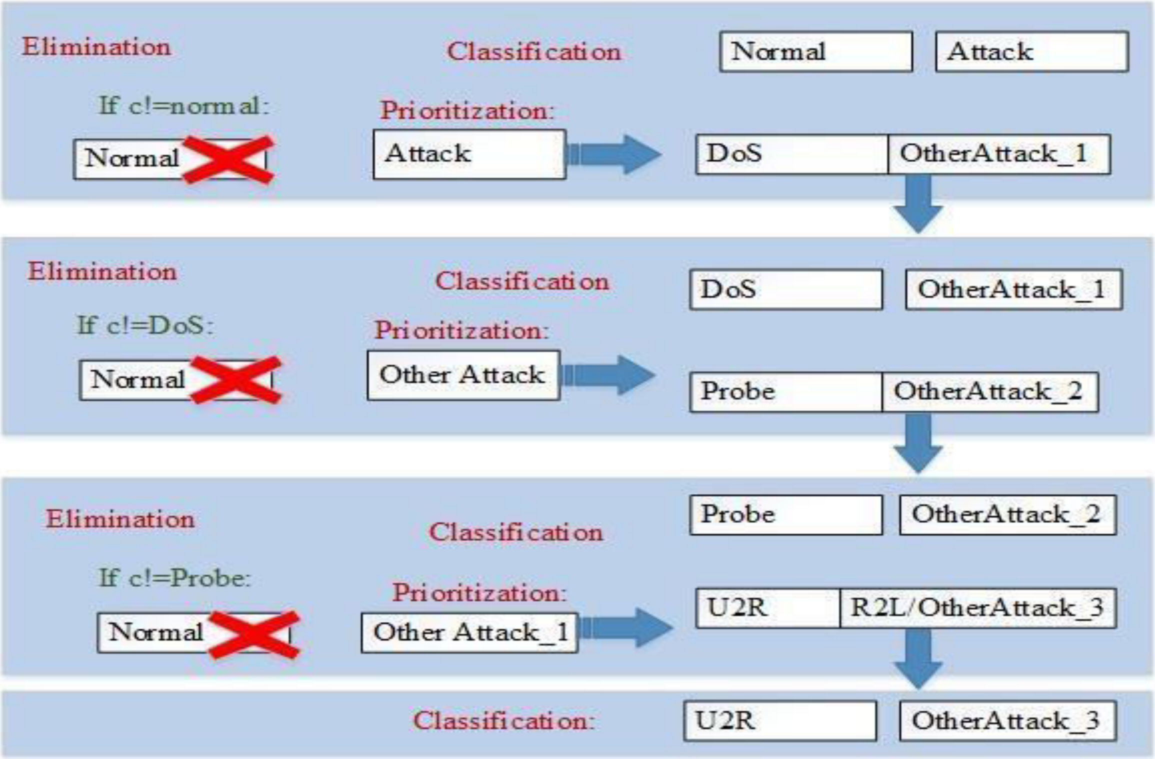


Fig.1ANN mechanism with the three main steps

R2L (Remote 2 Local), U2R (User 2 Root), Probe, and Denial of Service (DoS) are the 4 main kinds of network attack traffic presently in use. DoS is a term that encompassesall sorts of network traffic flooding attacks. Source bytes, packet speeds, and other relevant information are included. Probe attacks areattemptstogatherinformationaboutanetworkbydeliveringuselesspackets.Afeature likeconnection duration or source bytes is frequently used to detect them. Distant access assaults (R2L) are attempts by an attacker to acquire entry to a remote structure.The time of connections, the provision sought, and log-in effortsfailed are all relevant features. The U2R attack is one where attacker attempts in logging in to theregular account before gaining root managerpermission. Features like the total files generated and the total shell queries executed are frequently used to identify them. We use our evolving process on these four types of attack traffic and one type of regular traffic, which may be described in three basic steps, as explained below.

Classification
Classification uses a Multi-Layer Perceptron (MLP)ANN model to solve a two-class problem.
Initially, two classes are chosen, that is, an attack class as well as a normal class.

Elimination
Following the classification being successful, the classes with least probability are deleted inorder to efficiently clip the evaluated network data, as well as a original 2-class challenges are created from the latter class.

Prioritization
In the phase, the first form of classics hosenas the one to be analyzed, while another class is designated by another attack class.

Analgorithmfortheproposedmethodintheformoffourbasiccategoriesofnetworkattack traffic is depicted below.

Algorithm1: ANN Intrusion Detection System

```
group=sumof2ormoregroups; normal =1;
attack=0;
runclassificationtest; j = 1;
if a== 0&&group==TRUE then eliminatenormalinstances; dos = 1;
other_attackj=0;
ifc==0&&group==TRUEthen eliminateDoSinstances; probe =1;
other_attackj-1=0;
ifa==0&&group==TRUEthen eliminateprobeinstances; U2R=1;
R2Lother_attackj-2=0;
ifa==0&&group==TRUEthen traffic is R2L,
else
else
trafficisU2R;

else
else
trafficisprobe; traffic is DoS;
            trafficis normal;
```

IV. RESULT AND DISCUSSION

Thedetectionaccuracyandtrainingtime forvarioustypes ofattackusingallthefeaturesfromthe KDD99 dataset are examined. Along with typical network traffic, a total number of 1500 information samples from all the four types of network traffic attack is employed. The samples from each of the4main categories of network trafficattack subclasses are taken. The KDD99 dataset has 1500 cases with five classes, as given in Table 1.

Dataset	Normal	DoS	Probe	U2R	R2L
KDD99	350	450	300	100	300

Table1.KDD99 dataset with 5 attack classe

Table 2 lists all of the subtypes of the four basic forms of network attack traffic employed in the experiment.

Attackclasses	Attacktypes
R2L	Phf, Guess_ Password,WarezmasterImap,Ftp_write.
Probe	Ipsweep,Portsweep,Nmap,Satan,
DoS	Land,Pod,Teardrop,Neptune,Smurf,Back,
U2R	Loadmodule

Table2.Attackclassanditstypes

1.1 False alarm rate and Detection rate

AlowfalsealarmrateandahighdetectionratearerequiredforbetterIntrusionDetection System, and both can be computed using the formulae below.

$$Detectionrate= \frac{TP'}{TP'+FP'} \qquad (1)$$

$$Falsealarmrate= \frac{FP'}{FP'+TN'} \qquad (2)$$

Here,$'$=falsepositive,TN'=truenegative,TP'=truepositive,FN'=falsenegative

The artificial neural network which is proposed is compared with the existing ensemble clustering, Naive Bayes, K-means, One Rmethods for their detection rate and false alarm rate. The result shows that the proposed algorithm is havinga betterfalse alarm rate and detection rate when comparing with other methods. Table 3 shows both the detection rate and false alarm rate of various methods.

Method	Detectionrate (%)	Falsealarmrate(%)
K-means	78.05	8.30
NaiveBayes	86.24	8.40
OneR	51.91	4.87
Ensembleclustering	98.83	0.13
ANN	99.20	0.11

Table3.False alarm rate and Detection rate for different methods

1.2 Precision and Recall rate

In the Intrusion Detection System,recall and precision are highly valuable in determining how important each class is beingrecognised in the detection rate. In equations (3) and (4), respectively, a definition of recall andprecision is given.

$$Precision = \frac{TP'}{TP'+FP'} \quad (3)$$

$$Recall = \frac{TP'}{TP'+FN'} \quad (4)$$

The precision rate of five attack classes for the ensemble clustering method is compared with the proposed ANN model is shown in Fig. 2, where the ANN model has the precision rate higher than the existing method for all five classes.

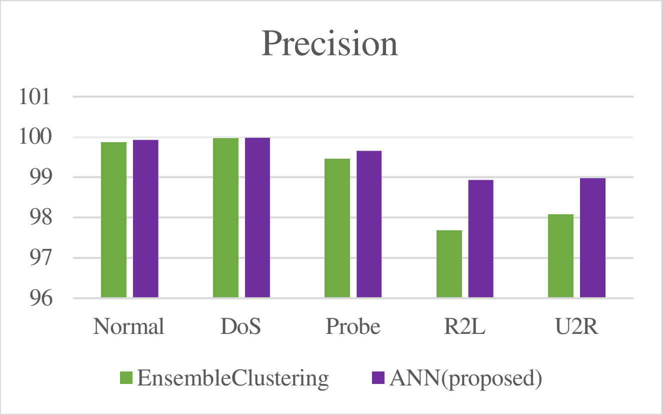


Fig.2Comparisonofprecisionrate

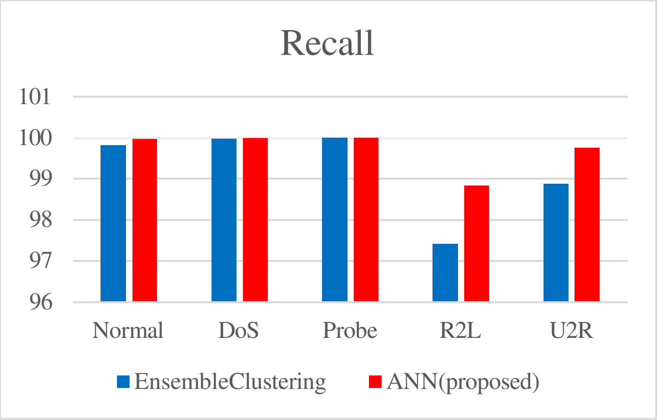


Fig.3Comparison of recall rate

Fig.3 shows the comparison of recall rate for ensemble clustering method and the proposed ANN model for five attack classes, where the ANN model has the recall rate higher than the existing method.

V. CONCLUSION

The rising demand for remote healthcare monitoring systems necessitates the development of a secure system that ensures the data's privacy and integrity. A patient's body is fitted with several small sensors that record biometric data to keep track the condition of the patients. However, because of physical limitations likeminimum processing capacity as well asminimum battery life, they might be unable to provide the needed confidentiality and privacy for patient data. Utilizing Intrusion Detection Systemsto make sure that such systems' safetyneeds are met is the alternative solution to such limits. In this proposed method, an IDS based on the classification of artificial neural network is presented to identify the four main forms of attack traffic which happens in a MCPS network. The experimental results reveal that the proposed technique has alesser false alarm rate and a greater detection rate than other current methods. Further more, the precision and recall rate of the suggested method are higher than those Of the existing method. As a result, the suggested ANN technique is having a detection rate as 99.20 percent as well as a false alarm rate as 0.11 percent.

REFERENCES

1. Bhuyan, M., Bhattacharyya, D. and Kalita, J. (2014) ‘Network anomaly detection: methods, systems, and tools’, IEEE Communications Surveys and Tutorials, Vol. 16, No. 1, pp.303–336.
2. Denatious, D.K. and John A. (2012) ‘Survey on data mining techniques to enhance intrusion detection’ in Proceedings of International Conference on Computer Communication and Informatics (ICCCI-2012), IEEE, Coimbatore, India.
3. Heckman,MarkR.2017.“ForImprovingINTRUSIONDETECTION.”
4. Schneble, William, and GeethapriyaThamilarasu. 2019. “Attack Detection Using Federated Learning in Medical Cyber-Physical Systems,” 8.
5. Wankhade, Kapil K, and Kalpana C Jondhale. 2019. “An Ensemble Clustering Method for Intrusion Detection,” 29.
6. Chauhan, P.and Shukla, M. (2015) ‘Areviewon outlier detection techniques on a data streamby using different approaches of k-means algorithm’, in the Proceedings of the International Conference on Advances in Computer Engineering and Applications (ICACEA), IEEE, pp.580–585.
7. Marchang, N., Datta, R. and Das, S.K. (2017) ‘A novel approach for efficient usage of the intrusion detection system in mobile ad hoc networks, *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 2, pp.1684–1695.
8. J.P.Planquart,"ApplicationofNeuralNetworkstoIntrusionDetection,"2001.
9. E.K.Wang,Y.Ye,X.Xu,S.M.Yiu,L.C.K.HuiandK.P.Chow,“SecurityIssuesandChallenges forCyberPhysicalSystem”,2010IEEE/ACMInternationalConferenceonGreenComputingand Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, (2010), pp. 733-738.
10. M. Alam, S. Abedin, M. Ameen, and C. Hong, "Web of Objects Based Ambient Assisted Living Framework for Emergency Psychiatric State Prediction," *Sensors,* Vol. 16, No.9, September2016.

11. O. Kocabas, 1. Soyata, and M. K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems", *IEEE/ACMTransactions on Computational Biology and Bioinformatics,* VO. [3, No.3, June 2016.
12. W. Gang, H. Jinxing, M. Jian, H. Lihua. "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering." *Expert Systems with Applications,* Vol. 37, No.9, pp. 6225-6232,2010.
13. S. K. Sahu, S. Sarangi, and S. K. Jena, "A detailed analysis on intrusion detection datasets," Souvenir 2014 IEEE [nt. Adv. Computer Conf. IACC 2014, pp. 1348- 1353,2014.
14. Vigna, Giovanni, and Richard A. Kemmerer. 1999. “NetSTAT: A Network-Based Intrusion Detection System.” *Journal of Computer Security* 7 (1): 37–71. https://doi.org/10.3233/JCS-1999-7103.
15. Sharafaldin, Iman, ArashHabibiLashkari, and Ali A. Ghorbani. 2018. “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization:” In *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–16. Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0006639801080116.
16. Hady, Anar A., Ali Ghubaish, Tara Salman, DevrimUnal, and Raj Jain. 2020. “Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study.” *IEEE Access* 8: 106576–84. https://doi.org/10.1109/ACCESS.2020.3000421.
17. Siniosoglou, Ilias, PanagiotisSarigiannidis, VasilisArgyriou, Thomas Lagkas, Sotirios K. Goudos,andMariaPoveda.2021.“FederatedIntrusionDetectionInNG-IoTHealthcareSystems: An Adversarial Approach.” In *ICC 2021 - IEEE International Conference on Communications*, 1–6. Montreal, QC, Canada: IEEE. https://doi.org/10.1109/ICC42927.2021.9500578.
18. You, Ilsun, KangbinYim, Vishal Sharma, GauravChoudhary, Ing-Ray Chen, and Jin-Hee Cho. 2018.“MisbehaviorDetectionofEmbeddedIoT DevicesinMedicalCyberPhysicalSystems.”In *Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems, and Engineering Technologies*, 88–93. Washington DC: ACM. https://doi.org/10.1145/3278576.3278601.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details