International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

REPEATER SECURITY-ENABLED INTRUSION DETECTION SCHEME FOR COMPUTER NETWORK USING A NOVEL DEEPTL-2ASHT-GRU AND C-KNN

Amaresan Venkatesan
v.amaresan@gmail.com

Abstract

In the modern era, the scope of the Computer Network (CN) has continuously evolved with increasing demands for data connectivity. Moreover, the security concern is an open challenge. But, secure maintenance of the Repeater Device (RD) in the CN was not concentrated in any of the prevailing works. Thus, a repeater security-enabled Intrusion Detection Scheme (IDS) for CN using Deep Transfer Learning-Alpine-Adaptive Slope Hyperbolic Tangent- Gated Recurrent Unit (DeepTL-2ASHT-GRU) and Chebanobis-based K-Nearest Neighbor (C-KNN) is proposed in this paper. Initially, the C-KNN-based mesh topology is created for internet users. Now, for the users, the unique session token is created. Next, the created token is sent to the targeted server. Then, the session token is fused with the user's data and then transmitted to the repeater side, where the IDS is performed. To perform attack prediction, the DeepTL-2ASHT-GRU is utilized. Also, to explain the detection outcomes, the Local Interpretable Model-agnostic Ellipsoid Explanation (LIM2E)-based deep plainer is integrated. Likewise, Super singular Isogeny-Koblitz Curve Cryptography (SIKCC) encrypts the normal data. Next, the encrypted data is retransmitted from the RD, followed by a firewall and router. After that, the token verification is carried out. Then, to capture the attacker's interaction, the honey pot is deployed in the network. Hence, the evaluation outcomes exhibited that the proposed mechanism had higher dominance with 98.99% accuracy.

Keywords *Computer Network (CN), Intrusion Detection Scheme (IDS), Repeater Device (RD), Deep Transfer Learning-Alpine-Adaptive Slope Hyperbolic Tangent- Gated Recurrent Unit (DeepTL-2ASHT-GRU), Chebanobis-based K-Nearest Neighbour (C-KNN), and explainable Artificial Intelligence (XAI).*

I. INTRODUCTION

Innovative applications for CNs have been developed by the rapid advancement in Internet technology (Sun et al., 2020). To transmit massive information, several devices are connected to the internet in the CN paradigm (Sun et al., 2021). Further, advancements in this field have fascinated many malicious threats that lead to huge data losses (Bhati et al., 2020)(Ayodeji et al., 2020). Therefore, IDS is important for ensuring secure data transmission (Masdari&Khezri, 2020). Hence, Artificial Intelligence (AI) emerges as a powerful tool for several applications, encompassing IDS (Drewek-Ossowicka et al., 2021).

Machine learning models, namely Decision Tree (DT) and Logistic Regression (LR) were established in the prevailing works to predict the network traffic and anomalies in the CN (Han et al., 2021)(Dini&Saponara, 2021). Also, to perform IDS in the CN, deep learning techniques like Convolutional Neural Network (CNN), Gated Recurrent Unit (GRU), and Deep Neural Network

(DNN) were established (Lee et al., 2021)(Yang et al., 2019). Nevertheless, security maintenance in the RD of the CN wasn't concentrated in any of the prevailing mechanisms. Hence, a repeater security-enabled IDS for CN is proposed using DeepTL-2ASHT-GRU and C-KNN in this article.

1.1 Problem statement

Conventional models' drawbacks are listed below:

- Existing frameworks didn't focus on reliable maintenance of the RD in CN.
- (Ozkan-Okay et al., 2021) failed to track the attacker's behavior, which degraded the security level.
- (Jevtic&Lanchier, 2020) had a single point of failure issue owing to the tree-based topology.
- Some of the traditional AI-based IDS were less reliable because of their black-box nature.

1.2 Objectives

The proposed technique's major contributions are given below:

- To provide security measures for RD, the proposed DeepTL-2ASHT-GRU-based IDS scheme and unique session key generation are established.
- To capture the attacker's interaction, an effective honeypot deployment is done.
- The C-KNN is employed to generate mesh network topology, thus enhancing the model's efficiency.
- To describe the detection results, a novel LIM2E is established.

The article's structure is given as: The related frameworks are examined in Section 2, the proposed IDS scheme is presented in Section 3, the proposed work's performance is assessed in Section 4, and Section 5 wraps up the paper.

II. LITERATURE SURVEY

(Jevtic&Lanchier, 2020) propounded a cyber-risk identification scheme for tree-centric local area network topology by utilizing a dynamic structural percolation model. To mitigate the complexity of cyber-risk phenomena efficiently, the percolation theory was established. But, owing to the tree-based topology, the model had a single point of failure issue.

(Latif et al., 2020) introduced a neural network-centric attack detection framework for the industrial Internet of Things paradigm. To predict different cyber threats, the lightweight random neural network was established. This model acquired maximum accuracy. However, it had high implementation complexity.

(Devan&Khare, 2020) presented a deep learning-centric network intrusion detection model. To perform feature selection and intrusion detection, extreme gradient boosting and deep neural networks were employed respectively. This technique had superior outcomes; however, it was inefficient because of its black-box nature.

(Ozkan-Okay et al., 2021) assessed a cyber-attack prediction-wide local area network centred on hybrid IDS. This work was assessed with KDD'99 and UNSW-NB15 datasets. Next, the optimal features were chosen, followed by intrusion detection. This framework considerably predicted the signature and anomaly-centric threats. But, this technique failed to track the attacker's activities.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

(Yang et al., 2020) explained a real-time IDS for wireless networks centered on deep learning mechanisms. To predict the various malicious threats proficiently, the Conditional Deep Belief Network (CDBN) was employed. Still, it had significant data loss owing to the dimensionality reduction.

III. PROPOSED METHODOLOGY FOR Deep-2ASHT-GRU AND C-KNN-BASED IDS FOR CN

Here, a repeater security-aware IDS for CN is implemented by utilizing DeepTL-2ASHT-GRU and C-KNN. Figure 1 exhibits the proposed mechanism's diagrammatic format.

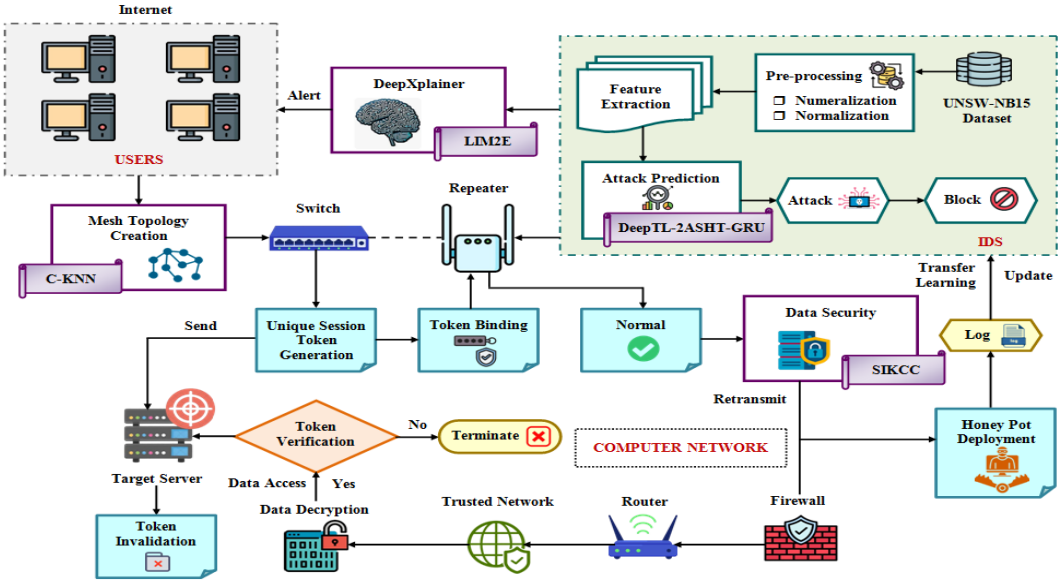


Figure 1: The structural depiction of the research methodology

3.1 Internet users

Initially, different kinds of users are connected to the network for sharing their information.

$$\varphi_y = \langle \varphi_1, \varphi_2, \ldots\ldots \varphi_Y \rangle \text{ Here, } y = 1 \, to \, Y \quad (1)$$

Here, Y signifies the number of internet users φ_y.

3.2 Mesh topology creation

Then, by utilizing the C-KNN, the mesh network topology is created from φ_y for elevating the communication efficacy. The KNN had high flexibility and adaptability. Still, it had suboptimal outcomes owing to the inappropriate distance metric. Thus, to increase the network reliability, the proposed technique employs the Chebanobis distance.

At first, the optimal k value (κ_Θ) is chosen from the data points φ_y. After that, the distance between the κ_Θ and φ_y is estimated using the chebanobis distance $(\partial\delta)$.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

$$\partial\delta\left(\kappa_{\Theta},\varphi_{y}\right)=\max_{y}\left(\left|\kappa_{\Theta}-\varphi_{y}\right|\right)\sqrt{\left(\kappa_{\Theta}-\varphi_{y}\right)^{T}\varsigma^{-1}\left(\kappa_{\Theta}-\varphi_{y}\right)} \quad (2)$$

Here, ς^{-1} is the covariance matrix. Next, centered on $\partial\delta$, the nearest neighbours are identified. The nearest neighbour (η) is the data point with the minimum distance to the k value. At last, the mesh network topology is created according to the η. Each user in the mesh network topology is connected to the CN's switch device.

3.3. Unique session token generation

Subsequently, the unique session token $(\aleph^{\circ})$is generated for the users via a random token generator. Moreover, to ensure transparency, the $\aleph^{\circ}$ is sent to the targeted server. Next, the token is fused with the user's request (λ). Further, the fused data $(\lambda_{\aleph^{\circ}})$is transferred to the repeater.

3.4 Intrusion detection system

Here, the IDS is established to maintain the security in the RD. The IDS is described further,

3.4.1 UNSW-NB15 dataset

Primarily, to implement the proposed IDS, the UNSW-NB15 dataset is collected from publically available resources. The input data is signified as (Z_{data}).

3.4.2 Pre-processing

Then, to elevate the data quality, the Z_{data} is pre-processed for nominalization and normalization. Initially, the Z_{data} is converted into numerical form (Num_{data}) via One-Hot Encoding (OHE). Then, the feature values in Num_{data} are transformed into 0s and 1s by utilizing min-max normalization.

$$\mathrm{P}\rightarrow\frac{Num_{data}-\min\left(Num_{data}\right)}{\max\left(Num_{data}\right)-\min\left(Num_{data}\right)} \quad (3)$$

Where, P is the pre-processed data.

3.4.3 Feature extraction

Next, to train the classifier model, the features like destination IP address, protocol, total bytes, total packets, and duration are extracted from P. Hence, the extracted features are symbolized as $(\Im_{g})$.

3.4.4 Attack prediction

Lastly, the $\Im_{g}$ is inputted into the proposed DeepTL-2ASHT-GRU, which predicts whether the data is normal or attacked. The long-term dependencies are efficiently captured by Deep-GRU. Still, due to improper activation and weight initialization, it had overfitting issues and vanishing gradient issues, correspondingly. Thus, to upgrade the classifier's efficacy, the proposed technique establishes the Alpine Function (AF) and Adaptive Slope Hyperbolic Tangent (ASHT) activation function. Figure 2 presents the proposed DeepTL-2ASHT-GRU's pictorial depiction.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

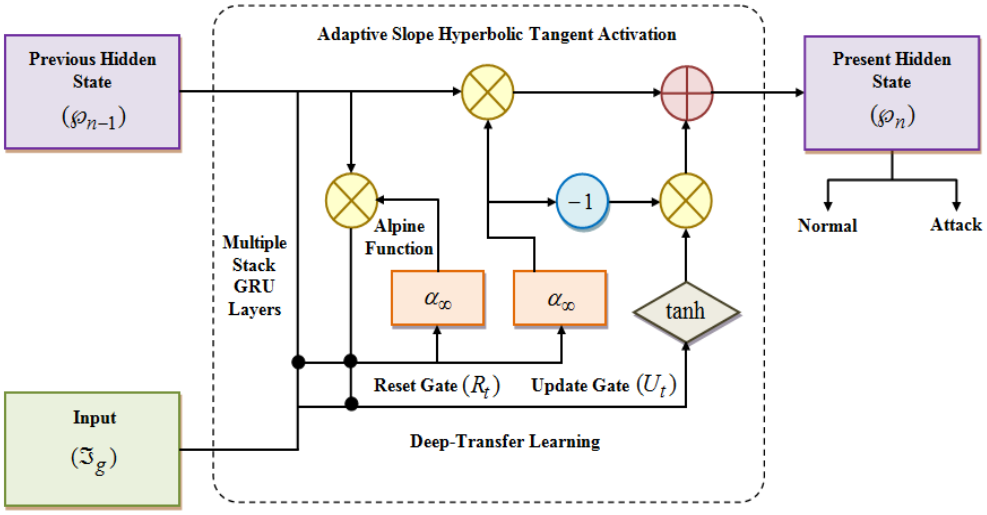


Figure 2: The architecture of the proposed DeepTL-2ASHT-GRU

- **Input:** Initially, the $\Im_g$ is transferred to the multiple stack GRU layers that perform classification tasks.

- **ASHT activation:** Here, to increase neurons' learning efficiency, the proposed technique uses the ASHT (α_∞).

$$\alpha_\infty(\Im_g) = \tanh(\ell^\circ{}_g \Im_g) \quad (4)$$

Where, $\ell^\circ{}_g$ is the learnable parameter.

- **Alpine function:** The proposed technique establishes AF to initialize the weight value (Wt), which enhances the classifier's performance.

$$Wt(\Im_g) = \sum_{g=1}^{G} \left| \Im_g \sin(\Im_g) + 0.1\Im_g \right| \quad (5)$$

- **Multiple stack GRU layers:** GRU layers' size is increased to learn more complex patterns, thus enhancing the model's capacity.
- **Reset gate:** The reset gate decides the information that is required to be forgotten.

$$R_t = \alpha_\infty(Wt \cdot (\wp_{n-1}, \Im_g)) + Bs \quad (6)$$

Here, $\wp_{n-1}$ is the previous hidden state, and Bs specifies the bias.

- **Update gate:** The update gate identifies the relevant information to be passed through the gates.

$$U_t = \alpha_\infty(Wt \cdot (\wp_{n-1}, \Im_g)) + Bs \quad (7)$$

- **Candidate hidden state:** Next, to capture the new information, the candidate hidden state

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

$(\hat{\wp}_n)$is utilized.

$$\hat{\wp}_n = \tanh\left(Wt \cdot \Im_g + R_t \otimes (U_t \cdot \wp_{n-1}) + Bs\right) \quad (8)$$

- **Hidden state:** Hence, the final hidden state $(\wp_n)$is given as,

$$\wp_n = (1 - U_t) \otimes \wp_{n-1} + U_t \otimes \hat{\wp}_n \quad (9)$$

- **Transfer learning:** Also, transfer learning is integrated to handle new threats. Hence, the proposed DeepTL-2ASHT-GRU effectively classifies the normal $(Norm)$and attacked (Att)data.

$$Out = \langle Norm, Att \rangle \quad (10)$$

Where, Out is the proposed DeepTL-2ASHT-GRU's outcome. The pseudo-code of the DeepTL-2ASHT-GRU is expressed below,

Input: Extracted features $\Im_g$
Output: Classified result Out
Begin
Initialize $\Im_g$, $\ell^\circ{}_g$, α_∞ and $\wp_n$
For 1 to each $\Im_g$ do,
Apply ASHT (α_∞)
Initialize weight Wt using AF
#multiple stack GRU layers
Perform reset gate
$R_t = \alpha_\infty\left(Wt \cdot \left(\wp_{n-1}, \Im_g\right)\right) + Bs$
Execute update gate $U_t = \alpha_\infty\left(Wt \cdot \left(\wp_{n-1}, \Im_g\right)\right) + Bs$
Determine hidden state $\wp_n = (1 - U_t) \otimes \wp_{n-1} + U_t \otimes \hat{\wp}_n$
Integrate transfer learning
IF (actual == target)
{
Terminate
}
Else
{
Back propagation
}
End IF
End For
Return $Out = \langle Norm, Att \rangle$
End

Thus, the Out is fed into the DeepXplainer.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

3.5 DeepXplainer

Here, to describe Out, the LIM2E-centric DeepXplainer is established, which helps the users to fix the issues effectively. The potential biases or errors are efficiently outlined by LIME. Still, it had suboptimal outcomes owing to the inappropriate kernel function. Thus, to increase the system's reliability, the proposed model employs the Ellipsoid Function (EF).

Initially, the instances Out are chosen to initiate the LIME process. Hence, to generate a new dataset of similar instances (ψ_o), the chosen instances are augmented. Next, the weight value (ϖ_Δ) is assigned to each instance via EF.

$$\varpi_\Delta = \sum_{o=1}^{O} 10^{6\cdot\frac{o-1}{O-1}} \psi_o^2 \tag{11}$$

Here, O signifies the number of instances. Next, the weighted dataset is utilized to train the local model, which interprets the complex model. The local model's coefficient is examined to highlight the features that influenced the decision. Finally, the description is utilized to alert the users. Here, the attacked data is blocked from the network, while the normal data is subjected to succeeding mechanisms.

3.6 Data security

Now, to ensure high security, the $Norm$ is encrypted by using the SIKCC. The ECC had faster encryption and decryption. Still, it had computational complexity owing to the traditional elliptic curve. Thus, to upgrade the security level, the proposed work establishes the Supersingular Isogeny-Koblitz Curve (SIKC). Therefore, the SIKC $(\delta\iota\kappa)$ is formulated as,

$$\delta\iota\kappa \rightarrow C^2 = D^6 + 2aC + b \tag{12}$$

Where, C and D are the curve coefficients, and a and b are the constant values.

- **Key generation:** Next, to perform encryption and decryption, the key generation is carried out. Here, the private key is randomly generated. Next, the public key (K) is created and is given as,

$$\mathrm{K} = \mathrm{X}\cdot\tau(\delta\iota\kappa); \qquad (1 \le \mathrm{X} \le \lambda - 1) \tag{13}$$

Here, λ is the maximum range, and τ is the curve parameter.

- **Encryption:** Subsequently, the two cipher texts are utilized to encrypt the data.

$$v_1 = j * \tau \tag{14}$$

$$v_2 = Norm + j \times \mathrm{X} \tag{15}$$

Where, j is the random value and v_1 and v_2 signify the cipher text 1 and cipher text 2, correspondingly.

- **Decryption:** Conversely, the decryption process is expressed as,
-

$$Norm = v_2 - \mathrm{X}\cdot v_1 \tag{16}$$

$$v_h = (v_1, v_2, \ldots\ldots v_H)$$

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

(17)

Here, $h = 1,2,\ldots H$ signifies the number of encrypted data (ν_h). The pseudo-code of the proposed SIKCC is expressed as,

Input: Normal data *Norm*
Output: Encrypted data ν_h
Begin
Initialize $\delta\iota\kappa$, τ, a and b
For 1 to each *Norm* do,
Define SKIC curve
$\delta\iota\kappa \rightarrow C^2 = D^6 + 2aC + b$
Perform key generation,
$\mathrm{K} = \mathrm{X} \cdot \tau(\delta\iota\kappa); \qquad (1 \le \mathrm{X} \le \lambda - 1)$
Encrypt data
Execute decryption
End For
Return ν_h
End

Now, the ν_h is retransmitted from the repeater $(\Re\Diamond)$ to the firewall (Ξ) reliably.

$$\Re\Diamond \xrightarrow[\nu_h]{retransmit} \Xi \tag{18}$$

In general, the network traffic is controlled by a firewall regarding predetermined security measures. Next, the firewall sends data to the trusted network (πrst) via a router.

$$\Xi \xrightarrow[Router]{send} \pi rst \tag{19}$$

Now, the targeted server decrypts the data, followed by session token verification.

3.7 Token verification

Here, by checking whether the session token is presented in the server (Svr) or not, the token verification is done. If the token (Tkn) is presented, then the data is accessed. Otherwise, the data is terminated.

$$Tkn \xrightarrow{verify} \begin{cases} IF(\aleph^\circ == Svr), & access \\ ELSE, & deny \end{cases} \tag{20}$$

Moreover, to prevent reuse, the session token invalidation is done.

3.8 Honeypot deployment

After that, to capture the interaction and activities of the intruders, the honey pot is deployed in the network. Next, to update the IDS via transfer learning, the outcomes from a honeypot are utilized. The proposed technique proficiently increases the CN's performance and reliability.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

IV. RESULTS AND DISCUSSION

Here, the proposed work's trustworthiness is assessed. Here, the proposed model's implementation is done on the working platform of PYTHON.

4.1 Dataset description

The UNSW-NB15 dataset is employed to evaluate the proposed IDS, and it involves vital features of the network traffic. From the total data, 80% of data are used to perform training and 20% of data are to perform testing.

4.2 Performance assessment

The proposed scheme's reliability is validated via the performance assessment, which is exhibited below,

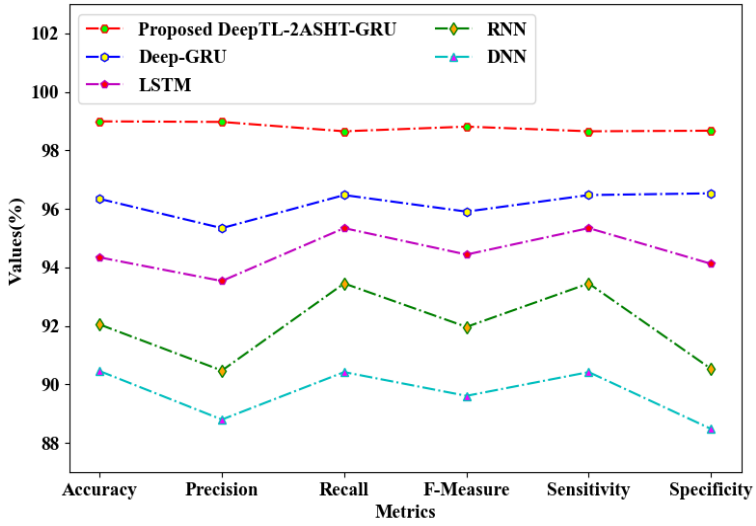


Figure 3:Performance validation for attack classification

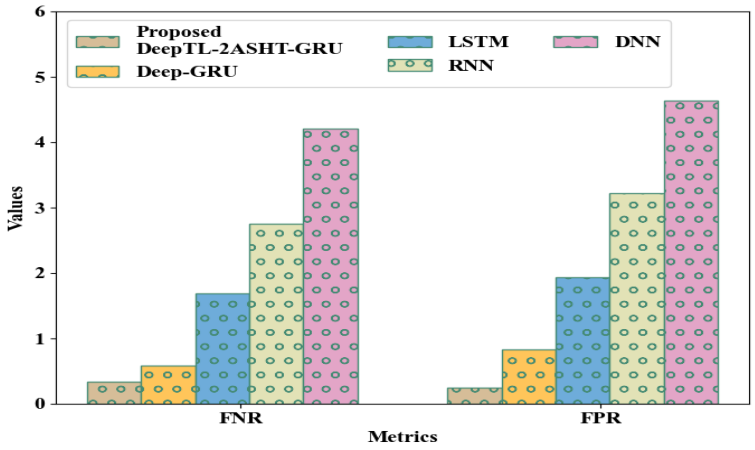


Figure 4: FNR and FPR analysis

In Figures 3 and 4, the performance analysis of the proposed DeepTL-2ASHT-GRU and prevailing Deep-GRU, Long Short Term Memory (LSTM), Recurrent Neural Network (RNN), and DNN is displayed. Accuracy, precision, recall, f-measure, sensitivity, specificity, False Negative Rate

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

(FNR), and False Positive Rate (FPR) of the proposed technique are 98.99%, 98.97%, 98.65%, 98.81%, 98.65%, 98.67%, 0.332, and 0.249, correspondingly. Similarly, the prevailing DNN attained 90.45% accuracy, 88.79% precision, 90.42% recall, 89.60% f-measure, 90.42% sensitivity, 88.47% specificity, 4.212 FNR, and 4.632 FPR. Hence, owing to the ASHT activation, the proposed model had higher prominence.

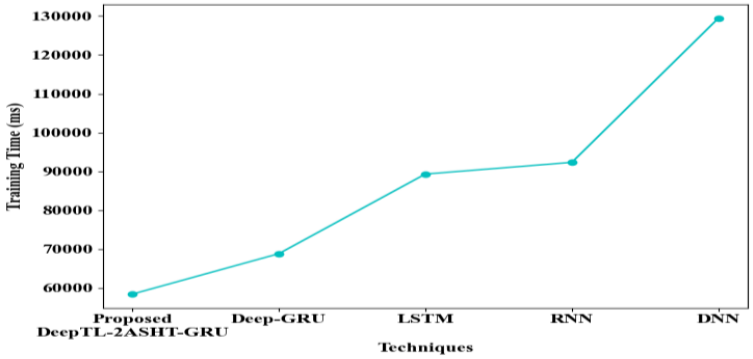


Figure 5: Training time

The Training Time (TT) of the proposed DeepTL-2ASHT-GRU as well as conventional classifiers is examined in Figure 5. The proposed DeepTL-2ASHT-GRU obtained a TT of 58374ms, while the prevailing techniques acquired a mean TT of 94965ms. The proposed method's performance is improved owing to the AF.

Table 1: Comparative analysis

Methods	Fidelity	Sparsity
Proposed LIM2E	0.973	0.985
LIME	0.736	0.634
SHAP	0.538	0.457
PDP	0.342	0.273
GS	0.223	0.142

Table 2: Stability score validation

Methods	Stability
Proposed LIM2E	0.993
LIME	0.662
SHAP	0.422
PDP	0.253
GS	0.123

EF's presence aids in enhancing the model's outcomes. The performance of the proposed LIM2E and prevailing algorithms like the SHaplety Additive exPlanations (SHAP), LIME, Global Surrogate (GS), and Partial Dependence Plot (PDP) is assessed in Tables 1 and 2. The proposed

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

LIM2E obtained fidelity, sparsity, and stability of 0.973, 0.985, and 0.993, correspondingly. Still, due to the improper weight assignment, the traditional algorithms had limited outcomes. Therefore, the proposed technique was more efficient than the prevailing models.

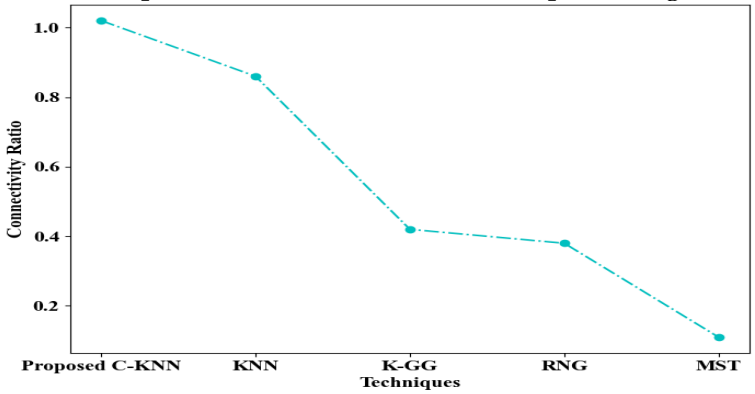


Figure 6: Connectivity ratio

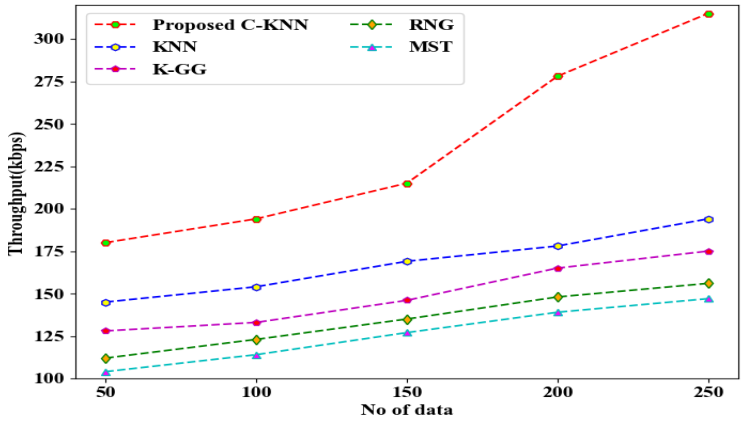
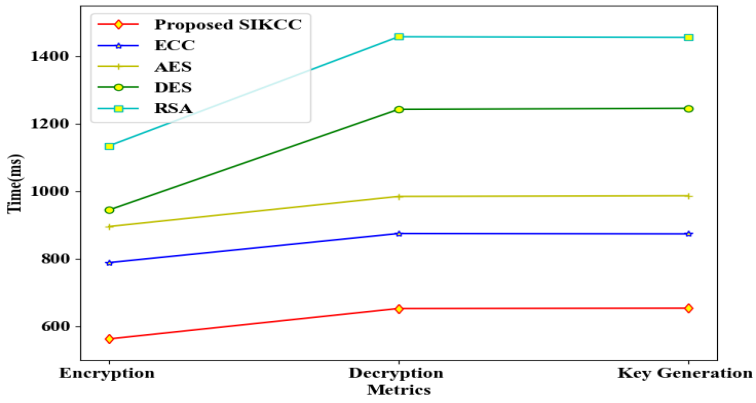


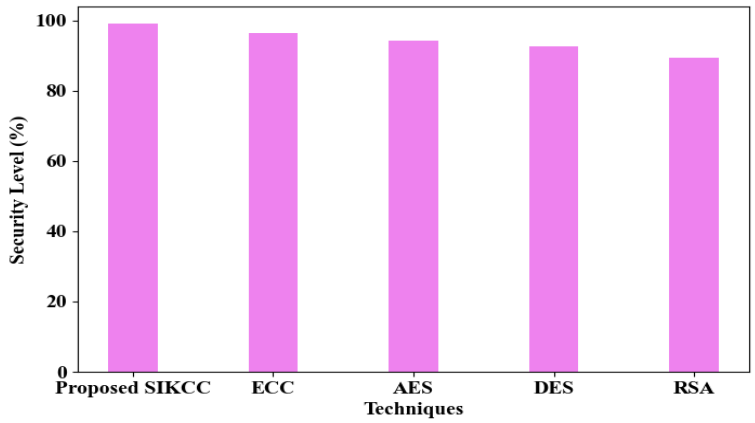
Figure 7: Throughput evaluation

In Figures 6 and 7, the Connectivity Ratio (CR) and throughput of the proposed C-KNN and existing methods like KNN, K-Gabriel Graph (K-GG), Relative Neighbourhood Graph (RNG), and Minimum Spanning Tree (MST) are evaluated correspondingly. The proposed C-KNN acquired a CR of 1.02, while the conventional methods achieved an average CR of 0.44. Similarly, the proposed C-KNN achieved throughput of 180Kbps and 315Kbps for 50 and 250 number of data, correspondingly. Yet, the traditional techniques had minimum throughput. Owing to the chebanobis distance, the proposed technique had higher superiority



International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

(a)



(b)

Figure 8: Performance analysis for data security regarding (a) ET, DT, and KGT and (b) security level

Figure 8 evaluates the performance of the proposed SIKCC by analogizing it with conventional methods, such as ECC, Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA). The Encryption Time (ET), Decryption Time (DT), Key Generation Time (KGT), and Security Level (SL) of the proposed SIKCC are 654ms, 653ms, 563ms, and 98.97%, correspondingly. Likewise, the traditional approaches achieved an average ET, DT, KGT, and SL of 1140ms, 1140ms, 941ms, and 93.15%, correspondingly. Hence, the analysis outcomes exhibited that the proposed model had a higher security rate and lower time complexity.

4.3 Comparative analysis

By comparing the proposed work with related models, a comparative assessment is done.

Table 3: Comparative validation

Author's name	Technique	Accuracy (%)	F-measure (%)
Proposed work	DeepTL-2ASHT-GRU and C-KNN	98.99	98.81
(Mebawondu et al., 2020)	Multi-Layer Perceptron (MLP)	76.96	-
(Bertoli et al., 2021)	Ensemble-ML		95
(Khare et al., 2020)	DNN	95.7	96.15
(Liu et al., 2021)	Hybrid-ML and DL	86.56	84.92
(Zhao et al., 2020)	MLP-neural network	97	-

In Table 3, the performances of the proposed model and associated frameworks are compared. Owing to the AF and ASHT, the proposed technique's performance is improved. The proposed DeepTL-2ASHT-GRU attained maximum accuracy (98.99%) and f-measure (98.81%). Still, the conventional DNN achieved 95.7% accuracy and 96.15% f-measure. Hence, the comparative analysis displayed the proposed work's efficacy.

V. CONCLUSION

Here, a repeater security-enabled intrusion detection scheme for CNs is proposed based on DeepTL-2ASHT-GRU and C-KNN. The mesh topology is efficiently created by the proposed C-KNN, which elevates the model's performance. Likewise, to effectively perform attack classification in the RD, the proposed DeepTL-2ASHT-GRU was established. Also, the system's reliability was elevated by unique session key generation and honeypot deployment. According to the experimental outcomes, the proposed DeepTL-2ASHT-GRU attained 98.99% accuracy and 58374ms TT, which exhibits better efficiency and low time complexity. Moreover, the proposed C-KNN achieved a coverage ratio of 1.02. Lastly, the proposed scheme effectively enhanced the CN's consistency and performance via AI techniques. Still, this system concentrated only on the CN's security measures.

Future scope: To ensure high reliability, advanced nature-inspired algorithms will be employed in the future to manage the transmitted loads in the CN.

REFERENCES

1. Dataset: https://research.unsw.edu.au/projects/unsw-nb15-dataset
2. Ayodeji, A., Liu, Y. kuo, Chao, N., & Yang, L. qun.(2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems.Nuclear Engineering and Technology, 52(12), 2687–2698. https://doi.org/10.1016/j.net.2020.05.012
3. Bertoli, G. D. C., Junior, L. A. P., Saotome, O., Santos, A. L. Dos, Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., & Oliveira, J. M. P. De. (2021). An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System. IEEE Access, 9, 106790–106805. https://doi.org/10.1109/ACCESS.2021.3101188
4. Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020).An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers and Electrical Engineering, 86, 1–9. https://doi.org/10.1016/j.compeleceng.2020.106742
5. Devan, P., &Khare, N. (2020). An efficient XGBoost–DNN-based classification model for network intrusion detection system.Neural Computing and Applications, 32(16), 1–16. https://doi.org/10.1007/s00521-020-04708-x
6. Dini, P., &Saponara, S. (2021). Analysis, design, and comparison of machine-learning techniques for networking intrusion detection.Designs, 5(1), 1–22. https://doi.org/10.3390/designs5010009
7. Drewek-Ossowicka, A., Pietrołaj, M., &Rumiński, J. (2021).A survey of neural networks usage for intrusion detection systems.Journal of Ambient Intelligence and Humanized Computing, 12(1), 497–514. https://doi.org/10.1007/s12652-020-02014-x
8. Han, D., Wang, Z., Zhong, Y., Chen, W., Yang, J., Lu, S., Shi, X., & Yin, X. (2021). Evaluating and Improving Adversarial Robustness of Machine Learning-Based Network Intrusion Detectors. IEEE Journal on Selected Areas in Communications, 39(8), 1–16. https://doi.org/10.1109/JSAC.2021.3087242
9. Jevtic, P., &Lanchier, N. (2020).Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology.Insurance: Mathematics and Economics, 91, 1–30. https://doi.org/10.1016/j.insmatheco.2020.02.005
10. Khare, N., Devan, P., Chowdhary, C. L., Bhattacharya, S., Singh, G., Singh, S., & Yoon, B.

(2020). SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. Electronics (Switzerland), 9(4), 1–18. https://doi.org/10.3390/electronics9040692

11. Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020).A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network.IEEE Access, 8, 89337–89350. https://doi.org/10.1109/ACCESS.2020.2994079
12. Lee, S. W., Sidqi, H. M., Mohammadi, M., Rashidi, S., Rahmani, A. M., Masdari, M., &Hosseinzadeh, M. (2021).Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review.Journal of Network and Computer Applications, 187, 1–22. https://doi.org/10.1016/j.jnca.2021.103111
13. Liu, L., Wang, P., Lin, J., & Liu, L. (2021). Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning. IEEE Access, 9, 7550–7563. https://doi.org/10.1109/ACCESS.2020.3048198
14. Masdari, M., &Khezri, H. (2020).A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems.Applied Soft Computing Journal, 92, 1–31.https://doi.org/10.1016/j.asoc.2020.106301
15. Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., &Adetunmbi, A. O. (2020). Network intrusion detection system using supervised learning paradigm.Scientific African, 9, 1–11. https://doi.org/10.1016/j.sciaf.2020.e00497
16. Ozkan-Okay, M., Aslan, O., Eryigit, R., &Samet, R. (2021). SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN. IEEE Access, 9, 157639–157653. https://doi.org/10.1109/ACCESS.2021.3129600
17. Sun, Y., Ochiai, H., & Esaki, H. (2020).Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs.Proceedings of the International Joint Conference on Neural Networks, 1–8. https://doi.org/10.1109/IJCNN48605.2020.9207094
18. Sun, Y., Ochiai, H., & Esaki, H. (2021).Intrusion Measurement and Detection in LAN Using Protocol-Wise Associative Memory.3rd International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2021, 5–9. https://doi.org/10.1109/ICAIIC51459.2021.9415195
19. Yang, H., Cheng, L., &Chuah, M. C. (2019).Deep-Learning-Based Network Intrusion Detection for SCADA Systems.IEEE Conference on Communications and Network Security, 1–7.
20. Yang, L., Li, J., Yin, L., Sun, Z., Zhao, Y., & Li, Z. (2020). Real-time intrusion detection in wireless network: A deep learning-based intelligent mechanism. IEEE Access, 8, 170128–170139. https://doi.org/10.1109/ACCESS.2020.3019973
21. Zhao, H., Li, M., & Zhao, H. (2020). Artificial intelligence based ensemble approach for intrusion detection systems. Journal of Visual Communication and Image Representation, 71, 1–25. https://doi.org/10.1016/j.jvcir.2019.102736