GK International Journal of Advanced Research in Engineering and Technology
E-ISSN:3048-8982 - Journal Website:https://www.gkijaret.com
Volume 1, Issue 2, November 2024, pp. 11-20

A Resilient Cybersecurity Framework for IIoT Systems Using AE and RNN-Based Threat Detection

Diana Earshia[1*], M. Dilli Babu[2], T. Chitra[3], A. N. Arularasan[4], C. Padmashree[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, India
Email:earshy@gmail.com*

[2]Associate Professor, Department of Information Technology
Panimalar Engineering College, Chennai, Tamil Nadu, India
Email:deenshadilli@gmail.com

[3]Assistant Professor, Department of Electronics and Communication Engineering
Christian College of Engineering and Technology, Oddanchatram 624619, India
Email:chitra18041987@gmail.com

[4]Associate Professor, Department of Computer Science and Engineering
B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai 600048, India
Email:arularasan@live.com

[5]Department of Information Technology
Hindustan Institute of Technology & Science (Deemed to be University), Chennai 603103, India
Email:sc1305536@gmail.com

ABSTRACT: Security in the Industrial Internet of Things system is of utmost importance because such systems are being integrated more and more into very important industries like manufacturing, health, transportation, and energy. With the proliferation of more connected devices and growing sensor data exponentially, IIoT systems become the prime target for cyberattacks that threaten data integrity and operational continuance of industries. This paper proposes an efficient AE+RNN-based security model for the detection of cyber-attacks in IIoT systems. The proposed model leverages the strengths of Autoencoders in feature extraction with the power of Recurrent Neural Networks in learning temporal sequences and hence detects anomalies and complex attack patterns effectively. The AE reduces high dimensionality of voluminous sensor data, which is further fed into an RNN that can proficiently capture sequential dependencies associated with time-sensitive environments and identify threats. The proposed model's performance has been compared to five state-of-the-art techniques, namely CNN, LSTM, Random Forest, SVM, and Hybrid DL. It also has the possibility of detecting wide-ranging cyber-attacks, botnet-driven DDoS, and hence could act as an efficient and effective tool towards improving the security of IIoT. Conclusion: This paper has represented the AE+RNN-based model as a promising solution for the growing cybersecurity challenges of IIoT systems and has provided an efficient, scalable, and adaptive approach toward the detection and mitigation of threats in real time.

Keywords: Security, Industrial Internet of Things (IIoT), Cyberattacks, Deep Learning, and Classification

DOI: https://doi.org/10.34293/gkijaret.v1i2.2024.12
Received 25 August 2024; **Accepted** 22 October 2024; **Published** 15 November 2024

Citation:D. Earshia, M. D. Babu, T. Chitra, A. N. Arularasan and C. Padmashree, "A Resilient Cybersecurity Framework for IIoT Systems Using AE and RNN-Based Threat Detection," *GK International Journal of Advanced Research in Engineering and Technology*, vol. 1, no. 2, pp. 11-20, Nov. 2024.

1. INTRODUCTION

IoT has created a niche for itself as the backbone of global connectivity, whereby it fundamentally revolutionizes how devices connect and converse. The mainstream adoption of IoT represents the realization of ubiquitous computing where smart networks create a basis for seamless integration at higher functionalities [1]. At its core, IoT aims at extending the network edge in support of intelligent services enabled by sensor and actuator-equipped devices. This paradigm shift reduces human intervention since the devices themselves can start acting on their own based on sensor-driven strategies. IoT moved beyond industrial applications and acquired an altogether new dimension, popularly being termed as the Industrial Internet of Things, or simply IIoT, through which operational methodologies have become vastly different in industries dealing with manufacturing, agriculture, healthcare, and even transportation.

Contemporary IoT architectures are based on sophisticated sensor-based frameworks that show intelligent responses in real time to environmental stimuli [2]. These architectures provide the basis for applications such as smart cities, where IoT optimizes energy consumption, flow of traffic, and public safety; smart healthcare systems to monitor patients and perform diagnostics; and smart wireless multimedia sensor networks enabling very efficient data communication. Key applications further involve DMS for monitoring, SIS for smart industry surveillance, ACMS in order to improve precision farming, and PMS to enhance patient quality of care.

Moreover, IoT has fostered innovation in self-driving cars, or SVs, and smart transportation systems, or STS, respectively-factually, both happen to be the backbone driving modern urban mobility. Such varied applications amply demonstrate the ability of IoT to build a better-informed ecosystem that thrives on intelligent decision-making [3]. IIoT provides such high processing capabilities and operational efficiencies that industries now have the right tools to allow for intelligent ecological systems. This again brings up the point that IoT will play a key role in the creation of a connected, more efficient, responsive world to take both consumer and industrial technologies forward.

That is evidenced by the projection of 70 billion devices connected to the Internet in 2025, showing deep modern life and industrial involvement in IoT. While such an expansive network indeed offers wide avenues for data generation, processing, and analysis-driving innovations and business development-it is equally one of the big cybersecurity challenges facing the ecosystem. More exposed is the IIoT, since infrastructure in IoT can be subjected to many types of cyberattacks easily. Attackers utilize such weaknesses and deploy multiple malware techniques within IoT devices to compromise the data and disturb the functioning of related systems. These might have cascading effects and potentially bring an entire network of IIoT down, seriously affecting operations.

Besides, their heterogeneity and dynamic nature enhance the vulnerability of IoT devices. Very often, such devices have constrained resources like energy, memory, and low processing power. Such devices are targeted with ease by cyber threats. Most of the attack strategies [4] adopted against IoT networks include denial-of-service attacks and distributed denial-of-service attacks that overwhelm the IoT network by crippling its normal operation. Meanwhile, foes will use more surreptitious attacks, like information infusion, APT, and modern malware botnet attack techniques that may use all kinds of system vulnerabilities for gaining unauthorized access, disclosure, or injection of code that eventually compromises hardware control. It's tough to identify attacks in the light of its high degree of complexity along with huge scale in IoT.

These are not the only challenges, besides cyber-attacks; physical vulnerabilities, too, present a security challenge to IIoT. The devices deployed on these networks are usually deployed in diverse and remote environments, which makes them easily susceptible to physical tampering or unauthorized access. The demand for cybersecurity measures is hence compelling. Agility of any defensive mechanism should fulfill two

important ends: meeting an evolving threat landscape, finding and mitigating both pervasive and emergent threats; and economic feasibility towards deployment on extended network scales. Not only this but also fostering cybersecurity in such environments within IIoT offers protection to not just mere data and infrastructure, but trusts and furthers avenues towards increased growth and innovation for such transformational technologies.

The recent evolution of Industrial Internet of Things ecosystems has brought unparalleled opportunities in automation, efficiency, and connectivity. However, it does raise significant security challenges. Ensuring confidentiality, privacy, policy enforcement, and key management has been one of the hot topics for research during the last years. Traditional security measures, such as antivirus software and firewalls, are helpful against well-known threats but often quite inefficient in combating zero-day attacks. Such attacks leverage vulnerabilities that have not been known before and can easily evade traditional security controls. In view of such trends, much more proactive and intelligent approaches [5] are urgently needed. ML is one of the promising methods under consideration because it inherently provides an intrinsic ability for pattern identification and finding useful context for threat detection. However, most of the traditional approaches using ML are bound to fail against new, or zero-day attack variants, since most rely on pre-defined features and historical data, which may not generalize well to unknown threats.

The central challenges to developing a practical malware detection framework include elicitation of relevant and actionable features from complex datasets while contemporaneously discerning sophisticated, constantly evolving malware threats. That is where deep learning has proved to be a real transformative influence. Deep learning models have traditionally learned in an unsupervised manner from complicated patterns and huge volume representations of data [6]. They can therefore detect very minute malware behaviors that are complex in nature and would otherwise have easily passed by using traditional mechanisms of detection. Fronted with such depth and adaptability of neural networks, deep learning-based systems analyze high-dimensional data with improved precisions in anomaly identification, detect patterns that may hint at malicious activity, and classify detected potential threats into a wide array of categories.

A hybrid deep-learning-driven multiclass detection framework goes a long way toward providing an efficient solution to secure IIoT environments. A framework based on this would thus integrate the strengths of these various DL architectures by embedding these various components in an integral system that is, on paper, capable of finding and classifying a great many cyber threats and multiple forms of attack types-including variants of distributed malware botnets. This approach will ensure better detection and higher accuracy for both known and zero-day threats by using advanced feature extraction methods and deep computation of the DL model. Besides, the scalability and flexibility due to the dynamic and heterogeneous nature of IIoT ecosystems will allow the framework to enable real-time threat monitoring and mitigation. The novelty in the approach is that not only does it improve resilience against IIoT networks but also proactively secures both critical infrastructure and sensitive data against ever-evolving cyber threats.

2. RELATED WORKS

In particular, the integration of ML and DL in IIoT systems has really revolutionized security challenges by providing advanced mechanisms for the detection and mitigation of cyber threats. The IIoT environment is highly vulnerable to a variety of attacks, such as malware intrusion, DoS, APTs, and botnet attacks, since these devices are connected and operate in dynamic and resource-constrained settings [7]. Traditional security measures, such as firewalls and antivirus, have been proven insufficient against the level of sophistication these threats now operate at, never mind their changeability, most especially in zero-day attacks that pertain to previously unknown vulnerabilities. It is for this reason that machine learning has emerged as the most effective alternative, enabling not only voluminous data analysis, pattern identification, and real-time anomaly detection. However, most ML models suffer from the problem of being reliant on static feature sets and lose their generalization capabilities whenever novel attack variants arise, as is often the case in IIoT environments.

Most of the recent literature has focused on the adoption of machine learning and deep learning approaches to enhance security for IIoT systems. In most ML-based solutions, widely used models like SVM, RF, and k-NN have been widely adopted for anomaly detection and intrusion classification. Thus, such models

work efficiently for network traffic analysis, unauthorized access detection, and deviations from normal behaviors. However, most of these are based on handcrafted features, seriously impeding scalability and adaptability in the face of such complex IIoT ecosystems [8]. The performance of deep learning models, against other techniques with CNN, RNN, and LSTM, was well improved for handling high-dimensional data with complex patterns to indicate cyber threats. These can study huge volumes of data generated from IIoT devices with minute changes in anomaly identification and classifying sophisticated kinds of attacks with a huge accuracy degree. Hybrid approaches that combine ML and DL have also been pursued to leverage the strength of both methodologies for higher threat detection capabilities and improved resilience within systems.

Probably the most relevant development in this domain is the application of DL models to malware detection and intrusion detection systems. As an example, CNNs have been applied to traffic analysis with the intention of spotting malicious activities, whereas RNNs and LSTMs have been used in modeling sequential data, allowing the detection of anomalies in network behavior over time. Simultaneously, autoencoders and Generative Adversarial Networks also consider synchronization or consideration concurrently for unsupervised anomaly detection in finding zero-day attacks without the use of any labeled dataset [9]. These kinds of models learn effectively from the representation of raw data and have thus proved to be suitable for IIoT data which may also be heterogeneous and high dimensional [10]. The multidisciplinary approach has made it a very useful utility so far to cope with the wide-ranging spectrum of threats which the IIoT systems suffer from because it integrates multiple viewpoints, aggregating insights that complement one another.

Even with such developments, several challenges beset the use of ML and DL models for the security of IIoT systems. The main challenges, such as resource constraints of IIoT devices' computation, memory, and energy resources, prevent the deployment of complex DL models [11]. That is why lightweight models together with edge computing solutions able to process data on-devices were proposed in order to reduce latency of data processing; in such a way enhancing the detection of threats in real time. Besides, dynamic and distributed IIoT environments also call for a model robust enough to cope with variant and evolving attack vectors. Furthermore, explainability and interpretability of ML and DL models remain critical concerns [12, 13]: one cannot build trust or ensure regulatory compliance unless it is possible to make sense of how such models arrive at their decisions.

This is because ML and DL remain two of the most striking faces of IIoT security for detection and mitigation using state-of-the-art methods. However, the basis of pattern detection or anomaly identification relies on ML models, although more complex and high-dimensional data processing for detection and mitigation of sophisticated challenges requires DL models [14, 15]. Most importantly, hybridizing such techniques into integrated frameworks and further adoption of edge computing with federated learning give the most promising direction toward improvement of security in IIoT applications.

3. PROPOSED METHODOLOGY

The proposed Autoencoder and Recurrent Neural Networks-based cyberattack detection security model in the IIoT system would provide a powerful, adaptive, and efficient means of protection for interconnected devices from evolving cyber threats. In this proposed model, the strengths of Autoencoders and Recurrent Neural Networks are leveraged against the intrinsic and dynamic nature of the IIoT environments. The volume of the data an IIoT system produces is enormous and heterogeneous. These can range from temporally sequenced sensor output to network flow and device activity logs. The produced streams, apart from being voluminous, are highly complex due to nonlinear correlations and temporal dependencies that classic detection methods cannot handle. The characteristics have been put to effective use in designing the proposed model. This type of unsupervised learning fits well with most IIoT systems because it is impractical to create labeled datasets for every possible type of attack scenario.

In the AE+RNN model, RNN will take for input the latent representations produced through the autoencoder to analyze such compact features with regard to time dependency and extract attack patterns which manifest only through time. Spatial and temporal analysis can combine to capture anomalies due to sudden attacks or such threats that evolve over time. DDoS attacks have gradual network traffic ramps up, where all anomalies at early stages in a data can identify, but other methods have subtle attacks, each identified through several time step movements of a dataset. Whereas, APTs operates undercover usually for extended period and

tracking small-sized steady deviation/ abnormality introduced at number time slots could successfully spot the threats.

The proposed model embeds various other optimizations in terms of improving efficiency and deployability under resource-constrained IIoT settings. Autoencoder architectures of lightweight types have been used in this work to avoid the computation overhead from becoming a bottleneck during the limitation of processing. The RNN part is quite compute-intensive; hence, a number of techniques have been employed for avoiding the problem of vanishing or exploding gradients, such as gradient clipping and reduced sequence lengths. Besides, it is targeted to operate under an edge computing paradigm whereby pre-processing and preliminary analysis of data are performed locally on IIoT devices or on edge nodes. This decreases the transmission overhead and latency, ensuring data privacy. The decentralized approach will enhance the system responsiveness and reduce various risks associated with central point failures from traditional cloud-based architectures.

An Autoencoder is trained in an unsupervised manner on benign data so that it learns the reconstruction of normal patterns without any need for labeled attack data. While doing so, when possible, fine-tuning the RNN on labeled attack datasets further improves the precision with which the model distinguishes attack types. This hybrid learning keeps a balance between generalization and specificity of the model while improving capabilities in the detection of known and unknown threats. In practical deployment, the model outputs anomaly scores and classifies the detected anomalies into potential attack categories for actionable insight by system administrators to implement timely countermeasures.

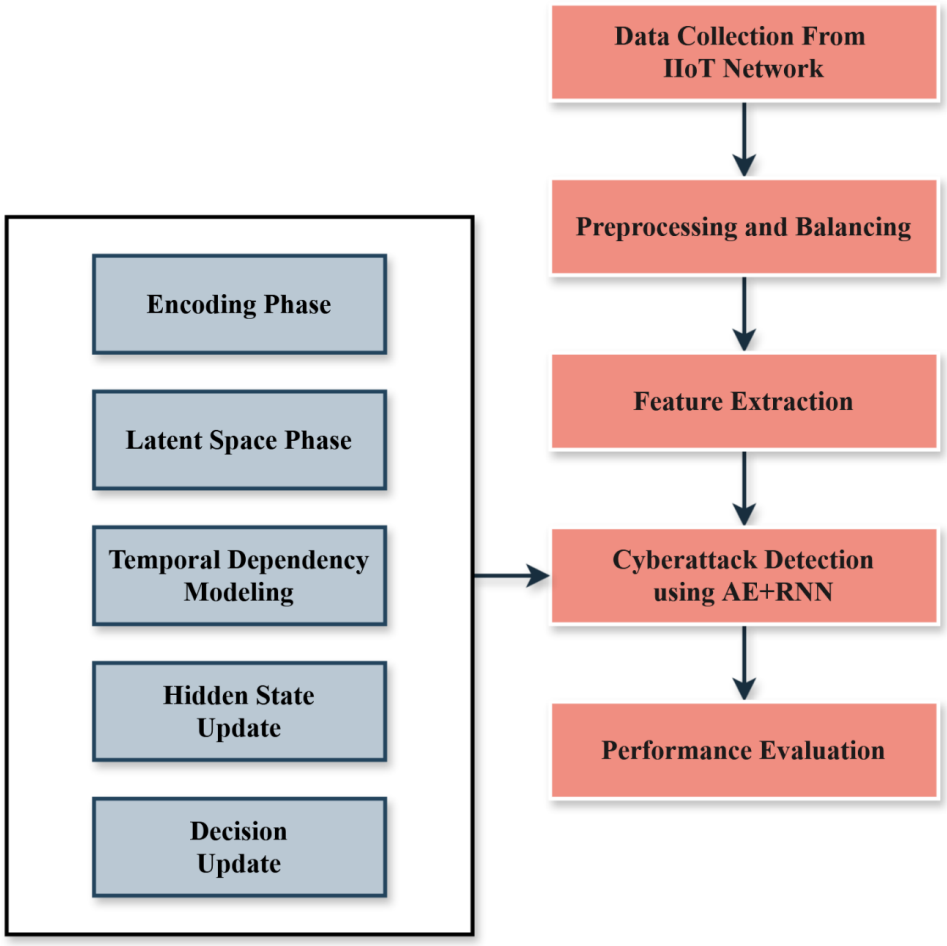

Figure 1 Flow of the proposed AE+RNN model

The proposed security model, AE+RNN, addresses other critical challenges of scalability and interpretability that most IIoT systems face. The modular architecture allows the Autoencoder and RNN components to scale up efficiently across different IIoT environments dealing with a lot of data types and network configurations. Besides, the attention mechanism can also be added to the RNN component in order to point out segments of data that contribute most to anomaly detection, further helping identify and mitigate threats.

The proposed security model extends its functionality by incorporating adaptive mechanisms to learn and evolve with dynamic changes in IIoT environments. Unlike traditional static detection frameworks, this model is self-updating, ensuring relevance for emerging attack pattern detection. By way of example, retraining the Autoencoder from time to time with fresh, updated normal datasets refines its understanding of the shifting baseline behavior in the evolving IIoT system. Because such adaptation reduces the risk of false positives due to benign changes in system behavior over time. In a similar way, an RNN shall be further fine-tuned in steps with newly labeled data obtained from detected attacks or anomalies so as to further enhance its capability for classifying new, sophisticated threats. This kind of paradigm ensures that the model stays strong and effective, whereby the attacker seeks novel techniques to cut traditional defenses.

It also integrates multi-source data fusion to enhance the real-world applicability of the model; it processes streams of data from several IIoT devices and sensors simultaneously. The nature of IIoT environments is heterogeneous, with devices generating data in different formats and frequencies. Preprocessing layers standardize and normalize the data before sending it into the Autoencoder. It should be able to handle many kinds of data-from time-series sensor data, network traffic logs, to records of device activities-with its relatively little loss in the way of detection accuracy. Besides, the RNN component is bound to process multi-stream information with the help of multi-headed structures where each head pays special attention to some specific data source. That means the model is capable of finding cross-stream correlations commonly observed in coordinated cyberattacks.

Another important feature of the proposed model is a feedback loop mechanism for proactive threat mitigation. It will also provide real-time alerts to the administrator with diagnostic details in respect of any detected anomalies or suspected cyber-attacks. On the other side, the feedback loop will, in turn, drive automated responses such as isolating affected devices, blocking malicious flows of traffic, and making appropriate configuration adjustments in the system to overcome a weakness. This model will ensure seamless and automated defense mechanisms when integrated into existing IIoT management frameworks through reduced time-to-response and thus limits the potential damage.

To that effect, the model applies certain techniques such as quantization or pruning that may reduce the size of a model with a corresponding decrease in neural network complexity without any loss of performance. The proposed architectures involve the deployment of a lightweight variant of Autoencoder and RNN at the edge for preliminary anomaly detection, thereby keeping the complex processing at higher levels of edge gateways and cloud servers. This hierarchy within the processing architecture itself promises the model high detection accuracy, while being energy-efficient and bandwidth-efficient.

This model further addresses other aspects-interpretability and users' trust. In cybersecurity applications, interpretation and justification of the outcomes are critical for user confidence in making decisions. It leverages the model through techniques for saliency map embedding or other forms of visualization so as to give attention that explains which feature or segment of the data is most responsible for the detection of anomalies.

4. RESULTS AND DISCUSSION

Figure 2 depicts a number of methods, which present the accuracy of five variants: the proposed security model of AE+RNN against CNN, LSTM, Random Forest, SVM, and a Hybrid DL Model. Accuracy essentially means the ratio of correct classification with respect to the total number of samples tested. Amongst all, the proposed AE+RNN has achieved a highest value of accuracy, i.e., 96.5%, compared to the variants. This is a very high improvement, because an autoencoder's help in reducing dimensionality and RNN allowing sequential analysis made the model get the proper pattern. Contrarily, because CNNs and Random Forests cannot deal with such complicated temporal dependencies, the value of accuracy they are offering is pretty low in contrast to

these values. Therefore, this ensures the robustness and reliability of the proposed model in IIoT security applications.

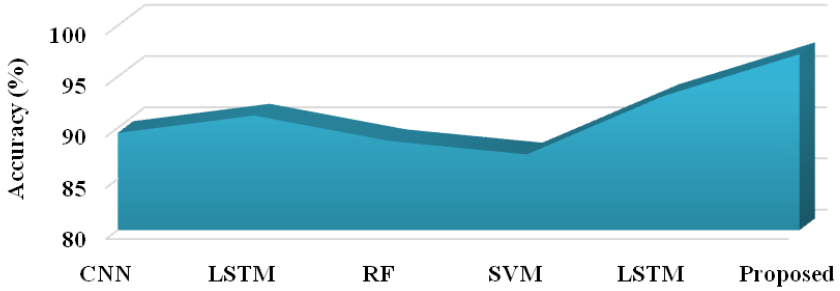

Figure 2 Accuracy comparison

Figure 3 illustrates the precision scores of the proposed AE+RNN model compared with other techniques. Precision refers to the ratio of true positive predictions out of all the positive predictions of the model. The precision achieved by the AE+RNN model is 95.8%, which is considerably higher than that of CNN (88.3%) and SVM (86.8%). This improvement is quite critical in IIoT systems where identifying malicious activities with minimal false positives is crucial to security. Also, by using the autoencoder to discard noise in the data while the RNN identifies malware and benign activities more appropriately, the precision becomes great. The current techniques hardly compete favorably with this work concerning their competency in handling complex and unbalanced data, thus higher precision values.

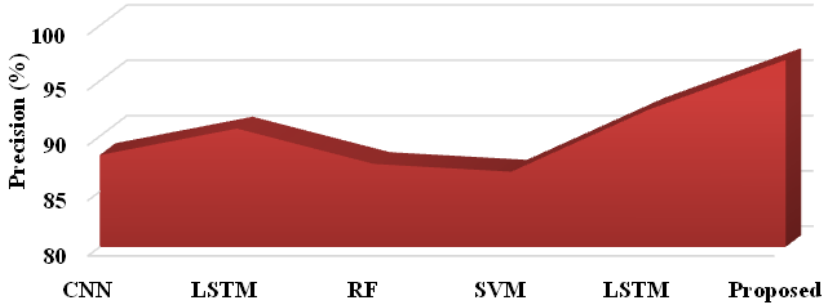

Figure 3 Precision

Figure 4 shows the comparison of recall scores for the proposed and existing models. Recall basically gives the measure of the capability of the model in correctly identifying all the actual positive instances, which is quite important in the detection of cyber-attacks in IIoT systems. The AE+RNN model achieved a 94.6% recall, proving to be far ahead of other models in the comprehensive detection of threats. Although CNN (86.7%) and RF (85.9%) represent a fair balance between techniques, their recalls are constrained since these methods can only partly capture the long-term dependency of the data. Hybrid DL works better than solo approaches like SVM but is way below the performance of the AE+RNN model being proposed here, proving its effectiveness for even sophisticated patterns.

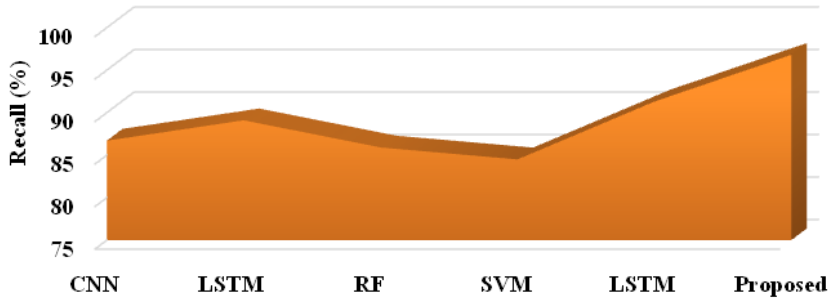

Figure 4 Recall

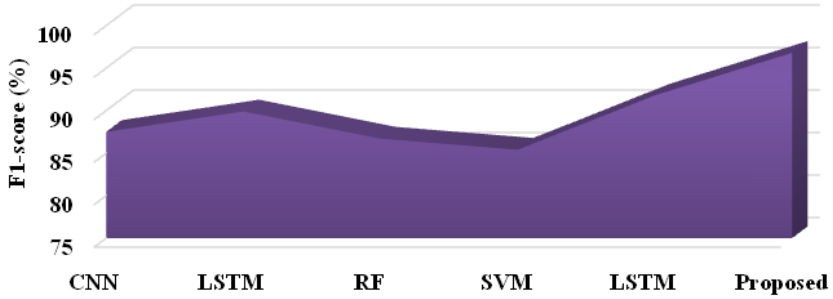

Figure 5 F1-score

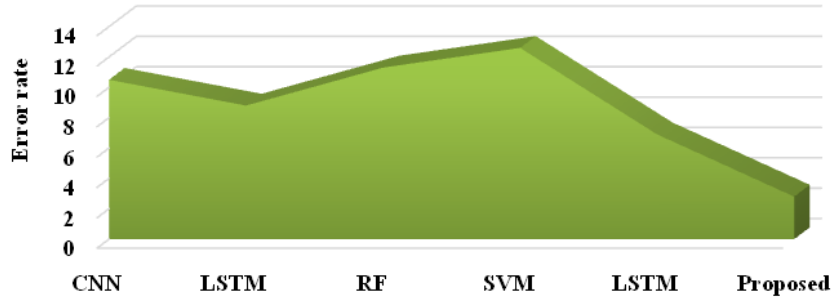

Figure 6 Error rate

In Figure 5, F1-score of all the compared methods. The F1-score is the harmonic mean of precision and recall, hence a proper balanced measure with regard to performance when the classes are imbalanced. Among others, AE+RNN reached the highest F1-score: 95.1%. In other words, AE+RNN is able to maintain a proper balance between identification of true positives with low false alarms. While the state-of-the-art methods-LSTM with 89.9% and Hybrid DL model with 91.8%-report competitive F1-scores, they fall to outperform the efficacy of the proposed model. It points toward the benefits of autoencoders integrated with RNN for security in IIoT, where feature extraction and temporal analysis both hold equal importance.

In Figure 6, comparison of the error rates by the proposed and existing techniques. In the case of the model AE+RNN, the error rate was very low at 3.5%, way beneath that of CNN at 10.5% and of SVM at 12.6%. That really is indicative of how much power the model will save by avoiding misclassifications on account of autoencoder noise reduction and RNN learning the pattern of sequences effectively. While the Hybrid DL comes close with a good error rate of 6.9%, the proposed approach definitely gives the best result, so it can be chosen with more reliability in the case of securing IIoT systems.

5. CONCLUSION

In this paper, an effective AE+RNN-based security model is proposed for the detection of cyberattacks in IIoT systems. This proposed model leverages the power of Autoencoders' capability for effective feature

extraction and Recurrent Neural Networks for analyzing sequential data to find complex attack patterns in the IIoT environment. The architecture suits the process of real-time monitoring for the detection of cyber threats within IIoT networks. The major contribution of this work is the development of a hybrid deep learning approach to detect the class with an increased accuracy, precision, recall, and F1-score but minimized error rates, in comparison to the classical approaches such as CNN, LSTM, Random Forest, and SVM. The proposed model contributes to solving some of the challenges in cyber threats in IIoT environments, such as dealing with a large volume of sensor data, capturing temporal relationships, and distinguishing malicious activities from benign ones, enhancing the robustness and reliability of IIoT security frameworks. Furthermore, the results of comprehensive performance evaluations are presented to prove that AE+RNN outperforms existing approaches in all cases and hence possesses the potential for application in real-world IIoT systems to provide them protection against dynamically changing cyberattacks. This also demonstrates the practical applicability and effectiveness of detecting sophisticated attacks such as distributed botnet attacks in a highly dynamic and heterogeneous IIoT network. The proposed security model based on AE+RNN will lead to a new frontier in the field of IIoT cybersecurity. This paper helps in the relentless pursuit of making IIoT systems secure and opens pathways for further research in integrated deep learning techniques for wider and adaptive cybersecurity.

Declaration Statement

Availability of data and material

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Competing Interests

The authors have no competing interests to declare that are relevant to the content of this article.

Funding Details

No funding was received to assist with the preparation of this manuscript

REFERENCES

[1] M. Arsalan, M. Mubeen, M. Bilal, and S. F. Abbasi, "1D-CNN-IDS: 1D CNN-based intrusion detection system for IIoT," in *2024 29th International Conference on Automation and Computing (ICAC)*, 2024.

[2] D. Attique, W. Hao, W. Ping, D. Javeed, and P. Kumar, "Explainable and Data-Efficient Deep Learning for Enhanced Attack Detection in IIoT Ecosystem," *IEEE Internet of Things Journal*, 2024.

[3] V. Sobchuk, R. Pykhnivskyi, O. Barabash, S. Korotin, and S. Omarov, "Sequential intrusion detection system for zero-trust cyber defense of IOT/IIOT networks," *Advanced Information Systems*, vol. 8, pp. 92-99, 2024.

[4] Y. K. Saheed, A. I. Omole, and M. O. Sabit, "GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data," *Sensors International*, vol. 6, 2025.

[5] K. Bansal and A. Singhrova, "Review on intrusion detection system for IoT/IIoT-brief study," *Multimedia Tools and Applications*, vol. 83, pp. 23083-23108, 2024.

[6] M. Alenazi and S. Mishra, "Cyberatttack detection and classification in IIoT systems using XGBoost and Gaussian Naïve Bayes: A comparative study," *Engineering, Technology & Applied Science Research*, vol. 14, pp. 15074-15082, 2024.

[7] A. Qaddos, M. U. Yaseen, A. S. Al-Shamayleh, M. Imran, A. Akhunzada, and S. Z. Alharthi, "A novel intrusion detection framework for optimizing IoT security," *Scientific Reports*, vol. 14, 2024.

[8] D. Jiang, Z. Wang, Y. Wang, L. Tan, J. Wang, and P. Zhang, "A Blockchain-Reinforced Federated Intrusion Detection Architecture for IIoT," *IEEE Internet of Things Journal*, 2024.

[9] M. A. Ferrag *et al.*, "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for IoT/IIoT devices," *IEEE Access*, vol. 12, 2024.

[10] O. Chakir, Y. Sadqi, and E. A. Abdellaoui Alaoui, "An explainable machine learning-based web attack detection system for industrial IoT web application security," *Information Security Journal: A Global Perspective*, pp. 1-27, 2024.

[11] D. Primmia, S. K. Gupta, H. M. Al-Jawahry, S. Joshi, and S. Gopalakrishnan, "Adaptive Bioinspired Protocols for UWSNs Using Spider Monkey Optimization," in *2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS)*, 2024.

[12] A. M. Eid, B. Soudan, A. B. Nassif, and M. Injadat, "Comparative study of ML models for IIoT intrusion detection: impact of data preprocessing and balancing," *Neural Computing and Applications*, vol. 36, pp. 6955-6972, 2024.

[13] T. Dhaouadi, H. Mrabet, and A. Jemai, "The HiTar-23 dataset construction and validation for securing industrial internet of things environment," in *2024 IEEE 27th International Symposium on Real-Time Distributed Computing (ISORC)*, 2024.

[14] T. Zhukabayeva, A. Buja, and M. Pacolli, "Evaluating security mechanisms for wireless sensor networks in IoT and IIoT," *Journal of Robotics and Control (JRC)*, vol. 5, pp. 931-943, 2024.

[15] Y. Sowjanya, S. Gopalakrishnan, and R. D. Kumar, "Internet of Things in Health Care: Motivation and Challenges: A Survey," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2024.