Keywords
Intrusion detection systems, Liquid Time Consatant Neural networks, Runge-Kutta method, Euler method, Discrete and Continuous time neural dynamics.

Authors
Venkata Ramani Varanasi[1*], Reasearch Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. :varanasivenkataramani@gmail.com

Shaik Razia[2], Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.

Received:27-06-2026
Revised:30-07-2026
Accepted:05-08-2026
Doi:10.1922/ejprd.v34i7s.1717

European Journal of Prosthodontics and Restorative Dentistry (2026) 34(7s), 984–992

Liquid Time-Constant Neural Networks with Runge Kutta and Euler Solvers for High-Accuracy Intrusion Detection

Abstract
A Liquid time constant neural network-based intrusion detection sytem (LTCNN-IDS), is an innovative approach for optimizing the feature extraction process to enhance the performance of intrusion detection systems. To simulate the continuous-time dynamics of LTCNNs, the authors combined intrinsic differential equations that regulate neuronal state evolution. While existing work has mostly used discrete time-based Recurrent neural network variations such as Long short-term memory, this study investigates the use of basic first-order solvers such as Euler's method, and the fourth order solver, the Runge-Kutta method (RK4) in the LTCNN architecture. The Euler method is one of the simplest and most intuitive method for numerically solving ordinary differential equations (ODEs). It is particularly useful in neural models such as LTCNNs, where the dynamics of neurons are described by differential equations. This allows the simulation of continuous-time neural dynamics in discrete-time steps, where the RK4 solver uses a higher-order approximation of latent dynamics, resulting in more accurate and stable updates throughout the temporal integration. Including RK4 in the network architecture enables end-to-end training of latent ODE-based systems, combining the interpretability of dynamical systems with the flexibility of deep learning. The performance of the proposed technique is compared with that of LSTM. The results exhibited an accuracy exceeding 0.99.

INTRODUCTION

The purpose of an Intrusion detection system (IDS) is to alert the systems administrator of any malicious attacks in the network that can aid in taking actions to alleviate risks and safeguard network security. Currently, researchers to detect malicious activities in networks utilize deep learning methods. Nevertheless, these models might find it difficult to adjust to extremely dynamic and inconsistent temporal patterns that define the actual network traffic.

Background

A recurrent neural network (RNN) is a neural network designed to handle sequential data by processing information over time. The main disadvantage of RNN is that they may lead to vanishing and exploding gradient problem with backpropagation. Long short-term memory (LSTM) architectures can be used to overcome these vanishing or exploding gradient problems where gates are used to memorize long-term dependencies [1]. LSTM was introduced in 2017 by K Greff known by the name of "LSTM: a space search odyssey" [2], similarly GRU was invented in 2018, by Guizhu Shen and others [3] for financial accounting issues.

Liquid Neural Networks also referred to as LNNs functions on a comparable framework; however, it employs methods for solving Ordinary Differential Equations (ODE), recognized for their speed in current computing generation. The team at the MIT Computer Science and Artificial Intelligence Lab, led by Ramin Hasani, created liquid neural networks, that could significantly enhance the adaptability of AI technology post-training, particularly when applied to real-world inference tasks [4].

Liquid neural networks are made of Liquid time constant cells. LTCNN is a type of RNN designed for modelling complex temporal dependencies of sequential, time-series data through real-time adaptation of their internal structure. Unlike conventional RNNs such as LSTMs or GRUs, LTCNNs use continuous-time models with learnable neuronal dynamics, making them highly effective for irregular or asynchronous time-series data. The actual implementation of the LTC layer involves solving differential equations for state transitions using liquid dynamics [5].

To model the continuous-time behaviour of Liquid Time-Constant Neural Networks (LTCNNs), the authors combine internal differential equations that dictate how neuron states change. Previous approaches mostly used LSTMs, but this study examines how to integrate basic first-order techniques such as Euler's method, and fourth-order technique such as the Runge-Kutta method (RK4) into the LTCNN framework. The RK4 technique offers a more precise approximation of hidden dynamics, resulting in better and more dependable updates during the time integration process. This enhancement improves the modelling of long-term relationships and creates richer temporal representations, which are particularly important for time-series applications such as intrusion detection. By incorporating RK4 into the network framework, we allow for complete training of latent ODE-based systems, merging the clarity of dynamic systems with the adaptability of deep learning.

Highlights

- A novel Liquid neural network model (LTCNN-IDS) is developed to detect intrusions within the network.
- RK4 method of ODE solver is used for implementing the model.
- Compared with Euler method of ODE solvers.
- Compared with Non-ODE based LSTM

Literature Survey

Kramarczyk et al [6] introduced a different approach to detect intrusions in IoT-H networks. They developed Liquid NeorIoTic, an intrusion detection system designed specifically for IoT-H networks utilizing an LNN. The findings from their experiments indicated that the LNN could minimize neurons by up to 40% and epochs by up to 64% compared to the leading ANN and RNN models.

Pendyala et.al [7] presented a model for explainable predictions that integrated as LTCN with symbolic regression to estimate link quality. This approach serves as an alternative to traditional methods such as RNN and LSTM. The authors evaluated the model and the findings indicated that the LTCN achieved performance levels that surpassed LSTM by a factor of 13.

Hasani et.al [8] introduced a continuous-time neural network in a closed form, which consisted of Liquid Time-Constant (LTC) layers and was crucial for advancements in this field. This method simulates the interactions between neurons and synapses within a continuous time context, surpassing traditional RNNs in several areas, particularly in handling time series and irregular datasets. The author tested approach across various datasets for different tasks, including classification and prediction. The experimental findings indicated that the model achieved speeds that were 1-5 times faster than the numeric solver, while maintaining comparable performance levels.

Chen et.al [9] introduced the idea of RK-style solvers in different models.

Kidger, P. et.al [10] exhibited the impact of the solver choice on the model accuracy.

Material and Methods

Liquid Time Constant Neural Network (LTCN)

LTCN models dynamics as differential equations (ODEs), offers continuous time flexibility but requires numerical integration.

For a generic ODE:

$$dh(t) / dt = f(h(t),x(t),\theta) \quad \text{------- (1)}$$

Numerical solvers such as Euler or Runge-Kutta methods can be used to simulate the models.

Euler method of solving ODE: [11]

According to a first-order differential equation,

For the hidden state h(t),

$$dht/dt=-ht+Win, xt+Wrecht+b/\tau \quad \text{------- (2)}$$

Euler based update with time constant,

ht+1=ht+Δtτht+Win,xt+Wrecht+b ------- (3)
ht - hidden state at time t
xt - input vector at time t
Win - input weight matrix
Wrec - Recurrent (hidden-to-hidden) weights
b - bias vector
tau - Time constant (controls decay rate)
Delta t - Integration step size (e.g., 0.01)
f(xt,ht): neural update function (e.g., a small MLP or linear layer)
f(xt,ht) = - ht + Win xt + Wrec ht + b

Runge-Kutta method of solving ODE: [11]
The 4th-order Runge-Kutta (RK4) method approximates h t+1 as:
k1=fht, xt
k2=fht+Δtk1/2,xt
k3=fht+Δtk2/2xt
k4=fht+Δtk3,xt
ht+1=ht+Δt6k1+2k2+2k3+k4 ----------(4)

This gives the final hidden state, which is then passed to a classifier:
y = softmaxWout hT+b ---------(5)

Long Short Term Memory (LSTM)
LSTM models dicrete recurrence equations and update states via gates, and no ODEs. LSTM updates the cell state C and avoids vanishing/exploding gradients to learn long-term dependencies without gradient issues.
For continuous-time systems, LTCNs replace C with ODE-based dynamics.
Forget Gate: ft=σWf .ht−1,xt+bf
Input Gate: it=σWi .ht−1,xt+bi
Output Gate: ot =σWo. ht−1,xt+b0
Candidate Cell State: gt=tanhWght−1, xt+bg
Cell State Update: Ct=ft⊙Ct−1+it⊙gt
Hidden State: ht=ot⊙tanhCt

Figure 1 provides a diagrammatic representation of the update procedures for each of the three approaches (LSTM, Euler, and RK4).

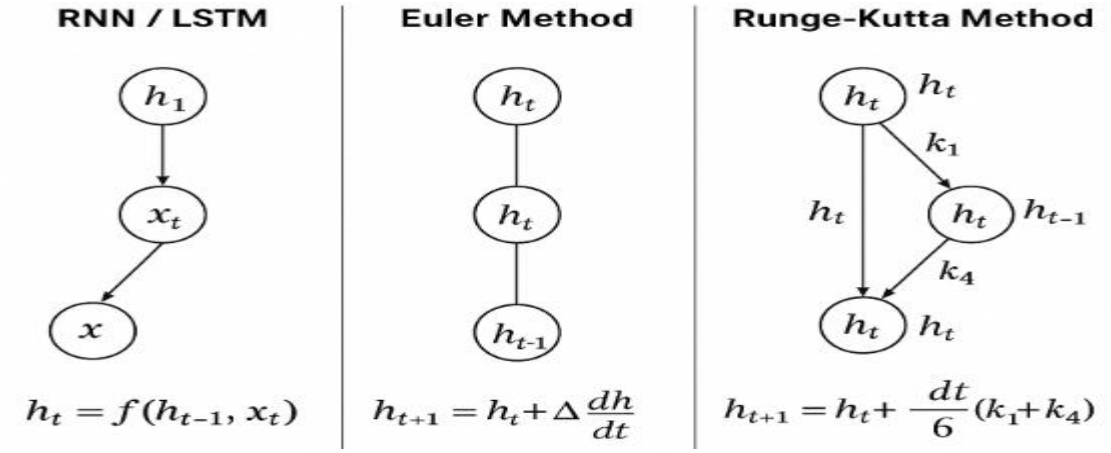

Figure 1: Update steps for LSTM, Euler-based LTCNN and RK4-based LTCNN

Importance of Neural Dynamics in Cyber security
1. Comprehending Neural Dynamics
The term neural dynamics describes how do the neural states change over time in a network, particularly in the models such as Liquid Time-Constant Neural Networks (LTCNNs) or Neural ODEs, which are affected by differential equations. These dynamics regulate how information flows, decays, or accumulates over time within a neural system. Models with neural dynamics continuously monitor the impact of inputs on internal states, in contrast to static models or those that update states in discrete time intervals (such as conventional feedforward networks or even LSTMs). This reflects a more realistic and responsive mechanism, which is particularly helpful for time-sensitive data.
2. Application in Cybersecurity
In the cybersecurity field, particularly in intrusion detection systems (IDS), the data is Time-dependent and sequential, Noisy and Variable, Unpredictable in terms of the timing and frequency of attacks. The ways in which neural dynamics can help are listed below:
a. Representing Changes over Time or Modelling Temporal Behaviour
Attacks such as DDoS, slow infiltration, and port scanning. exhibit temporal signatures. Neural dynamics models are able to respond adaptably to varying time intervals and keep or discard information according to the frequency or significance of input.
b. Early Threat Detection
Reactive security is enabled by the ability of dynamic systems to notice slight deviations in behavioural patterns that may indicate an imminent attack (e.g., several failed login attempts prior to a brute-force attack).
c. Lower False Positives
Models with neural dynamics are more effective at differentiating between actual threats and harmless anomalies, which lowers the frequency of false alerts by recording complicated temporal linkages.
d. Biological Inspiration
The manner in which neurons in the brain function over time serves as the foundation for LTCNNs and other similar models. This level of biological realism enables reliable pattern identification in complex and unpredictable circumstances, such as network traffic.

III. Proposed Methodology
The proposed methods Euler, RK4 were implemented in Python using CICIDS 2017 dataset. The CICIDS

2017[12] dataset contain packet flows data captured for one week in the form of CSV files and was used in this study [13]. This data underwent pre-processing, self-assembly of model architecture, training, validation and testing phases and different metrics were considered for comparison with the baseline LSTM model. The flowchart for this study is shown in Figure-2.

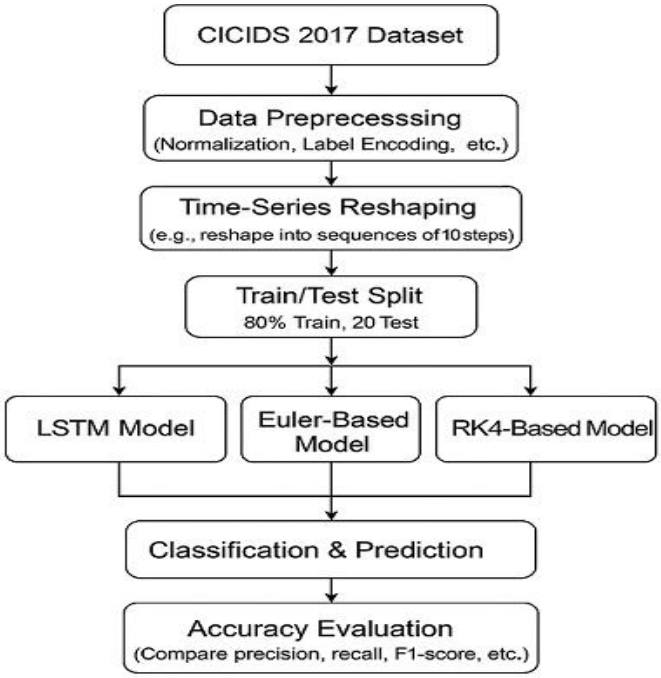

Figure 2: Flowchart of this study

IV. Experimentation and Result Discussion

Under data pre-processing, duplicate data elimination, infinity values and null data elimination, normalization, data balancing, data reshaping into sequences of 10 steps, and train-test splitting. Figure3 displays the number of samples obtained for this study after balancing the data. Then, the proposed LTCNN method was implemented using Euler and RK4, evaluated, and compared with the baseline LSTM method.

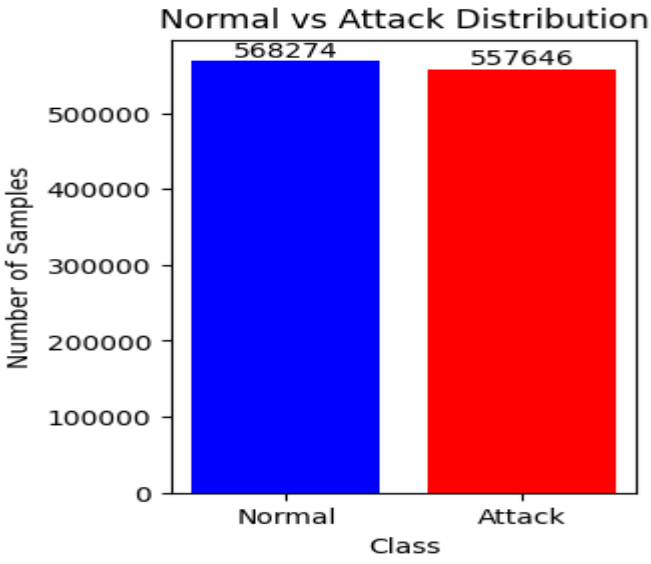

Figure 3: Balanced Data Samples Considered For Experimentation

Figure 4, 5, 6 shows the image graph plotting training and validation accuracy over epochs and training and validation loss over epochs for an intrusion detection system using the LTCNN and LSTM. The training accuracy is consistently high (near 1.0), indicating that the model fits the training data well. The validation accuracy also increases and reaches stability over the epochs, which improves generalization and ensures the reliable detection of network intrusions.

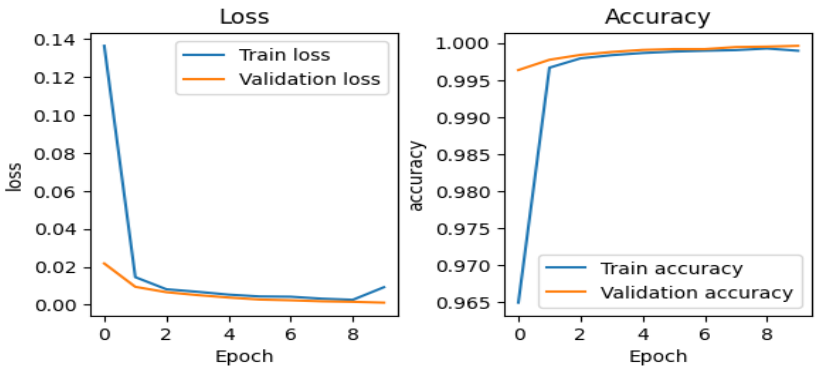

Figure 4: Euler Method

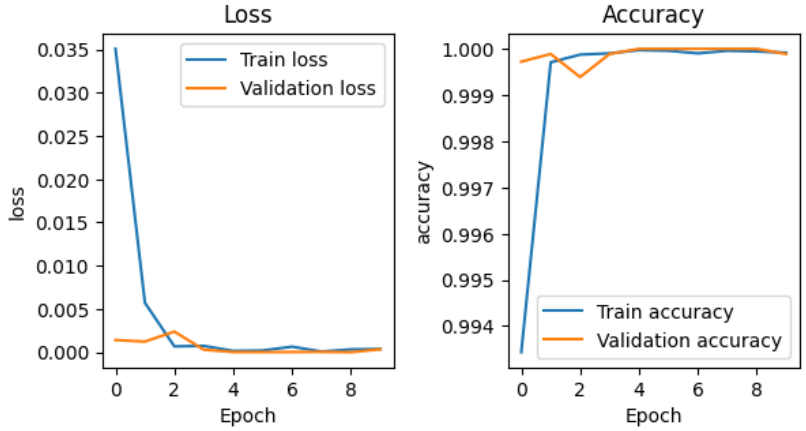

Figure 5: LSTM Method

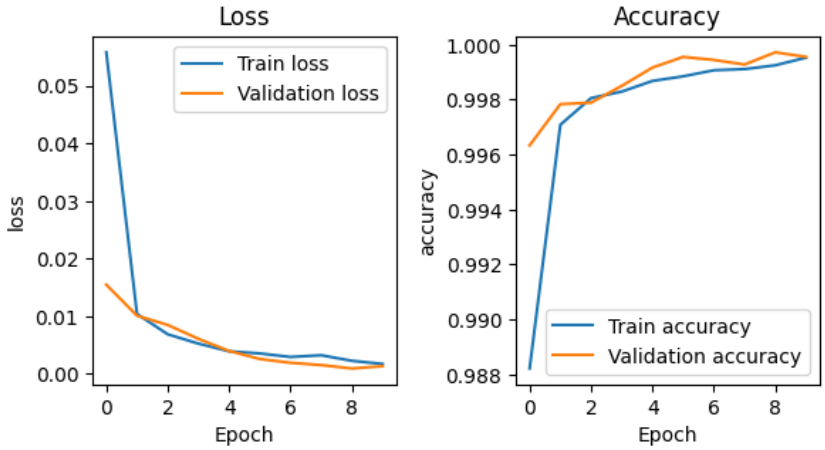

Figure 6: RK4 Method

Figure 7, 8, and 9 displays a confusion matrix in a table that shows the grouping model on a set of data. Each line of the grid addresses the genuine class of a case, and every section addresses the class predicted by the model. The inclining cells show the number of occurrences correctly classified, whereas the off-aslant cells show the number of cases that were misclassified.

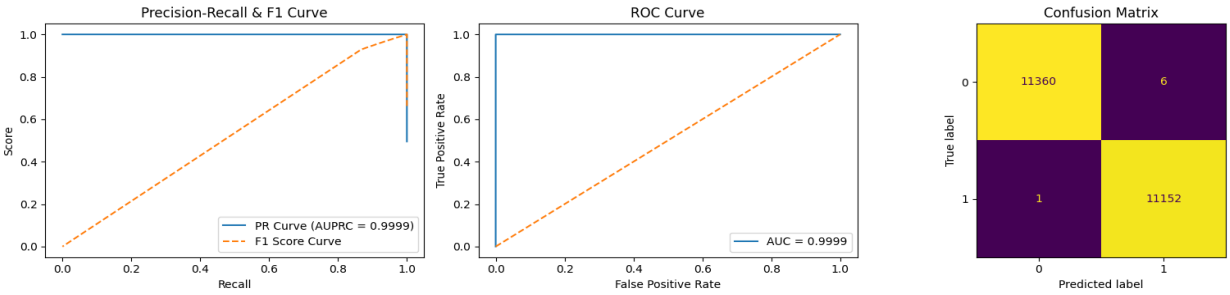

Figure 7: Pr-f1 Curve, Roc Curve and Confusion Matrix of LSTM

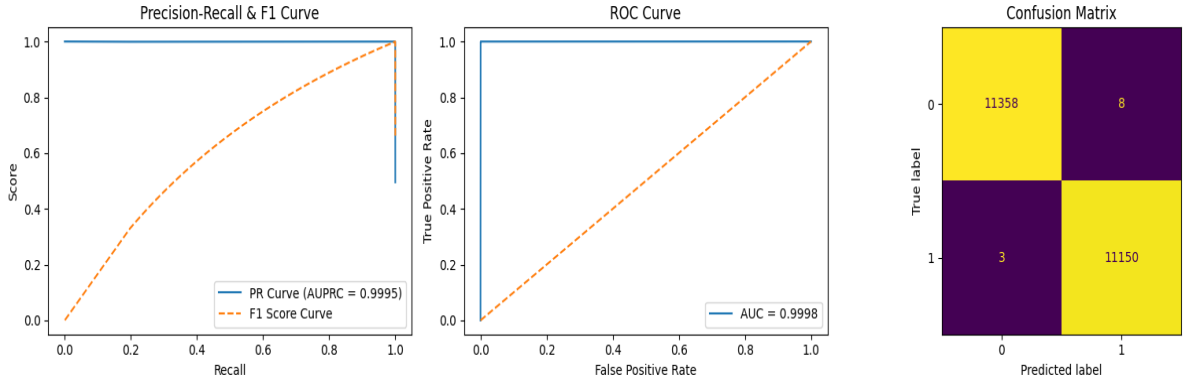

Figure 8: Pr-f1 Curve, Roc Curve and Confusion Matrix of LTCNN Using Rk4 Method

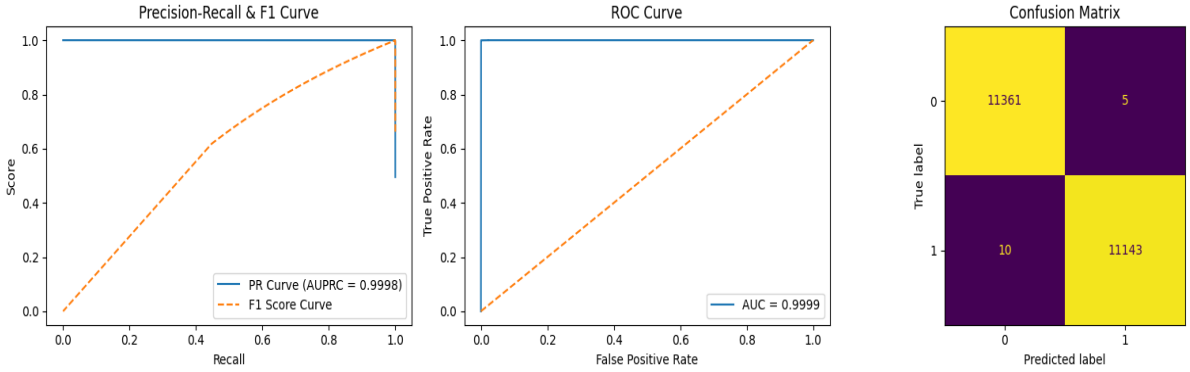

Figure 9: Pr-f1 Curve, Roc Curve and Confusion Matrix of LTCNN Using Euler Method

The Euler and RK4-based Liquid Time-Constant Neural Network (LTCNN) exhibits classification accuracy of 99.96% and 99.95% for Euler and RK4 models. The LSTM model exhibits 99.9%accuracy on the CICIDS 2017 dataset, but it has several conceptual and practical benefits that make it a viable alternative in certain use cases.

Training time Comparison

The training time and testing time for the proposed method and LSTM are shown in Figure 10. This comparison indicated important differences in model complexity and computational efficiency. The gated design of the LSTM model, which involves multiple internal processes such as input, forget, and output gating, as well as backpropagation through time, resulted in the training time of 173 seconds. The Euler-based LTCNN, which has the shortest training duration of 168 seconds, was able to achieve this by delivering a simple first-order ODE update and reducing the computational overhead per time step.

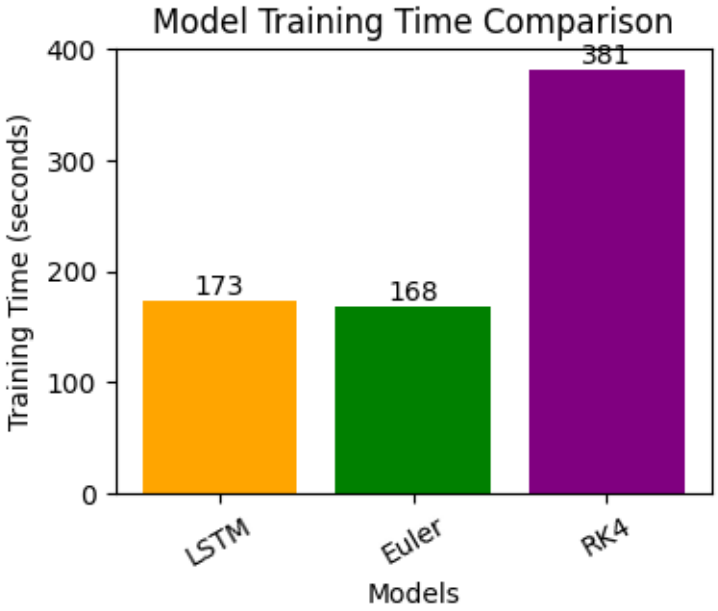

Figure 10: Training Time Comparison

Although four intermediate calculations added to each time step, the RK4-based LTCNN had a longest training time of 381 seconds, which is significantly slower than that of LSTM, but exhibited almost similar accuracy as that of LSTM. The outcomes demonstrate that, among other continuous-time models, Euler method offer superior training and are well suited for real-time intrusion detection applications where latency or computing resources are scarce.

The experimental pipeline demonstrates that the sequence-based deep learning models—especially ODE-inspired architectures—provide robust and generalizable intrusion detection capabilities.

Model Complexity:

The LSTM model contains 38,465 trainable parameters, which is approximately two times higher than the Euler and RK4-based models (20,353 and 20,289 parameters, respectively). Despite this significant difference in model complexity, the ODE-based architectures achieve comparable performance, demonstrating their ability to capture temporal dependencies with a substantially lower parameter footprint efficiently. This highlights the suitability of ODE-inspired models for resource-constrained intrusion detection environments.

First, the LTCNN architecture treats neuronal dynamics as a continuous-time system, allowing for a more realistic depiction of real-world temporal processes that occur continuously rather than in distinct stages. The Cybersecurity and Network-traffic-analysis areas, where events and packet flows frequently occur at unpredictable intervals, fit nicely with this continuous-time viewpoint.

Second, Euler and RK4-based LTCNN are more interpretable than LSTM. Explicit differential equations govern how hidden states evolve, that facilitates analysis, visualization, and the possibility of explaining system behaviour— an important trait for domains that require explainability such as anomaly detection and threat intelligence. The RK4 method also offers flexibility in dealing with various data granularities owing to its adaptive numerical accuracy and temporal resolution.

Finally, LTCNNs can be more parameter-efficient than LSTMs. These models require fewer learned parameters because they use a structured integration scheme such as Euler and RK4 while yet capturing complicated temporal connections. In addition, the suggested approach produced greater raw accuracy, facilitated superior generalization, sometimes resulted in quicker training, and provided a more in-depth understanding of the model's inner workings.

Therefore, in applications where trust, transparency, or continuous-time modelling are crucial, Euler and RK4-based LTCNNs may be favoured because of their interpretable, theoretically sound, and biologically inspired methodology.

V. Conclusion

The research focused on using continuous-time neural networks, particularly Euler and Runge-Kutta (RK4) based models, as alternatives to traditional LSTM architectures for intrusion detection, using the CICIDS 2017 dataset. Although LSTM, Euler-based LTCNN, and RK4-derived LTCNN shows similar and greater accuracy, a comparison of the time-frames used for training these models indicates important differences in model complexity and computational efficiency. The Euler method, which is computationally the simplest, offers the fastest training, whereas the RK4 method provided a balanced trade-off between accuracy and efficiency by better approximating the dynamic behaviour of the system. ODE-based models achieve comparable performance with 70% fewer parameters, making them computationally efficient alternatives to LSTM. Future work could explore hybrid designs or adaptive step-size solvers to enhance the performance and generalization, multiclass intrusion detection.

Funding

There is no funding involved in this submission.

Competing Interests
Authors do not have any relevant financial or non-financial competing interests.

Data Availability Statement:
The datasets supporting the findings of this study are openly available. The original CICIDS2017 dataset is publicly accessible from the Canadian Institute for Cybersecurity at:
https://www.unb.ca/cic/datasets/ids-2017.html
In addition, all processed datasets, feature-engineered data, model input/output files, and the values underlying all reported results (including means, standard deviations, and metrics used in tables and figures) have been made openly available in the Zenodo repository under a CC-BY license: https://doi.org/10.5281/zenodo.XXXXXXX

The shared materials include:

- Pre-processed and cleaned datasets used for training and testing;
- Feature extraction and selection outputs;
- Values used to generate all graphs and figures presented in the article;
- Model predictions, evaluation metrics, and confusion matrix values;
- Extracted data points used in statistical and performance analyses.

These datasets and materials are sufficient to enable full replication of the study results.
No data were excluded from sharing. There are no ethical, privacy, or security restrictions associated with the data used in this study.
The authors have used the dataset extracted from the CICIDS2017 dataset. Pre-processing steps were applied including data cleaning and label encoding. The processed dataset prior to normalization and train test splitting made publicly available to ensure reproducibility. All subsequent steps, including sequence generation, normalization, and data splitting performed within the experimental pipeline.

References

1. Laghrissi, F., Douzi, S., Douzi, K. et al. “Intrusion detection systems using long short-term memory (LSTM)”. J Big Data (2021) vol 8, n0. 65. https://doi.org/10.1186/s40537-021-00448-4
2. K. Greff, R. K. Srivastava, J. Koutn ık, B. R. Steunebrink and J. Schmidhuber, “LSTM: A Search Space Odyssey,” IEEE Transactions on Neural Networks and Learning Systems, , Oct. 2017, vol. 28, no. 10, pp. 2222- 2232. https://10.1109/TNNLS.2016.2582924
3. Guizhu Shen, Qingping Tan, Haoyu Zhang, Ping Zeng, Jianjun Xu, “Deep Learning with Gated Recurrent Unit Networks for Financial Sequence Predictions”, Procedia Computer Science, 2018, , Volume 131, Pages 895- 903, ISSN 1877-0509 https://doi.org/10.1016/j.procs.2018.04.298.
4. R. Hasani, M. Lechner, A. Amini, D. Rus, and R. Grosu, “Liquid Time constant Networks.” arXiv, 2020. https://10.48550/ARXIV.2006.04439 .
5. Himanshu Singh, “Federated Intrusion Detection System using Liquid Neural Network” student project, 2023, Nirma University, Ahmedabad.
6. J.M. Kramarczyk, “Liquid NeurIoTic: liquid neural network-based intrusion detecting system for internet of things in healthcare networks”, (Doctoral dissertation, The George Washington University (2024).
7. V.S. Pendyala, M. Patil “Multi-link prediction for mmWave wireless communication systems using liquid time-constant networks, long short-term memory, and interpretation using symbolic regression” Electronics, (2024), vol 13 no. 14, pp. 2736.
8. R. Hasani, M. Lechner, A. Amini, L. Liebenwein, A. Ray, M. Tschaikowski “Closed-form continuous-time neural networks” Nature Machine Intelligence, (2022), 4 (11), pp. 992-1003. https://doi.org/10.1038/s42256-022-00556-7
9. Chen, R. T. Q., Rubanova, Y., Bettencourt, J., & Duvenaud, D. “Neural Ordinary Differential Equations." Advances in Neural Information Processing Systems (NeurIPS), 2018. arXiv:1806.07366.
10. Kidger, P., Morrill, J., Foster, J., & Lyons, T. “Neural Controlled Differential Equations for Irregular Time Series." Advances in Neural Information Processing Systems (NeurIPS), 2020. arXiv:2005.08926.
11. Numerical ODE Solvers (Theory Reference) Butcher, J. C. (2016), “Numerical Methods for Ordinary Differential Equations.” Wiley.
12. CICIDS 2017 Data Set. Available online. https://www.unb.ca/cic/datasets/ids2017.html
13. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A., “CICIDS 2017 DataseT (Benchmark for IDS): Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, ICISSP (2018) https://www.scitepress.org/Papers/2018/66339/

Venkata Ramani Varanasi completed Msc, Computer Science from Andhra University, received M.Tech, Computer Science and Engineering from Osmania University Campus and pursuing Ph.D. in Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. She is currently working as an Assistant Professor at GITAM Deemed to be University, Hyderabad. She has 17 years of Teaching and Industrial Experience. She is a member of International Association of Engineers (IAENG), and the Computer Science Teacher Association (CSTA). Her Research Interests include Network Security, Machine Learning and Deep Learning, Artificial Intelligence, Data Science.

Professor Dr. Shaik Razia received her Ph.D in Computer Science and Engineering from the Koneru Lakshmaiah Education Foundation (formerly KL deemed to be University) and M. Tech Computer Science and Engineering, from Acharya Nagarjuna University. She has more than 19 years of experience in Teaching 15 years in KL University, and 4 Years Industry. Completed 7 Consultancy Funded projects, member of various professional bodies such as LMISTE, LMISCA, LM369 (SOLETE), SDIWC, CSTA, IEDRC and IAENG. 45 Research papers published in various National and International Journals and Conferences (25-Scopus indexed, 2-SCIE,2-(ESCI) Web of Science paper published by Taylor and Francis. 16-Nonscopus papers in various UGC, National and International Journals), Active Editorial Board Member, Committee member, Conference Chair and Reviewer of various National, International Conferences, Workshops and Seminars, having h-index: 10, 234 citations and i10:10. One Book Chapter and published 6 no. of patents. She has been awarded different prestigious awards such as Best Academician National Award 2022, Women Researcher National Award 2020 from the IJIEMR – Elsevier SSRN Research Awards, India, and Best Senior Faculty Inter National Award 2021 from Novel Research Academy, Puducherry, India. Research Achievement Award 2018 and Best Teacher Award 2013 from KLEF University, Vaddeswaram, India. Served in various capacities as committee member PSET2021, Reviewer for ICSCT-2019 (International Conference at Anurag Group of Institutions), IJICSE-2021 (IJICSE, University of Technology and Applied Sciences, Muscat), Microsoft CMT (International Conference on Emerging Electrical Energy, Electronics and Computing Technologies 2021) and Editor for Immortal Publications (Begonia no:4, Harbour view -2, Mayer Street, Port Louis, Al-Khuwair, Muscat, Sultanate of Oman, Vijayawada). She is a recognized supervisor for Ph.D Programme. Supervising 6 no. of Ph.D. Scholars. The Fields of research include Machine Learning, Deep Learning, Data Science, Artificial Intelligence, Data Analytics and Soft Computing.