Mesopotamian journal of Cybersecurity
Vol.4,No.2, **pp**. 120–128
DOI: https://doi.org/10.58496/MJCS/2024/011; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Anomaly Intrusion Detection Method based on RNA Encoding and ResNet50 Model

Mohammed Ahmed Subhi [1*], Omar Fitian Rashid [2], Safa Ahmed Abdulsahib [3], Mohammed Khaleel Hussein [1], Saleh Mahdi Mohammed [4]

1 Department of Planning, Directorate of Private University Education, Ministry of Higher Education and Scientific Research, Baghdad, Iraq
2 Department of Geology, College of Science, University of Baghdad, Baghdad, Iraq
3 Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.
4 Department of Computer Technology Engineering, Technical College, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.

ARTICLE INFO

Article history
Received 03 Jun 2024
Accepted 04 Aug 2024
Published 28 Aug 2024

Keywords
Anomaly
Encoding
Intrusion detection
Boyer–Moore Algorithm
Matching

ABSTRACT

Cybersecurity refers to the actions that are used by people and companies to protect themselves and their information from cyber threats. Different security methods have been proposed for detecting abnormal network behavior, but some effective attacks are still a major concern in the computer community. Many security gaps, such as denial of service, spam, phishing, and other types of attacks, are reported daily, and the number of attacks is growing. Intrusion detection is a security protection method that is used to detect and report any abnormal traffic automatically that may affect network security, such as internal attacks, external attacks, and maloperations. This paper proposes an anomaly intrusion detection system method based on a new RNA encoding method and the ResNet50 Model, where encoding is performed by splitting the training records into different groups. These groups are protocol, service, flag, and digit, and each group is represented by the number of RNA characters that can represent the group's values. The RNA encoding phase converts network traffic records into RNA sequences, allowing for a comprehensive representation of the dataset. The detection model, which uses the ResNet architecture, effectively addresses training challenges and achieves high detection rates for different attack types. The KDD-Cup99 dataset is used for both training and testing. The testing dataset includes new attacks that do not appear in the training dataset, which means that the system can detect new attacks in the future. The efficiency of the suggested anomaly intrusion detection system is determined by calculating the detection rate (DR), false alarm rate (FAR), and accuracy. The achieved DR, FAR, and accuracy are 96.24%, 6.133%, and 95.99%, respectively. The experimental results revealed that the RNA encoding method can improve intrusion detection.

1. INTRODUCTION

Cybersecurity detection systems include various techniques that can be used to identify potential threats or malicious activities in computer systems. The main goal of these techniques is to reduce the impact of cyberattacks by detecting these threats [1]. An intrusion detection system (IDS) is one of these techniques that is effectively used to indicate unauthorized access to networks and computers [2]. An IDS is a computational tool (software in the majority; however, hardware implementations are possible [3]) that is tasked with observing a computer network or a computerized industrial plant [4] and monitoring its transactions to distinguish and detect potential violations made by those transactions. Distributed denial of service (DDoS) and code injection attacks are major types of attacks that need to be detected by IDS [4][5]. The system needs to learn the operation of the network and monitor its behavior to create a classification tree for the type of action being performed. A major part of IDS operation involves detecting intrusions made by outsiders (i.e., users or malfunctioning parts of the network) to protect the system from breakdowns or data exploitation [6]. IDS can be implemented in various applications that include and are not exclusive to home automation, industrial plants, data storage enterprises, and stock markets [7]. The current development of internet protocols and applications requires robust implementation of IDS systems. IoT applications also benefit substantially from IDS systems and frameworks [8]. Vehicular networks require special treatment when implementing the IDS system [9]. Car manufacturers implement various electronic control units (ECUs) with multiple capabilities, resulting in complicated networks of processing capabilities that must follow controlled area network (CAN) rules to achieve seamless operation of attack prevention systems. Firewalls are a special case of an IDS. Firewalls, however, are not required to identify the intrusion type and classify it, as they are mostly tasked with limiting the

*Corresponding author. Email: mohd.a.subhi@gmail.com

network connections to apprehend the attack made on the network. IDS are required to learn the types of anomalies and create rules to solve each type. This requires the system to be intelligent and prompt in response to various attacks that may occur in the deployed system. Residual neural network (ResNet) is a deep learning method that can easily optimize and gain accuracy from greatly increased depth; this leads to better results than other previous network methods can achieve [10][11].

Various approaches have been proposed for IDS solutions. Entezari-Maleki et al. [12] evaluated the IDS operation against black and gray-hole attacks in wireless ad hoc networks. The attack is modelled via two variations of continuous-time Markov chains. The evaluation metric used is based on detection. The proposed model automatically generates reward nets that are stochastic in the next step of the Markov chain. CEP (complex event processing) engines have been explored to develop an IDS model. Rashid et al. [13] proposed an intrusion detection method based on two DNA sequence generation methods using different network parameter values and then applied the matching algorithm to classify network traffic as either attack or normal. 'Wisdom,' developed by [14], is a stream processor based on a hybrid CEP optimizer that uses bisection algorithms and particle swarm optimization (PSO). The developed algorithm has been tested on the CICIDS 2017 dataset with more than 2.5 million events per second.

The results show that the algorithm is capable of detecting attacks with an accuracy of 99.98% and a mean recall of 93.42%. De Oliveira et al. [3] proposed an IDS that detects attacks related to chemical water contamination. Using sensors deployed in the water stream, the system detects parathion pesticides through its chemical reaction with water. The deployed sensors detect this reaction, creating data via the EPANET-MSX program. The water quality and hydraulic model represent the generated data. From the data acquired, a recognition pattern is made via the NARX neural network. The results show that the system detects the simulated attacks rather accurately. Code injection is one of the most commonly used types of attacks in web applications. CODDLE is an IDS proposed by [4] that utilizes deep learning against web-based attacks. The method encodes SQL/XSS symbols and processes them through a conventional deep neural network. The proposed method shows that through real-world datasets, it is possible to achieve attack detection with an accuracy of 95%, precision of 99%, and 92% recall value. The IACF (intrusion action correlation framework) was developed in [7] to improve the alert scenario process, extraction, and aggregation. Using intrinsic strong correlations to group raw alerts. The action links mode and redundant actions are removed via a pruning algorithm to discover highly stable correlations. This process is mandatory to limit the number of false positives. The findings of the proposed method show its efficiency in alert correlation and scenario construction of the intrusion.

The detection of botnets is an important task in an IDS. Alhijaj et al. [15] proposed a genetic algorithm (GA) that searches for feature combinations from botnets. A classifier based on a decision tree (DT) is devised to direct the GA for feature combination locations. Using the UNSW-NB15 and CICIDS2017 datasets, the results show that the developed GA can find features from the total feature set with efficient botnet detection outcomes. CAN (controlled area network) is widely used in vehicular networks. IDS is an important asset in such networks. [16] proposed an unsupervised intrusion prevention system (IPS). The system is developed in a way that does not require the modification of car manufacturer information. Using off-the-shelf components and machine learning, the proposed system achieves an attack detection accuracy of 99% with a processing time of 80 µs. The method, however, requires the data processed to be short in bit number. The moth-flame optimization (MTO) algorithm was proposed as a decision tree algorithm by [17]. The proposed method adopts the MTO decision tree while minimizing exploration via cosine similarity. Compared with several other methods, the proposed method achieves significant results in terms of attack detection accuracy on the KDDCUPP99 and UNSW-NB15 datasets. A new DNA encoding method was proposed for IDSs by [18]; this method is performed by suggesting a new DNA encoding method to convert network traffic to DNA sequences. The brute-force algorithm is subsequently used for the classification process. Recent developments in IoT applications require accurate attack detection by IDSs. Sugitha et al. [19] proposed a deep neural network (DNN) IDS that uses a stacked autoencoder for an IoT environment. The method employs GEO (golden eagle optimization) to select the features with optimum values from preprocessed data. The proposed method simulation results reveal that the accuracy of attack detection reaches 99.75%. Enhancing the security of wireless sensor networks (WSNs) is a major paradigm in IDS methods. Behiry and Aly [20] proposed deep learning with a feed-forward neural network to increase the efficiency of attack detection. The method adopts k-means models for feature extraction, and the final results show significant improvement in the IDS operation using benchmark datasets: NSL-KDD, UNSW-NB15, and CICIDS2017. Multiple classification models have been explored [21]. The proposed method is based on feature reconstruction and matching. The proposed method can be implemented on small-scale edge node(s) via adaptive scaling and reconstruction errors. The proposed method has been benchmarked using the CICIDS2017 dataset and shows an attack detection accuracy of 99.81%, which outperforms similar methods in its class. Fouad and Hameed [22] proposed a new IDS by using genetic algorithm-based clustering that is used to distinguish network traffic from normal traffic and attack, where two genetic algorithm methods are proposed: one handles the numeric features only, and the second uses all the features. An efficient new IDS method was proposed in [23]; this method can detect new attacks and is based on data stream classification methods and additional incoming stream-based learning with limited labels. Recent advancements in machine learning algorithms have significantly contributed to the development of sophisticated intrusion detection models, as proposed in [24] and [25].

These models provide robust solutions for detecting anomalies, enhancing the ability of intrusion detection systems to adapt to emerging threats and evolving security challenges.

The proposed anomaly IDS method uses a suggested RNA encoding method and ResNet50 Model, where RNA encoding is used to represent all the dataset records, whereas the ResNe method is used as a detection model. The advantage of using the suggested methods is their ability to address training challenges and obtain results with high detection rates.

2. MATERIALS AND METHODS

A new anomaly intrusion detection technique is proposed; the proposed method is based on three phases: preprocessing, RNA encoding, and an anomaly detection model.

2.1 Preprocessing

The main purpose of this phase is to analyse the dataset before training the detection model via the ResNet model, where the encoded KDD-Cup 99 dataset is used as the source for model training. The following preprocessing steps are implemented:

A. Data collection: This step is performed by dividing the dataset into normal records and attack records and labelling these records by their type, either normal or attack name.

B. Splitting dataset: This is performed by dividing the dataset into a training dataset and a testing dataset, where the training dataset is used to train the model, while the test dataset is used to evaluate the performance of the proposed model.

C. Record redundancy removal: This step is used to remove redundant records from both the training and testing datasets, with the aim of increasing the accuracy of the achieved results.

2.2 RNA encoding

Ribonucleic acid (RNA) is a nucleic acid found in most living cells; unlike DNA, RNA is single-stranded and includes a backbone made of phosphate groups and the sugar ribose, where each sugar is attached to one of four bases: adenine (A), uracil (U), cytosine (C) or guanine (G). This phase aims to encode network traffic records into RNA sequences by analysing and dividing dataset records into four groups: protocol groups, service groups, flag groups, and digit groups. After being divided into groups, the next step involves calculating the possible values for each group. The protocol group consists of 3 values: TCP, UDP, and ICMP. In comparison, the service group contains 71 values, which include HTTP, HTTP 443, DOMAIN U, ECR I, SMTP, ECO I, TELNET, NTP U, URP I, Z39 50, FTP, SSH, WHOIS, CTF, LINK, SUPDUP, ISO TSAP, UUCP PATH, FINGER, EXEC, NETBIOS DGM, COURIER, PM DUMP, TFTP U, RED I, FTP DATA, POP 3, AUTH, OTHER, PRIVATE, VMNET, BGP, DOMAIN, GOPHER, REMOTE JOB, RJE, HOSTNAMES, CSNET NS, POP 2, SUNRPC, LDAP, DISCARD, NAME, KLOGIN, IRC, X11, NNSP, NNTP, IMAP4, SQL NET, LOGIN, SHELL, PRINTER, EFS, DAYTIME, SYSTAT, NETSTAT, TIME, ECO, ICMP, MTP, NETBIOS NS, UUCP, AOL, HTTP 8001, NETBIOS SS The flag group includes 11 different values, which are SF, OTH, RSTO, REJ, S1, S2, S3, RSTOSO, S0, RSTR, and SH. Finally, the digit groups consist of 11 values, which include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and “.”[13]. After all possible values for each group are found, the next step is choosing the number of RNA characters required to represent all possible values, where for the protocol group, one RNA character is used to represent group values, whereas for the service group, four RNA characters are used to represent all group values, two RNA characters are chosen to represent all values in the flag group, and finally, two RNA characters are used to represent all possible values that appear in the digit group. After choosing the required number of RNA characters for each group, the next step is performed by randomly generating RNA characters for each value in the group. For example, the character C is randomly chosen to substitute all the TCP values in the network traffic record, G for UDP and U for ICMP, as shown in Table I. Similarly, Tables II, III, and IV represent the RNA character substitutions for the protocol group, service group, flag group, and digit group, respectively.

TABLE I. RNA ENCODING FOR THE PROTOCOL GROUP

Protocol Group	RNA
TCP	C
UDP	G
ICMP	U

TABLE II. RNA ENCODING FOR THE SERVICE GROUP

Service Group	RNA	Service Group	RNA
HTTP	CGAA	HOSTNAMES	GCGU

HTTP 443	GACU	CSNET NS	GAGC
DOMAIN U	CUCC	POP 2	UCAG
ECR I	UGGC	SUNRPC	GGUA
SMTP	AGGU	LDAP	UAUA
ECO I	UAGU	DISCARD	AUCC
TELNET	CGGG	NAME	AAAA
NTP U	CCCC	KLOGIN	GGGA
URP I	AAUA	IRC	CGUC
Z39 50	CCCA	X11	UGAG
FTP	CCGG	NNSP	GACC
SSH	AUGG	NNTP	CUUG
WHOIS	CAUC	IMAP4	CGCC
CTF	UGUA	SQL NET	CUAG
LINK	AAAC	LOGIN	CAAA
SUPDUP	AAGG	SHELL	CUGC
ISO TSAP	GUAA	PRINTER	UACC
UUCP PATH	GCCA	EFS	CGAG
FINGER	GUGA	DAYTIME	UGUG
EXEC	UCCC	SYSTAT	CGAU
NETBIOS DGM	ACAG	NETSTAT	UUCU
COURIER	AUAC	TIME	UGUU
PM DUMP	CUUC	ECO	CAUU
TFTP U	GCAA	ICMP	AGCA
RED I	CUCA	MTP	UACA
FTP DATA	CAUG	NETBIOS NS	UGCC
POP 3	UUCG	UUCP	UCGC
AUTH	AGCU	AOL	UGCA
OTHER	AUGC	HTTP 8001	CCGC
PRIVATE	ACAU	NETBIOS SSN	AUAU
VMNET	AACG	KSHELL	GGUG
BGP	UGCU	HTTP 2784	AUAG
DOMAIN	UGGU	URH I	UAUU
GOPHER	CCCG	TIM I	CCUU
REMOTE JOB	ACGU	HARVEST	CACC
RJE	GCGA		

TABLE III. RNA ENCODING FOR THE FLAG GROUP

Flag Group	RNA	Flag Group	RNA
SF	GG	S3	UC
OTH	GC	RSTOSO	AG
RSTO	CU	S0	AU
REJ	GU	RSTR	UG
S1	UU	SH	AC
S2	UA		

TABLE IV. RNA ENCODING FOR THE DIGIT GROUP

Digits group	RNA	Digits group	RNA
0	UG	6	UC
1	UU	7	AC

2	AG	8	CC
3	UA	9	GC
4	GA	.	CG
5	AA		

To understand the RNA encoding process, the following example illustrates how the network traffic "1,tcp, smtp,SF,2442,329,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,3,0.00,0.00,0.00,0.00,1.00,0.00,1.00,178,122,0.69,0.03,0.01,0.00,0.00,0.00,0.00,0.00" is encoded into RNA characters on the basis of previously mentioned RNA encoding tables, which is accomplished by dividing the network traffic into their total feature numbers, which equal 41 features, and representing each feature value by their equivalent RNA characters, as shown in Table V.

TABLE V. RNA ENCODING EXAMPLE

1	**tcp**	**Smtp**	**Sf**	**2442**	**329**
UU	C	AGGU	GG	AGGAGAAG	UAAGGC
0	**0**	**0**	**0**	**0**	**1**
UG	UG	UG	UG	UG	UU
0	**0**	**0**	**0**	**0**	**0**
UG	UG	UG	UG	UG	UG
0	**0**	**0**	**0**	**1**	**3**
UG	UG	UG	UG	UU	UA
0.00	**0.00**	**0.00**	**0.00**	**1.00**	**0.00**
UGCGUGUG	UGCGUGUG	UGCGUGUG	UGCGUGUG	UUCGUGUG	UGCGUGUG
1.00	**178**	**122**	**0.69**	**0.03**	**0.01**
UUCGUGUG	UUACCC	UUAGAG	UGCGUCGC	UGCGUGUA	UGCGUGUU
0.00	**0.00**	**0.00**	**0.00**	**0.00**	
UGCGUGUG	UGCGUGUG	UGCGUGUG	UGCGUGUG	UGCGUGUG	

2.3 Anomaly detection model

After the KDD cup99 dataset has been encoded into an RNA representation, the converted training data are fed into a CNN model and trained for anomaly/misuse detection. The residual neural network (ResNet) is a deep learning model chosen to train the detection model, and it is used to address the degradation problem that occurs during the training phase in deep neural networks [26]. It is well known for its ability to learn residual mappings; this helps mitigate the problem of vanishing gradients in deep neural network training. The architecture of the ResNet 50 architecture is depicted in Figure 1.

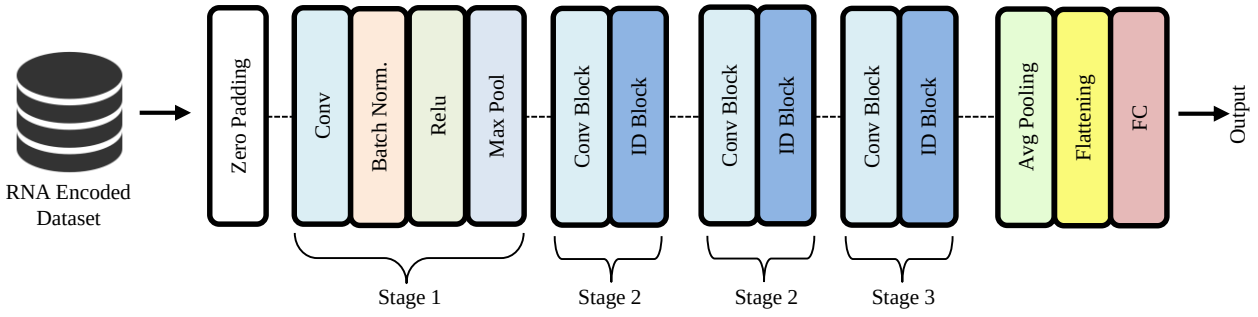

Fig. 1. ResNet50 Architecture for Anomaly Detection [24]

To adapt the architecture of ResNet50 to be trained with the RNA-encoded features of KDD Cup99, several modifications are needed; this includes the conversion of the RNA codes to numerical values and then organizing the data into matrices to match the input layer of the ResNet50 architecture. Table VI shows the mapping table of the converted RNA data to binary representation.

TABLE VI. ASCII AND BINARY REPRESENTATION OF RNA CODES

RNA Character	ASCII Code	Binary Representation
A	065	01000001
C	067	01000011
G	071	01000111
U	085	01010101

The model is trained with the hyperparameters shown in Table VII, and the initial training takes 100 epochs for the model to converge, with a learning rate of 0.001, a batch size of 32, and an Adam optimizer to update the weights of the model and minimize the loss function. The loss function is binary cross entropy since our objective is to classify anomaly cases. These hyperparameters have been tested and shown to have optimal performance.

TABLE VII. DETECTION MODEL HYPERPARAMETERS

Hyperparameter	Value
Learning Rate	0.001
Batch Size	32
Optimizer	Adam
Loss Function	Cross entropy
Dropout Rate	0.5

3. RESULTS AND DISCUSSION

To evaluate the proposed anomaly intrusion detection system, the KDD-Cup99 dataset is used for both training and testing, where the training dataset consists of 24 different attacks out of the 38 presents in the test dataset, and all these attack types can be categorized into four groups. These groups are Denial of Service (DoS) attacks, Probe attacks, Remote to Local (R2L) attacks and User to Root (U2R) attacks. The performance of the proposed method is evaluated on the basis of the detection rate (DR) for individual attack type, the DR for total attacks, the false alarm rate (FAR), and accuracy. The formulas used to calculate these measures are given in equations (1, 2 and 3).

$$\mathbf{DR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \quad \ldots (1)$$

$$\mathbf{FAR} = \frac{\mathrm{FP}}{\mathrm{TN} + \mathrm{FP}} \quad \ldots (2)$$

$$\mathbf{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad \ldots (3)$$

3.1 Detection Rate Analysis

The achieved detection rates (DR) of various type of attacks—95.34% for DoS, 96.51% for Probe, 92.42% for R2L, and 92.42% for U2R —are an indication that the model is very effective and efficient in the detection of all types of cyber threats. These results are important to note given the fact that R2L and U2R attacks are usually more difficult and follow less evident and uniform patterns. The fact that the system is capable of maintaining high DR across these categories implies that the RNA encoding method preserves features that other conventional encoding methodologies may omit. This is probably because overall representation of the network traffic adds to the model's ability to discern the fine details of various attacks. Table VIII and Figure 2 presents the achieved DR results for different attack types.

TABLE VIII. THE ACHIEVED DETECTION RATE RESULTS FOR DIFFERENT ATTACK TYPES

Attack name	**DR**

DoS	95.34%
Probe	96.51%
R2L	92.42%
U2R	92.42%

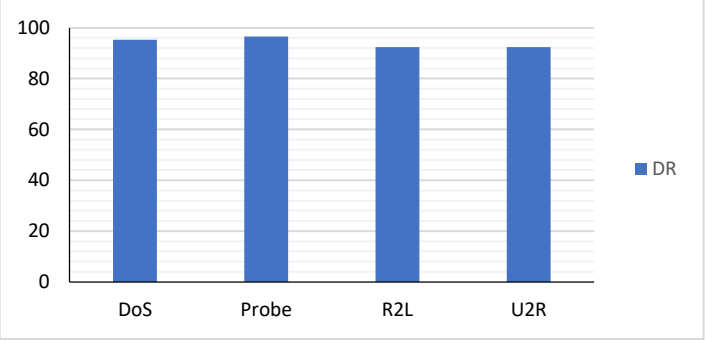

Fig. 2. The achieved detection rate results for different attack types.

3.2 False Alarm Rate and Accuracy Considerations

The system's False Alarm Rate (FAR) of 6.133% is good result especially when considering the balance between indicators as DR and FAR applied to intrusion detection systems where both values are essential. A lower FAR is important so that the security system does not classify too many benign events as threats, which would degrade the system's performance, consume resources and stress the system. The FAR realized by the proposed method suggests that the model has high capability in differentiating between normal and anomalous traffic while minimizing false alarms that normally accompanies most intrusion detection systems.

Achieving 95.99% accuracy means that there is a reduction of errors in the outcome that is being generated which improves the overall system reliability. The proposed method has shown great potentials in detecting the intrusions. This high accuracy is due to the preprocessing and encoding phases to make sure that the data fed to ResNet50 model is clean and contains accurate representation of traffic patterns. The integration of RNA encoding with the deep learning model does not only increase the identification capability but also increases the accuracy in the categorization of the tasks.

When testing the model overall on all the four types of attacks as shown in Figure 3 and Table IX there was a good performance of the model in the case of multiple attack types. The total DR in the treatment of the patients was 96.24%, FAR of 6.133%, and accuracy of 95.99% showing the ability of the model to keep the high level of detection accuracy even when multiple kinds of attacks are presented at once.

TABLE IX. THE RESULTS OBTAINED BY THE PROPOSED METHOD

	Result
DR	96.24%
FAR	6.133%
Accuracy	95.99%

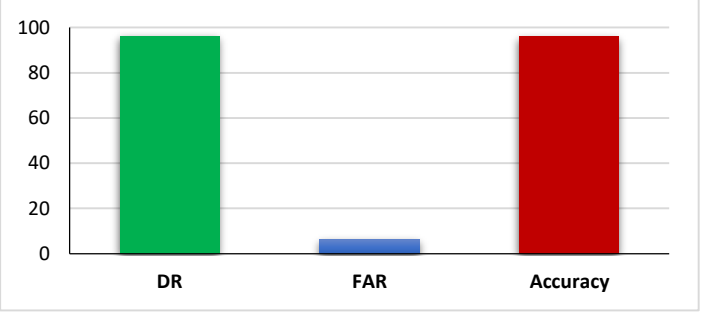

Fig. 3. The results obtained by the proposed method

3.3 Comparison with Existing Methods

The proposed method has the following advantages over other state-of-the-art techniques. Most of the conventional ML algorithms including Support Vector Machines (SVM) or Decision Trees lose their efficiency when processing data with high dimensionality like the network traffic data. On the other hand, the ResNet50 model, with RNA encoding, has a capability to learn deep hierarchical features which are more important when sorting out different types of network behavior. Further, the application of a deep residual network helps overcome the vanishing gradient problem that is typical for deep learning on large datasets.

3.4 Implications for Cybersecurity

The outcomes of this study are relevant for the improvement of the current approaches used in intrusion detection systems. This research proposes the use of RNA encoding as a superior solution because of its demonstrable ability to contain the complexity and variability of network traffic as opposed to traditional encoding techniques. In addition, the successful implementation of the deep learning architecture like the ResNet50 proves that it is possible to use the state-of-the-art neural networks in cybersecurity.

The high DR and low FAR attained in this study are significant especially considering real world scenarios where the cost of a false negative as in not detected intrusion is tremendously costly. The effectiveness of the proposed system in this study to identify new kind of attacks from the test dataset indicates its usefulness as a tool in the hands of network security specialist.

4. CONCLUSION

This research aims at developing a three-phase anomaly intrusion detection system with the preprocessing phase, RNA encoding phase, and an enhanced anomaly detection model that is based on ResNet. Network traffic is analyzed in terms of anomalies and categorized with the help of enhanced data preprocessing and data encoding. As a means to train the model, the KDD-Cup 99 dataset was preprocessed in the right manner. The data is gathered and then sorted as well to eliminate any redundant data that may have been obtained. These techniques enhanced the effectiveness and accuracy of the Anomaly detection since it eradicated any form of mess in the data. Additional technique was needed in order to map RNA sequences with network traffic records. Dividing data to protocol, service, flag, digit groups along with allocation of RNA characters produced a full data set representation. This made a positive transformation to the previous approach by capturing network traffic subtle patterns and properties. ResNet-based anomaly detection helps to clear up the problem of deterioration and gradient disappearance in deep neural network training. As a proof of concept, RNA codes were translated to numerical values and cross-validated with appropriate hyperparameters of the model. In the assessment of KDD-Cup 99 that we carried out in this work, the model highlighted DoS, Probe, R2L, and U2R attacks very well. As a result, our method has excellent detection rates, few false alarms, and high accuracy. Therefore, these findings suggest that this method has the potential of improving network security by detecting irregularities. This was achieved and proved that the strategy is applicable and established the groundwork for more research on intrusion detection systems. Therefore, the approach employing RNA encoding and deep learning models including ResNet can be considered as a potential for the development and solving of cybersecurity problems. The effectiveness of the system depends with the DR, FAR and accuracy of the system. For future work, the proposed method can be enhanced by applying different methods instead of matching and can also use different datasets, such as CIC-IDS2017 or CSE-CIC-IDS2018.

Conflicts of interest

The authors declare that they have no conflicts of interest.

References

[1] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, and H. Han, “A systematic literature review of methods and datasets for anomaly-based network intrusion detection,” Computers & Security, vol. 116. 2022.

[2] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, “Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities,” IEEE Access, vol. 10, pp. 112392-112415, 2022.

[3] L. L. de Oliveira, G. H. Eisenkraemer, E. A. Carara, J. B. Martins, and J. Monteiro, “Mobile Localization Techniques for Wireless Sensor Networks: Survey and Recommendations,” ACM Trans. Sens. Netw., vol. 19, no. 2, pp. 36:1-36:39, Apr. 2023, doi: 10.1145/3561512.

[4] S. Abaimov and G. Bianchi, “CODDLE: Code-Injection Detection with Deep Learning,” IEEE Access, vol. 7, pp. 128617–128627, 2019, doi: 10.1109/ACCESS.2019.2939870.

[5] D. K. Ghurkan and A. A. Abdulrahman, “Construct an Efficient DDoS Attack Detection System Based on RF-C4.5-GridSearchCV,” in 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), Sep. 2022, pp. 120–124. doi: 10.1109/IICCIT55816.2022.10010645.

[6] A. Tanwar, P. Sharma, A. Pandey, and S. Kumar, “Intrusion Detection System Based Ameliorated Technique of Pattern Matching,” Proceedings of the 4th International Conference on Information Management & Machine Intelligence, 2022. doi: 10.1145/3590837.3590947.

[7] K. Zhang, F. Zhao, S. Luo, Y. Xin, and H. Zhu, “An Intrusion Action-Based IDS Alert Correlation Analysis and Prediction Framework,” IEEE Access, vol. 7, pp. 150540–150551, 2019, doi: 10.1109/ACCESS.2019.2946261.

[8] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, “Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning,” J. Big Data, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00892-y.

[9] V. Tanksale, “Intrusion detection system for controller area network,” Cybersecurity, vol. 7, no. 1, 2024, doi: 10.1186/s42400-023-00195-4.

[10] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770-778, 2016. DOI: 10.1109/CVPR.2016.90.

[11] K. H. Abdulkareem, M. A. Subhi, M. A. Mohammed, M. Aljibawi, J. Nedoma, R. Martinek, M. Deveci, W. Shang, and W. Pedrycz, “A manifold intelligent decision system for fusion and benchmarking of deep waste-sorting models,” Engineering Applications of Artificial Intelligence, vol. 132, 2024, https://doi.org/10.1016/j.engappai.2024.107926.

[12] R. Entezari-Maleki, M. Gharib, M. Khosravi, and A. Movaghar, “IDS modelling and evaluation in WANETs against black/grey-hole attacks using stochastic models,” Int. J. Ad Hoc Ubiquitous Comput., vol. 27, no. 3, pp. 171–186, 2018, doi: 10.1504/IJAHUC.2018.089822.

[13] O. F. Rashid, Z. A. Othman, S. Zainudin and N. A. Samsudin, "DNA Encoding and STR Extraction for Anomaly Intrusion Detection Systems," in IEEE Access, vol. 9, pp. 31892-31907, 2021, doi: 10.1109/ACCESS.2021.3055431.

[14] G. Loganathan, J. Samarabandu, and X. Wang, “Real-Time Intrusion Detection in Network Traffic Using Adaptive and Auto-Scaling Stream Processor,” presented at the Proceedings - IEEE Global Communications Conference, GLOBECOM, 2018. doi: 10.1109/GLOCOM.2018.8647489.

[15] T. B. Alhijaj, S. M. Hameed, and B. A. Attea, “A Decision Tree-Aware Genetic Algorithm for Botnet Detection,” Iraqi J. Sci., pp. 2454–2462, Jul. 2021, doi: 10.24996/ijs.2021.62.7.34.

[16] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, “An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks with a Low-Cost Platform,” IEEE Access, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[17] M. Alazab, R. A. Khurma, A. Awajan, and D. Camacho, “A new intrusion detection system based on Moth–Flame Optimizer algorithm,” Expert Syst. Appl., vol. 210, 2022, doi: 10.1016/j.eswa.2022.118439.

[18] O. F. Rashid, Z. A., Othman, and S. Zainudin, “Four Char DNA Encoding for Anomaly Intrusion Detection System”, Proceedings of the 2019 5th International Conference on Computer and Technology Applications, 2019. DOI: 10.1145/3323933.3324069.

[19] G. Sugitha, B. C. Preethi, and G. Kavitha, “Intrusion detection framework using stacked auto encoder based deep neural network in IOT network,” Concurr. Comput. Pract. Exp., vol. 34, no. 28, 2022, doi: 10.1002/cpe.7401.

[20] M. H. Behiry and M. Aly, “Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods,” J. Big Data, vol. 11, no. 1, 2024, doi: 10.1186/s40537-023-00870-w.

[21] Y. Yang, J. Cheng, Z. Liu, H. Li, and G. Xu, “A multi-classification detection model for imbalanced data in NIDS based on reconstruction and feature matching,” J. Cloud Comput., vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00584-7.

[22] N. Fouad, and S. M. Hameed, “Genetic Algorithm based Clustering for Intrusion Detection”, Iraqi Journal of Science. Vol. 58, no. 2B, pp. 929-938, 2022, https://ijs.uobaghdad.edu.iq/index.php/eijs/article/view/6067.

[23] A. A. Abdualrahman, and M. K. Ibrahem, “Intrusion Detection System Using Data Stream Classification”, Iraqi Journal of Science, vol. 62, no. 1, p.p. 319-328, 2021, DOI: 10.24996/ijs.2021.62.1.30.

[24] J.Jasmine Hephzipah, Ranadheer Reddy Vallem, M.Sahaya Sheela, and G.Dhanalakshmi, “An efficient cyber security system based on flow-based anomaly detection using Artificial neural network”, Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 48–56, Mar. 2023, DOI: https://doi.org/10.58496/MJCS/2023/009.

[25] Muna Ismael Shihan Al-jumaili and Dr. Jad Bazzi, “Cyber-Attack Detection for Cloud-Based Intrusion Detection Systems ”, Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 170–182, Nov. 2023, DOI: https://doi.org/10.58496/MJCS/2022/019.

[26] R. Gomes, C. Kamrowski, J. Langlois, P. Rozario, I. Dircks, K. Grottodden, M. Martinez,W. Z. Tee, K. Sargeant, C. LaFleur, and M. Haley, “A Comprehensive Review of Machine Learning Used to Combat COVID-19,” Diagnostics, vol. 12, no. 8, pp. 1853, 2022,. https://doi.org/10.3390/diagnostics12081853.