Performance Evaluation of Artificial Intelligence Enabled Intrusion Detection System with Encryption Scheme for Network Security

[1]Mrs.Swapna Sunkara, [2]Dr.T.Suresh, [3]Dr.V.Sathiyasuntharam

[1]Research scholar, [2]Associate professor, [3]Professor&HoD
[1]Department of CSE, [2]Annamalai University ,[3]CSE - Cyber Security, CMR Engineering College, Hyderabad.

Abstract: Network security refers to the exercise of prevention of the unauthorized access of computer networks or their related devices and it comes under cybersecurity. In simpler terms protecting devices and network servers physically from external threats, along with that takinginitiative for network security. In a time of increasingly complicated cyberattacks, network security becomeshighly important. Two major solutions to accomplish network security are intrusion detection systems (IDS) and encryption. Intrusion Detection System (IDS) meansa system that would monitornetwork traffic for doubtful activity and grants alerts once the activity is found.Machine learning (ML) and deep learning (DL) models can be applied to design effective IDS models. On the other hand, encryption schemes can be developed to secure network data. Recently, numerous research works have been developed for attaining network security. This paper performs a study of various artificial intelligence (AI) techniques for IDS and encryption in network security. A detailed overview of various concepts involved in network security is elaborated. In addition, different IDS and encryption techniques can be derived to improve network efficiency. At last, a detailed experimental analysis is performed to demonstrate the performance of different models interms of different measures.

Keywords:Network security; Artificial intelligence; Intrusion detection system; Encryption; Machine learning

1. Introduction

Healthcare, commerce, energy, and manufacturing are only a portion of the areas of current culture that have been upset by the reception of computer systems and the infiltration of digital correspondences. Network security is an extensive term that covers an enormous amount of gadgets, cycles, and innovations. Generally, a group of configurations and rules designed to safeguard the integrity, confidentiality, and accessibility of computer networks and statistics with software and hardware developments [1]. Every organization pays small consideration to framework, size, or industry, which needs a level of network security arrangement settings to safeguard from the steadily emerging landscape of cyber threats. The present network design is mind boggling and is challenged with threats that are continuously changing and aggressors that are continuously making an effort to find and exploit weaknesses [2]. With this digitization pattern expanding with increasing rates, cyber-assaults and threats have likewise turned into a ubiquitous, all-pervasive peculiarity. It is a result of this entrance that today like never before, assailants have high inspiration to perform perfectly tuned assaults [3]. Intrusion Detection System (IDS) screens network traffics for issues cautions and dubious action once movement is found. A software application inspects a system or a network for strategy breaking or hurtful movement. Any vindictive infringement or endeavour is regularly detailed to a director or gathered midway using a security information and event management (SIEM) scheme. Despite the fact that IDS screen networks for feasibly pernicious movement, they are similarly arranged to false alarms [4]. Thus, association necessity to adjust their IDS items once they are primarily introduced. It infers properly setting up the IDS to observe what ordinary traffic on the network resembles than malevolent action. Machine Learning (ML), data analysis, and Artificial Intelligence (AI) techniques, while applied effectively to different domains, have just seen halfway useful applications in intrusion detection [5]. Fig. 1 showcases the elements of network security.

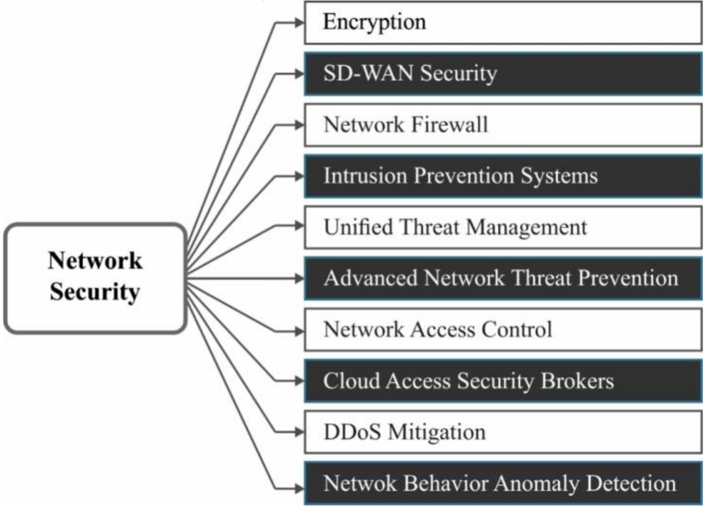
Network Security
Encryption
SD-WAN Security
Network Firewall
Intrusion Prevention Systems
Unified Threat Management
Advanced Network Threat Prevention
Network Access Control
Cloud Access Security Brokers
DDoS Mitigation
Netwok Behavior Anomaly Detection

Fig. 1. Elements of network security

The security necessities for data and calculations have ended up being outstandingly extreme over the latest two or three years. For taking care of and perusing data securely, there exist a couple of possible results like secure data encryption [6]. The issue was erratic while mentioning the opportunity to figure (openly) with scrambled data or to modify works that can be yet practicable while the security is ensured. To safeguard the data with high security, homomorphic cryptosystems wereused. Homomorphic cryptosystems were created to be incredibly worthwhile and empowering; in any case, there is at this point a ton of examination that ought to be finished to make these systems to be made practical with benefits [7]. HE at first encodes the text and functionsunder ciphertext, and then, at that point, the result is made by deciphering the text by the legitimate client. As of now, the data proprietor obtains an indistinguishable message; like it can be performed on 2 plain messages. Capacity and transmission, encryption is a very capable gadget, yet when the sensitive data was decrypted, the information isn't guaranteed any more [8]. In the event that the pictures are in plain-text, it is challenging to get to it and step by step logs through the gate crasher. Fundamental encryption calculations put the highlight on paired or textual datasets [9]. Therefore, standard codes like RSA, IDEA, AES, DES, and so on are inappropriate for persistent picture encryption as these codes required higher computation time and power for enrolling. Through understanding the benefits of encryption in providing fit security to novel information, a viable calculation is acquainted with encoding and decrypting the clinical pictures [10]. Swarm Intelligence (SI) is a creative clever dispersion model for taking care of optimization issues that initially got motivation from natural models by scaling, running, and brushing peculiarities in vertebrates. The Optimization technique is to decrypt and scramble the picture for safely exchanging among the transmissions and getting side pictures.

Recently, numerous research works have been developed for attaining network security. This paper performs a study of various artificial intelligence (AI) techniques for IDS and encryption in network security. A detailed overview of various concepts involved in network security is elaborated. In addition, different IDS and encryption techniques can be derived to improve network efficiency. At last, a detailed experimental analysis is performed to demonstrate the performance of different models interms of different measures.

2. Overview of Network Security

NSis crucial to keeping up with the trustworthiness of information and the protection of employees and organizations. It includes the whole thing from the essential practices, namely completely logging out of local area PCs and making solid passwords, to the most perplexing, substantial level cycles that keep clients safe, network, and gadgets. Increasingly more delicate data is put away on the web and in these different gadgets and assuming unauthorized client access that information, might prompt shocking consequences. Enough safeguarding networks and their related gadgets necessitate extensive network preparing, an exhaustive understanding of how network works, and the ability to try that data. It becomes essential for networks that appropriately and completely set up, got, and witnessed to save protection completely.

Normal Network Security Vulnerabilities

To successfully execute and keep up with secured network, it's vital to comprehend the normal weaknesses, issues, and threats confronting IT experts today. When some could be fixed reasonably effectively, others need elaborate arrangements. Generally, each PC network has weaknesses that leave them open to outside assaults; furthermore, networks and gadgets were as yet weak notwithstanding of nobody is efficiently focusing or threatening them. Weakness was a state of network or its hardware, not consequence of outside activity. They are possibly the well-known network weaknesses:

- Unsuitably presented hardware or software
- Working firmware or frameworks that poor person been refreshed
- Abused software or hardware
- Poor or a total absence of physical security
- Shaky password
- Configuration defect in a gadget's working in the network or framework

Physical Security Considerations

The physical security of the different gadgets, servers, and frameworks that can be utilized to control and keep up with your network. The chance that network was materially defenceless, it doesn't make any variance how solid or broad its security was, since, in such a case that somebody can acquire physical admittance to any of these things, the whole network is negotiated. Significant physical wellbeing contemplations incorporate the accompanying:

- Putting away network servers and gadgets in a protected area
- Rejecting open admittance to this area to individuals from your association
- Utilizing video observation to stop and recognize anybody who endeavors to get to this area
- Avoiding potential risks to keep up with physical wellbeing of your network would guarantee that it's ready to run as without a hitch and securely as could be expected.

Kinds of Network Security Attacks

Throughout recent years, cyberattacks arebecoming more refined, broad, continuous, and more challenging to shield against. Numerous cybersecurity specialists accept that such assaults would just keep on developing more mind boggling and forceful. Probably the commonest kinds of network security assaults any IT experts should know about the following:

Data Theft: named as data exfiltration, data theft will occur once an assailant utilizes their unauthorized admittance for acquiring personal information from the network. The time taken login certification to inspect safeguarded records or take the information.

Insider Threat: it comes from workers within the organization. The worker utilizes their own access to invade network and get delicate or privately owned business information.

Malware Attacks: it happens when a malevolent code (malware) embeds undesirable, unauthorized software on a network gadget. Malware could without much of a stretch spread starting with one gadget then onto the next, making it undeniably challenging to dispose of completely.

Password Attacks: it includes somebody endeavouring to exploit a password mistakenly is regarded as password assault. The programmer might get access by breaking, speculating, or taking passwords.

Social Engineering: It employs trickery and deception to persuade others to submit private data, like record passwords, or to abuse privacy conventions. They frequently attack targeted individual who is not educated, they might similarly target expert staff with bogus solicitation.

Sorts of Network Security Solutions

There are abundant methods of penetrating a network, there are extensive procedures and techniques that IT experts could employ to get one. The absolute most normal forms of network security arrangement include:

Antivirus Software: it is presented on every networked gadget to examine them for vindictive projects. It is refreshed routinely to fix any weaknesses or issues.

Encryption: it was the method involved with scrambling information to the place of incoherence and offering approved parties the key (password or decryption keys) to disentangle it. Regardless of whether information is seen or caught by an unauthorized user, they can't understand it.

Firewalls: they are software programs, hardware gadgets, or mixture of blocks spontaneous traffic from entering the network.

Multi-Factor Authentication: Multi-factor authentication was straightforward: user should offer 2 distinct techniques for recognizable proof to sign into a record (composing in a password and later composing in a numerical code that was shipped off other gadgets).

Network Segmentation: Network segmentation includes separating a bigger network into different subnetworks or fragments. when any of the subnetworks were invaded or compromised, the others remainedimmaculate on the grounds that they exist autonomously of one another.

3. Existing IDS and Encryption Schemes for Network Security

Pascale et al. [11] introduced an embedded IDS for the automotive field. This work by assuming a two-phase method that offers recognition of potential cyberattacks. Initially, the approach offers a filter of each message on the Controller Area Network (CAN-Bus) because of the usage of temporal and spatial examination; when a group of messages is feasibly malevolent, they are examined using a Bayesian network that provides the possibility that an occurrence could be categorized into the attack. Shrestha et al. [12] developed a satellite based 5G-network security and UAV system that could connect ML techniques for efficiently identify cyberattacks and vulnerabilities. The solution is classified as follows: the execution of ML-based technique into satellite or terrestrial gateways and the model creation for IDS with different ML approaches. The study illustrates that ML technique is utilized for categorizing benign or malicious packets in UAV networks to improve privacy.

Elhoseny et al. [13] examined the privacy of medicinal images in IoT with an advanced cryptographic technique using optimization strategy. Generally, the patient information is saved as a cloud server in the clinic accordingly privacy is crucial. Hence, other frameworks are essential for the efficient storage and secured transmission of medicinal images inserted with patient datasets. For improving the privacy levels of decryption and encryption systems, the optimum key would be selected by means of hybrid swarm optimization, that is, GOA and PSO in elliptic curve cryptography (ECC).

Kalyani and Chaudhari [14] developed secured IoT sensitive information using Optimum Homomorphic Encryption (OHE) with higher reliability. Sensitive information from IoTs is categorized according to the Deep Learning Neural Network architecture (DNN). Then, OHE implements sensitive information during decryption and encryption. In the encryption process, the key is validated and the optimum key is preferred through Step size Fire Fly (SFF) optimization approach. This technique could increase the encrypted keys and accomplishes the predominant privacy-preserving dataset in IoT.

Shankar et al. [15] examined and distinguished the open challenges in stimulating privacy in IoTs that integrate encryption schemes to provide security for the interchanged images among interconnected networks. The device is based mostly on hybrid model which employs optimization and encryption methods are utilized. The presented technique with elephant based optimization technique has been utilized. The aim is to select the more beneficial keys in encryption algorithm, now, Adaptive Elephant Herding Optimization (AEHO) has been employed. Signcryption is a method which integrates the digital signature and functionality of encryption in one logical phase.

Prabhakaran and Kulandasamy[16] developed the abovementioned problems by presenting the attention-based RCNN. The presented technique utilized for detecting either the textual information is intrusion or non-intrusion. The non-intrusion textual dataset is later utilized for additional processing and encrypted by means of two-way encryption system. Then, presented the ECC technique for increasing the security-level performance of non-intrusion dataset.

Alghamdi[17] designed an architecture named trust-aware ID and prevention scheme (TA-IDPS) for defending the network from adversary attacks. The presented technique comprises a cloud service layer, a MANET, and a cloudlet. In the initial stage, authenticate and register mobile nodes by means of light weighted symmetric cryptographic approach that is extremely appropriate for resource-constraint environment. In MANET, authentication, higher energy consumption, and scalability are significant problems that are tackled through the presented moth flame optimization (MFO) technetium. When CH received the data packet from the source nodes, they are categorized into suspicious, normal, and malicious with the help of DBN.

Prabhakaran and Kulandasamy [18] developed a hybrid semantic DL (HSDL) framework by incorporating LSTM, CNN, and SVM techniques. The semantic data existing in the network traffics are recognized by means of semantic layers called as Word2Vec embedding layers. The presented technique categorizes the intrusion existing in the text together with its respective attack types. The normal text without the trace of intrusion is encrypted with the innovative encryption standard (AES) procedure to improve the security of cloud storage, and the optimum key using the large key breaking time for AES approach is chosen by means of the crossover based mine blast optimization approach (CMBA).

Pham et al. [19] developed a light weighted IDS that transformed raw network traffics into representative images. Then, examining the features of malevolent network traffics of CSE-CIC-IDS2018 data. Later, adapt method for efficiently demonstrating these features into image dataset. A CNN based recognition technique is utilized for identifying malicious traffics within image dataset.Sun et al. [20] recommended a two-phase cyber intrusion security technique. Initially, SVM is utilized as a recognition system to determine suspected behaviors inside a smart meter. Next, the Temporal Failure Propagation Graph (TFPG) method is applied for generating attack routes to recognize attack events. At last, the presented technique is utilized for evaluating the similarity amongst pre-determined cyberattacks and detected abnormal events.

Manimurugan et al. [21] present a Crow Search Optimization approach with Adaptive Neuro-Fuzzy Inference System (CSO-ANFIS) employed. The ANFIS was an integration of fuzzy interference system and ANN, and to improve the efficiency of the presented technique. Yin et al. [22] proposed an advanced technique for Cybersecurity Solution based IDS for identifying malicious activities targeting the Distributed Network Protocol (DNP3) layer in the Supervisory Control and Data Acquisition (SCADA) system. Since Information and Communication Technology is interconnected with the grid, it is subjected to physical and cyberattacks due to the communication among the outside Internet environments and industrial control systems with IoT technique. Anitha Ruthet al. [23] developed an efficient technique for text dataset-based IDS and secured data storage. In the presented technique, input text documents are preprocessed and later changed to the preferred format. Now, user text data was checked; either the provided information was normal or intrusive depending on the modified ANN (MANN). Now, conventional NN is adapted by means of adapted PSO. Lastly, encrypt the file by means of dual encryption algorithms (AES and RSA).

Singh et al. [24] developed novel trust management using ECC approach. Initially, a trust manager is retained, the function is to categorize the trust into three distinct sets of trust levels depending on Schnorr’s signature and ECC in MANET. Every trust level has recognized a single attacker. Therefore, the presented technique has discovered 3 kinds of attackers namely selective packet dropping attack, black hole attack, and flooding attack. Vinayakumaret al. [25] DNN, a kind of DL technique, is examined for developing an efficient and flexible IDS to classify and detect unpredictable and unforeseen cyberattacks. The rapid evolution of attacks and constantly changing network behavior make them essential to estimate different data that are produced via static and dynamic techniques. This kind of approach facilitates recognizing the better technique which might efficiently work in identifying upcoming cyberattacks.

4. Results and Discussion

In this section, we assess the intrusion detection and encryption results of various models exist in the earlier studies.Table 1 and Fig. 2 offer the IDS outcomes of various models on KDDCup 99 dataset. The experimental outcomes implied that the GNB model has shown poor performance over other models. Next, the LR and SVM-rbf models have reported slightly raised classification results. Following by, the SGD and AB models have reported closer classifier results while the LDA and DT models have reached even improved outcomes. Finally, the KNN model has shown higher $accu_y$, $prec_n$, $reca_l$, and F_{score} of 0.8996, 0.8205, 0.5973, and 0.5705.

Table 1 IDS analysis of various approaches with distinct measures under KDDCup 99 dataset

Methods	Accuracy	Precision	Recall	F-Score
LR	0.8996	0.8205	0.5673	0.5705
LDA	0.9597	0.7423	0.7383	0.6758
KNN	0.9669	0.8890	0.8872	0.8880
DT	0.9775	0.9297	0.9280	0.9288
GNB	0.5920	0.4598	0.9820	0.5598
SGD	0.9143	0.6390	0.5512	0.5740
AB	0.9250	0.9960	0.9100	0.9510
SVM-rbf	0.8770	0.9940	0.8520	0.9180

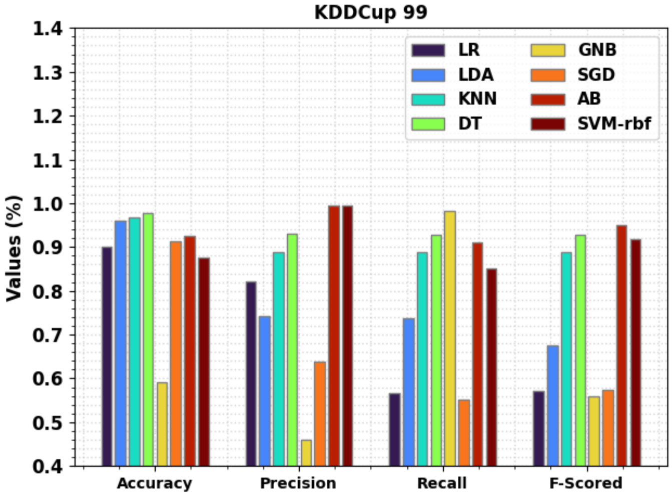

Fig. 2. IDS analysis of various approaches under KDDCup 99 dataset.

Table 2 IDS analysis of various approaches with distinct measures under NSL-KDD dataset

Methods	Accuracy	Precision	Recall	F-Scored
LR	0.8986	0.7985	0.5483	0.5565
LDA	0.9127	0.8552	0.5993	0.7572
KNN	0.9269	0.8840	0.9012	0.8850
DT	0.9595	0.9147	0.9740	0.9248
GNB	0.6170	0.4768	0.0130	0.5438
SGD	0.8843	0.6800	0.5292	0.6060
AB	0.9590	0.9890	0.8650	0.9630
SVM-rbf	0.9190	0.9010	0.8330	0.9670

Table 2 and Fig. 3 provide the IDS result of various algorithms on NSL-KDD dataset. The experimental result stated that the GNB approach has demonstrated the least performance over other techniques. Afterward, the LR and SVM-rbfsystems reported somewhat raised classification results. Moreover, the SGD and AB techniques have reported closer classifier results while the LDA and KNN algorithms have attained even higher outcomes. At last, the DT methodology has exhibited superior $accu_y$, $prec_n$, $reca_l$, and F_{score} of 0.9595, 0.9147, 0.9740, and 0.9248.

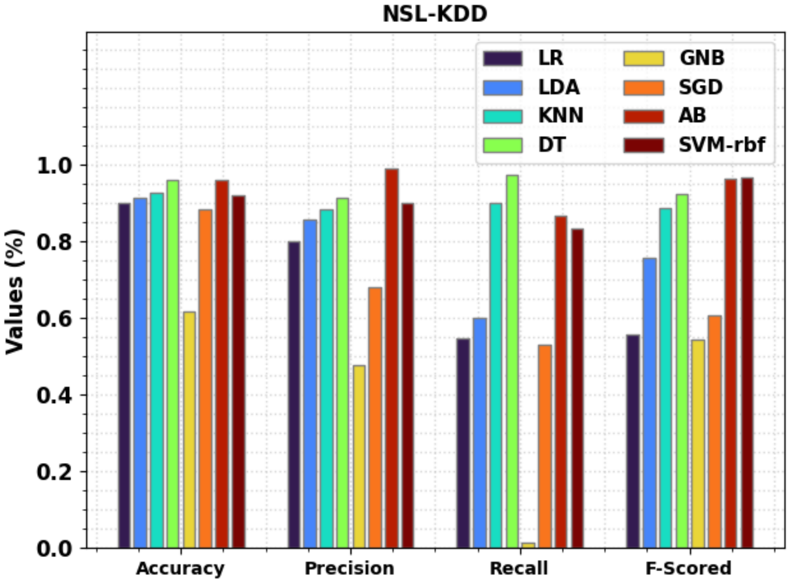

Fig. 3. IDS analysis of various approaches under NSL-KDD dataset

Table 3 provides a brief set of encryption results offered by different models [12, 15, 13, 25].

Fig. 4 portrays the MSE and RMSE assessment of various encryption techniques. The results implied that the AES and dual encryption-OFP models are found to be superior to other models. For instance, based on MSE, the Dual Encryption-OFP and AES technique have reached identical MSE of 0.020 whereas the RSA, ECC, ECC-GO, signcryption-AEHO, and HE-ALO models have resulted in MSE of 0.110, 0.100, 0.120, 0.090, and 0.060. Also, with respect to RMSE, the Dual Encryption-OFP and AES systems have reached similar RMSE of 0.141 whereas the RSA, ECC, ECC-GO, signcryption-AEHO, and HE-ALO methodologies have resulted in RMSE of 0.332, 0.316, 0.346, 0.300, and 0.245.

Table 3 Comparative analysis of various encryption techniques interms of MSE, RMSE, and PSNR

Methods	MSE	RMSE	PSNR
AES	0.020	0.141	65.121
RSA	0.110	0.332	57.717
ECC	0.100	0.316	58.131
ECC-GO	0.120	0.346	57.339
Signcryption-AEHO	0.090	0.300	58.588
HE-ALO	0.060	0.245	60.349

Dual Encryption-OFP	0.020	0.141	65.121

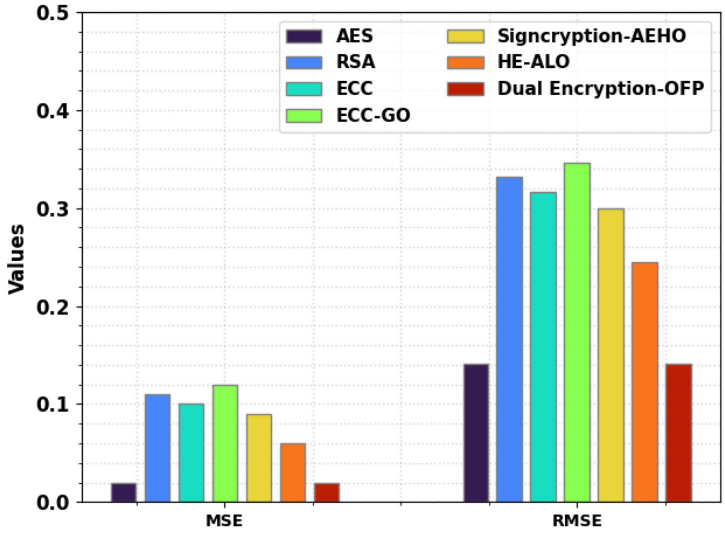

Fig. 4. MSE and RMSE analysis of various encryption techniques

Fig. 5 depicts the PNSR analysis of various encryption approaches. The outcomes revealed that the AES and dual encryption-OFP techniques are found that higher than other techniques. For sample, interms of PNSR, the Dual Encryption-OFP, and AES techniques have achieved same PSNR of 65.121dB whereas the RSA, ECC, ECC-GO, signcryption-AEHO, and HE-ALO algorithms have resulted in PSNR of 57.717dB, 58.131dB, 57.339dB, 58.588dB, and 60.349dB.

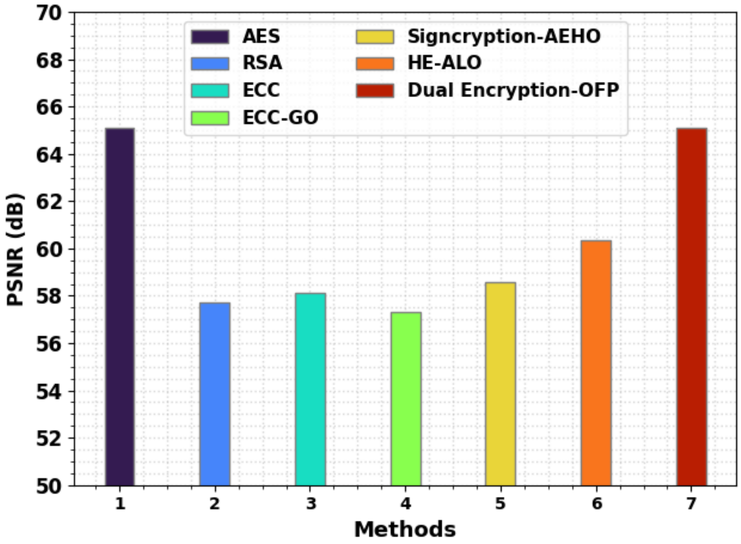

Fig. 5. PSNR analysis of various encryption techniques

5. Conclusion

Effective IDS and encryption schemes can be developed to secure network data. Recently, numerous research works have been developed for attaining network security. This paper performs a study of various AI techniques for IDS and encryption in network security. A detailed overview of various concepts involved in network security is elaborated. In addition, different IDS and encryption techniques can be derived to improve network efficiency. At last, a detailed experimental analysis is performed to demonstrate the performance of different models interms of different measures. In the future, lightweight cryptographic solutions with ensemble DL models can be designed to improve network security.

References

1. Papadogiannaki, E. and Ioannidis, S., 2021. Acceleration of intrusion detection in encrypted network traffic using heterogeneous hardware. *Sensors*, *21*(4), p.1140.
2. Mondal, A. and Goswami, R.T., 2021. Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. *Microprocessors and Microsystems*, *81*, p.103719.
3. Kim, W., Lee, J., Lee, Y., Kim, Y., Chung, J. and Woo, S., 2022. Vehicular Multilevel Data Arrangement-Based Intrusion Detection System for In-Vehicle CAN. *Security and Communication Networks*, *2022*.
4. Umba, S.M.W., Abu-Mahfouz, A.M., Ramotsoela, T.D. and Hancke, G.P., 2019, June. A review of artificial intelligence based intrusion detection for software-defined wireless sensor networks. In *2019 IEEE 28th International symposium on industrial electronics (ISIE)* (pp. 1277-1282). IEEE.

5. Laqtib, S., El Yassini, K. and Hasnaoui, M.L., 2020. A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. *International Journal of Electrical and Computer Engineering*, *10*(3), p.2701.
6. Gupta, A.S., Prasad, G.S. and Nayak, S.R., 2019. A new and secure intrusion detecting system for detection of anomalies within the big data. In *Cloud computing for geospatial big data analytics* (pp. 177-190). Springer, Cham.
7. Newaz, A.I., Sikder, A.K., Babun, L. and Uluagac, A.S., 2020, June. Heka: A novel intrusion detection system for attacks to personal medical devices. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.
8. Alves, T., Das, R. and Morris, T., 2018. Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *IEEE Embedded Systems Letters*, *10*(3), pp.99-102.
9. Bakir, C., 2022, June. New Hybrid Intrusion Detection and Prevention System to Ensure Security and Privacy in Big Data. In *2022 26th International Conference Electronics* (pp. 1-6). IEEE.
10. Bandecchi, S. and Dascalu, N., 2021. Intrusion Detection Scheme in Secure Zone Based System. *Journal of Computing and Natural Science*, pp.19-25.
11. Pascale, F., Adinolfi, E.A., Coppola, S. and Santonicola, E., 2021. Cybersecurity in automotive: An intrusion detection system in connected vehicles. *Electronics*, *10*(15), p.1765.
12. Shrestha, R., Omidkar, A., Roudi, S.A., Abbas, R. and Kim, S., 2021. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics*, *10*(13), p.1549.
13. Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2020. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, *32*(15), pp.10979-10993.
14. Kalyani, G. and Chaudhari, S., 2020. An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *International Journal of Computers and Applications*, *42*(3), pp.306-314.
15. Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M. and Sathesh Kumar, K., 2019. An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization. In *Cybersecurity and Secure Information Systems* (pp. 31-42). Springer, Cham.
16. Prabhakaran, V. and Kulandasamy, A., 2021. Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. *Computational Intelligence*, *37*(1), pp.344-370.
17. Alghamdi, S.A., 2022. Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud. *International Journal of Information Security*, *21*(3), pp.469-488.
18. Prabhakaran, V. and Kulandasamy, A., 2021. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. *Neural Computing and Applications*, *33*(21), pp.14459-14479.
19. Pham, V., Seo, E. and Chung, T.M., 2020. Lightweight Convolutional Neural Network Based Intrusion Detection System. *J. Commun.*, *15*(11), pp.808-817.
20. Sun, C.C., Cardenas, D.J.S., Hahn, A. and Liu, C.C., 2020. Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid*, *12*(1), pp.612-622.
21. Manimurugan, S., Majdi, A.Q., Mohmmed, M., Narmatha, C. and Varatharajan, R., 2020. Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system. *Microprocessors and Microsystems*, *79*, p.103261.
22. Yin, X.C., Liu, Z.G., Nkenyereye, L. and Ndibanje, B., 2019. Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. *Sensors*, *19*(22), p.4952.
23. Anitha Ruth, J., Sirmathi, H. and Meenakshi, A., 2019. Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks. *IET Information Security*, *13*(4), pp.321-329.
24. Singh, O., Singh, J. and Singh, R., 2018. Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. *Cluster Computing*, *21*(1), pp.51-63.
25. Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. and Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. *Ieee Access*, *7*, pp.41525-41550.