Babylonian Journal of Internet of Things
Vol.2024, **pp.** 106–114
DOI: https://doi.org/10.58496/BJIoT/2024/013; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

RNN-Based Framework for IoT Healthcare Security for Improving Anomaly Detection and System Integrity

S. Rajaprakash[1,], C. Bagath Basha [2,], M. Nithya [3,*], K. Karthik [4,], Nitisha Aggarwal [5,], S. Kayathri [6,]

[1]*Department of Computer science & Engineering,Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology , Chennai , Tamilnadu, India*
[2]*Department of Computer Science and Engineering, Kommuri Pratap Reddy Institute of Technology, Autonomous, Hyderabad, Telangana, India.*
[3]*Department of Computer Science and Engineering , Vinayaka Missions Kirupananda Variyar Engineering college, Vinayaka Missions Research Foundation, Salem, Tamil Nadu.*
[4] *Department of Computer Science and Engineering,Aarupadai Veedu Institute of Technology,Chennai 603104, Tamil Nadu, India.*
[5]*Panipat Institute of Engineering and Technology, Samalkha, Haryana, India.*
[6]*Department of Computer Science and Engineering, P.S.R Engineering college, Sivakasi, Tamil Nadu 626140, India.*

ARTICLE INFO

Article History
Received 17 Jun 2024
Revised: 18 Aug 2024
Accepted 20 Sep 2024
Published 11 Oct 2024

Keywords

IoT Healthcare
Recurrent Neural Networks (RNNs)
Deep Learning
Classification
Healthcare Data Protection

ABSTRACT

The rapid rise of the Internet of Things greatly benefited the healthcare sector by opening up new ways of monitoring patients and ingeniously collecting data on disease management. However, this increased connectivity and health system data interchange introduce many critical security vulnerabilities that are more likely to discredit highly sensitive patient information along with system integrity. The paper investigates only one critical IoT health care security issue, for which a new security framework based on RNNs was used to investigate enhancements in the threat detection and response. This approach modelled network traffic and device behavior sequentially for anomaly and potential breach detection using RNNs. Hence, we introduce the RNN-based model combined with an inclusive security architecture, including data encryption, mechanisms of authentication, and monitoring tools in real time. Experimental results prove that our RNN-based framework significantly improves malicious activity detection and reduces false positives compared to traditional security solutions. The proposed model would provide a strong, scalable, and adaptable security solution tailored to the IoT healthcare environment dynamics. These findings could indicate how RNNs can enhance security in IoTs and provide new ways in which better and more secure healthcare systems can be developed.

1. INTRODUCTION

The IoT has grown into a major and continuously growing research area stimulated by important advances in electronics, the spreading of IPv6, and increased coverage and deployment of wireless networks, thus enabling the integration of many physical devices that can then be interconnected to communicate with each other and exchange information in real time. IoT technologies are characterized by their functionality to connect all ordinary objects [1], including household appliances, medical devices, vehicles, and industrial equipment, to the internet for data collection and sharing. The concept has consequently given rise to several varieties of smart environments which get integrated into homes, healthcare, aerospace, and transport systems, changing the way these sectors function. The continuous development of IoT devices and technologies has ensured an increasing pace of research into methods through which their functionality, efficiency, and scalability can be realized.

There exist various challenges related to the expanding landscape of IoT, of which one is associated with integrating IoT devices into control systems [2]. This is structured to execute tasks in the regulation of the behavior of IoT networks, as a

*Corresponding author. Email: nithyam@vmkvec.edu.in

way to ensure further seamless and autonomous functioning of these devices. The researchers are more interested in developing new methodologies and techniques to improve the management of IoT devices, particularly for those application environments where precision and reliability matter, such as in healthcare, aerospace, and industrial automation. The management of IoT devices effectively requires sophisticated algorithms and technologies that can handle large-scale distributed networks with minimal latency, while ensuring scalability and preserving energy efficiency.

However, since the technology of IoT began proliferating, security has become the top concern. The prime characteristic of IoT devices, therefore, is that they would be more vulnerable to scores of different kinds of attacks due to their being interconnected with other such devices or systems. These devices, which deal in their operation with highly varied and decentralized ecosystems, are hard to protect. Most of them also lack the processing power, storage, and bandwidth whereby good security can be implemented [3]. In turn, IoT security has surged to the forefront of current priorities, both for researchers and for professionals. Accordingly, the protection of IoT devices from unauthorized access, data breach malware, and other forms of cyber-attacks requires further advancement in protocols and frameworks for IoT security. This would not only protect the device itself but also the information it generates for integrity, confidentiality, and availability of the IoT ecosystem information. Thus, IoT security became one of the most critical research areas that has been striving to come up with enhanced various encryption methods, secure protocols of communication, intrusion detection systems, and decentralized security models based on unique challenges presented by the IoT environments.

Consequently, data protection has become the most critical concern among network devices, especially under IoT conditions with large sets of connected devices transmitting sensitive information. In ensuring security for IoT ecosystems, it is not just an issue concerning protection of data, but also a core issue pertaining to human life, especially in applications related to health care, automation of industry, and transporting systems. A consequence of an IoT device being attacked, interfered with, or controlled in an unauthorized manner in this type of environment could be nothing less than a catastrophe: personal injury, collapse of systems, or even loss of life [4]. Securing IoT systems becomes all the more important when many devices interact with real-world environments and thus immediate and tangible results are manifested in security breaches. Thus, security in IoT is not a background but a foreground issue to be considered at each step of the deployment and operation of IoT.

In the core of security problems in IoT, there is authentication. Authentication is a process that gives verification of the identity either of a user or a device with the purpose of assuring that the commands coming to the IoT devices are coming from trusted and authorized sources. Now, in an IoT environment, where devices continuously run by executing one task or another through commands from a control system, authenticity needs to be assured. In the absence of authentication of those commands, malicious entities could hijack the devices' control and lead to hazardous outcomes [5]. For instance, in smart healthcare, unauthorized access to medical devices could lead to the wrong dosages, malfunctioning equipment, and direct risks to patients. It can be considered a first line of defense against such threats since it institutes trust between the control systems and devices they govern. This makes sure that only valid, authenticated subjects can issue commands or access data from the network.

Different research works have been carried out for developing authentication mechanisms related to both traditional networks and IoT systems. While these techniques remain effective in traditional settings, they often break down in the face of particular IoT requirements. Unlike other conventional network devices, IoT devices operate under resource-constrained environments; they have limited memory, processing power, and energy capacity that seriously constrains the level of complexity and robustness that the security protocols running on top can afford to support [6]. Traditional authentication schemes may contain resource-intensive cryptographic algorithms or multistep verification processes that are comparatively unsuitable for IoT devices due to the higher computational nature of these schemes. This quickly depletes the battery life of IoT devices, reduces efficiency, and impairs their real-time operating capability-all of which constitute critical factors in many IoT applications.

2. LITERATURE SURVEY

Literature on IoT data protection and security unmistakably indicates a growing consciousness of critical challenges emanating from the unique characteristics of IoT devices. Early efforts at ensuring security in IoT systems focused largely on adapting conventional network security protocols. Usually designed for more powerful computing systems, such protocols generally rely on computation-intensive encryption methods and multi-step authentication processes [7]. Most IoT devices in real life have constrained resources in terms of processing power, memory, and even battery life-all severely limit the potential to support this so-called resource-intensive security methodology. These are the limitations that are further muddled by the decentralized nature of IoT networks obviously called for more specialized lines of security solutions. Therefore, most researchers focused their attention on lightweight security mechanisms that would protect IoT devices without hindering their performance or shortening their lives.

Authentication is one of the main challenges in IoT security studies, in order to make sure only authorized entities interact with IoT devices or data generated by them. The literature has identified how important authentication will be to protect IoT networks against a wide variety of cyber threats, including unauthorized access, command spoofing, and data breaches [8]. Many novel approaches have, hence, been proposed in light of different limitations associated with traditional authentication methods. There are lightweight cryptographic algorithms that are quite often referred to in the literature for reducing computational load on IoT devices without compromising much on security features. These specifically designed algorithms require minimum processing power and energy. Besides that, hardware-based authentication has become popular and serves as another approach to safely verify identities directly at device levels in most cases without complicated software implementations.

Another interesting research area investigated in the literature is related to the decentralized authentication systems. In IoT networks that are characterized with distribution of huge number of connected devices geographically often in areas that are remote or may not easily be accessible, centralized authentication systems may prove to be a bottleneck or even a failure [9]. To this end, decentralized or peer to peer authentication schemes have been put forward that utilize the very P2P structure inherent in IoT systems. These approaches of authentication decentralize the processes, spread across the network which serves the purpose of improving reliability and eliminating the single points of failure. In addition, the concept of using blockchain technology in IoT authentication system has also been proposed to maintain the authenticity and certainty of transaction and interchange of messages between devices without needing the intervention of any third party.

Besides the authentication the literature also discusses general security measures of IoT like secure communication protocols and intrusion detection system. Some of the ways that have been proposed to tackle issues in IoT environment concerning transfer of data are the following: secure communication protocols have been proposed for IoT environment for secure data transfer across limited devices [10]. These protocols are meant to guarantee confidentiality and integrity in the data exchange during transmission besides bearing in mind the energy that is used to perform the exchange. Moreover, specific IDSs with focused on IoT networks – remain a popular issue in the literature. It is used to oversee the network in order to identify threats that may be in the process of attacking the system in order to reduce dangerous threats as early as possible. Nonetheless, developing IDS that can work perfectly well within the limits of IoT devices and at the same time, provide an equivalent level of real-time monitoring and minimal latency is still a concern for researchers working in this field.

Accordingly, the literature conveyed the general understanding that conventional security solutions are insufficient for IoT and that new solutions for IoT are needed. The advance of the security research is to address the issues of lightweight, decentralized, and scalability of IoT networks that make these systems more secure and reliable as they gain more popularity [11]. Despite the significant strides that have so far been made in IoT security, there are various critical research gaps that have not yet been addressed; hence, there exists a need for their further exploration.

Precisely, one of the key research gaps lies in the fact that the existing authentication mechanisms fall short of addressing the unique requirements of IoT environments. Traditional security protocols, though robust in general networks, are not usually optimized for IoT devices. Most IoT devices have limited computational power, memory, and energy resources. Most of the authentication systems standing today still tend to impose a heavy overhead on IoT devices [12], reducing their operational efficiency and shortening their battery life. Further, while some lightweight cryptographic methods have been proposed, the trade-off between the level of security and resource constraints of IoT devices remains an open challenge. Also, though promising, the various kinds of decentralized authentication models using blockchain technology for IoT are yet to be fully adapted or tested in large-scale IoT environments where heterogeneity of devices, scalability, and real-time communication are the main concerns.

Another gap in the literature is the comprehensive security frameworks that could integrate both authentication and secure communication protocols tailored for IoT ecosystems. Despite much into light-weight encryption and decentralized models, most solutions have been designed to cope either with authentication or data protection. Also, there is an emerging requirement for a single integrated approach that shall be capable of managing both secure identity verification and encrypted communication without overloading the resource-limited IoT devices [13]. Besides, intrusion detection systems for IoT networks, though researched extensively, remain a challenge for real-time threat detection and adaptability against diverse IoT architectures. Most of the proposed models regarding IDS are not that flexible to cope with dynamic IoT networks, where devices are joining and/or leaving the network quite frequently, while operating in a highly decentralized settings [14].

In this respect, the motivations toward this proposal are rooted in these research lacunae, in particular, by developing a lightweight and scalable security framework able to handle the multi-faceted challenges facing IoT environments. The increased usage of IoT devices within the important sectors of health care, transportation, and industrial automation further increases the urgency bar for robust security solutions [15]. Therefore, safety, privacy, and integrity of data across this networked system are not only a matter of preventing cyber threats but also of earning and upholding public confidence in IoT technology.

The proposed work tries to give a new direction by proposing lightweight authentication mechanisms that can be integrated within secure communication protocols to address the limitations of the existing protocols. The solution should, therefore, be resource-efficient and at the same time robust to cope with various cyber threats, while at the same time scalable for a growing number of devices in IoT ecosystems. The ultimate objective is thereby to fill the gap existing between security needs and resource constraints in IoT: it means enabling these devices to securely and efficiently perform their functions in applications ranging from current to future ones.

3. PROPOSED METHODOLOGY

The RNN-based security framework for IoT healthcare might become the most workable solution for such highly sensitive environments because the menace of data protection, unauthorized access, and malignant attacks is continuously growing. Continuous interaction through transmission and data collection of patients' real-time vital signs, medical imaging, and sensors is involved in the systems of IoT health care. Thus, these need to be secured. RNNs can model sequential data and catch temporal dependencies, hence they might be especially suitable to find patterns in streams of continuous data emanating from IoT health devices. This may make them very efficient in finding anomalies, unauthorized attempts at access, and possible breaches in security that may occur over time within a healthcare network.

The use of an RNN-based security framework in IoT healthcare has another great advantage in the area of the network learning from historical patterns, thereby catching subtleties within the flow of data indicative of a security threat. While most traditional security mechanisms normally rely on specific rule-based systems or static thresholds for intrusion detection, RNN can adapt dynamically with changing network traffic patterns. This flexibility is really important in health, as the quantity of data flowing from all those devices in IoT is a continuous stream; sometimes there are relationships in the data that just can't be modeled predictively or linearly.

Due to their internal memory, RNNs work especially fine with this kind of time-series data when the network remembers and uses previous inputs to give context to current decisions. Its readability is very helpful in the discovery of a cyber-attack that may be sophisticated or has a delay with respect to the attack, such as gradual manipulation of data or unauthorized long-term access that wouldn't be detected by traditional security ways. Another major plus of RNNs over any other machine learning models in IoT healthcare security is their capability to handle variable-length input sequences. IoT systems, in general, do not always generate data at fixed intervals, particularly in the case of healthcare. Sometimes, volume or frequencies of transmission may change with the type of device, or a particular condition to be monitored.

Unlike feed forward neural networks, RNNs process sequences of input of variable lengths and are hence more adaptive compared with traditional models that rely on inputs of a fixed size. This would, in turn, allow an RNN-based security framework to support the myriad IoT devices and sensors utilized in healthcare-from wearable devices reporting patient heart rate to large imaging systems with high-resolution scans. This flexibility extends the possibility of training RNNs on recognizing both individual device abnormal behavior and coordinated attacks across multiple devices within the network-a key capability in protecting interconnected healthcare systems.

A number of RNNs deployed in security frameworks bring forth hard benefits compared to the classic techniques, including signature-based IDS and rule-based firewalls. Since signature-based systems rely on predefined patterns of known threats, they will stop only previously encountered attacks. By contrast, RNNs will provide the possibility to detect zero-day attacks or unknown threats by learning the underlying normal network behavior distribution and detecting deviations from the established baseline. This is particularly important in IoT healthcare systems, since life-threatening risks might come along with a successful cyberattack. For instance, in the context of an RNN-based framework, the illegal intrusion into a patient's insulin pump would become predictable through recognition of abnormal patterns in the device's data transmission, even though such an attack has never been seen before.

Among other deep learning models, such as Convolutional Neural Networks, RNNs especially excel in the domain of security applications for IoT healthcare, since their scope resides under temporal sequences. Although CNNs are especially suitable for image and spatial data processing, the capability of RNNs to model temporal dependencies serves best for continuous network traffic monitoring and time-based anomaly detection. Moreover, one of the most famous modifications-RNN-LSTM-can resolve the problem of vanishing gradients: a model will be able to remember highly relevant information across very long sequences of data.

This is a big advantage in the healthcare security domain, as pattern detection across long time slots is an integral feature for different aspects of general protection. Such a framework can offer more flexibility in handling various and variable data streams and give huge advantages compared to traditional security mechanisms. What makes RNNs especially fitted to the security needs of IoT healthcare as a guarantee for safety, privacy, and reliability of the most sensitive systems in healthcare.

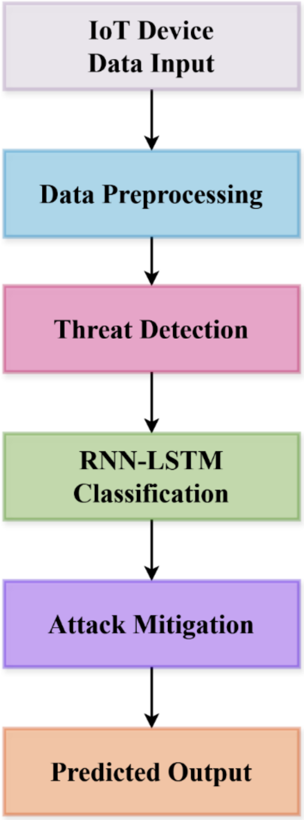

Fig .1. RNN-LSTM based IoT security framework

Fig 1 presents the proposed RNN-LSTM-based IoT security framework to extend security in IoT devices. In particular, these IoT devices run incessantly, generating data from various sensors and feeding the same to the RNN-LSTM processing module. It is here that the system actually learns from past sequences and recognizes those anomalies indicative of a security breach or an attack in progress. LSTM is known to cope much better with long-term dependencies and issues of vanishing gradients; therefore, it plays an important role in picking up time-dependent anomalies, which appear otherwise very minor and are not easily detectable through any conventional method.

In this way, it flags a possible threat against its known malicious behaviors after the RNN-LSTM has processed the data. It then refines this further in the prediction and response of zero-day attacks, which are new, previously unknown vulnerabilities. The third tier involves a strong module for attack mitigation that quickly triggers prevention measures, which neutralize or segregate the devices compromised by the detected threat from the rest of the IoT network before it spreads into the network. It will be useful, given the adaptation, scalability, and real-time processing for providing high advantages against a static or rule-based system that maintains limited flexibility for handling the evolution of cyber threats within the ecosystem of IoT.

4. RESULT AND DISCUSSION

The Fig. 2 compares the performance of the proposed IoT security based on RNN-LSTM with other well-known methods such as CNN, LSTM, RNN, and DNN. It is obvious from this graph that the traditional deep learning-based methods mainly comprising CNN and RNN for IoT security yield reasonable accuracy levels of security threats in IoT environments. The proposed model performs better compared to existing models. It might be because RNN can process in sequences, and LSTM has such a good ability in the capture of long-range dependency with reduced loss of context due to the vanishing gradient issue.

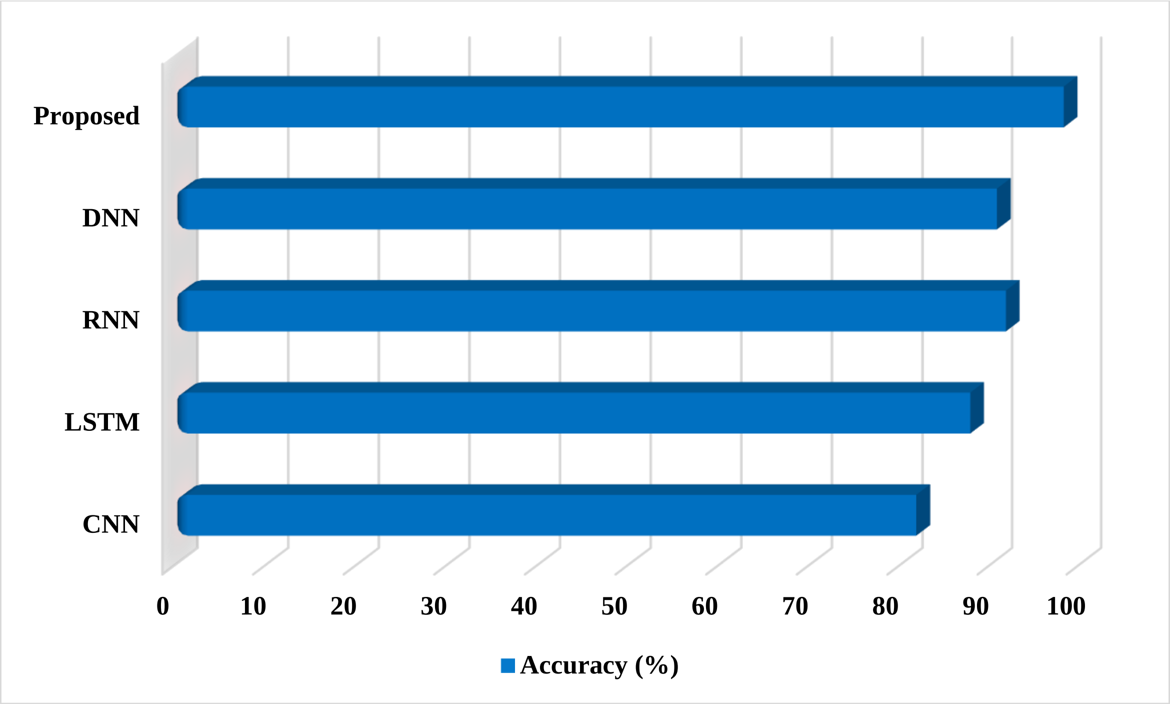

Fig .2. Accuracy comparison

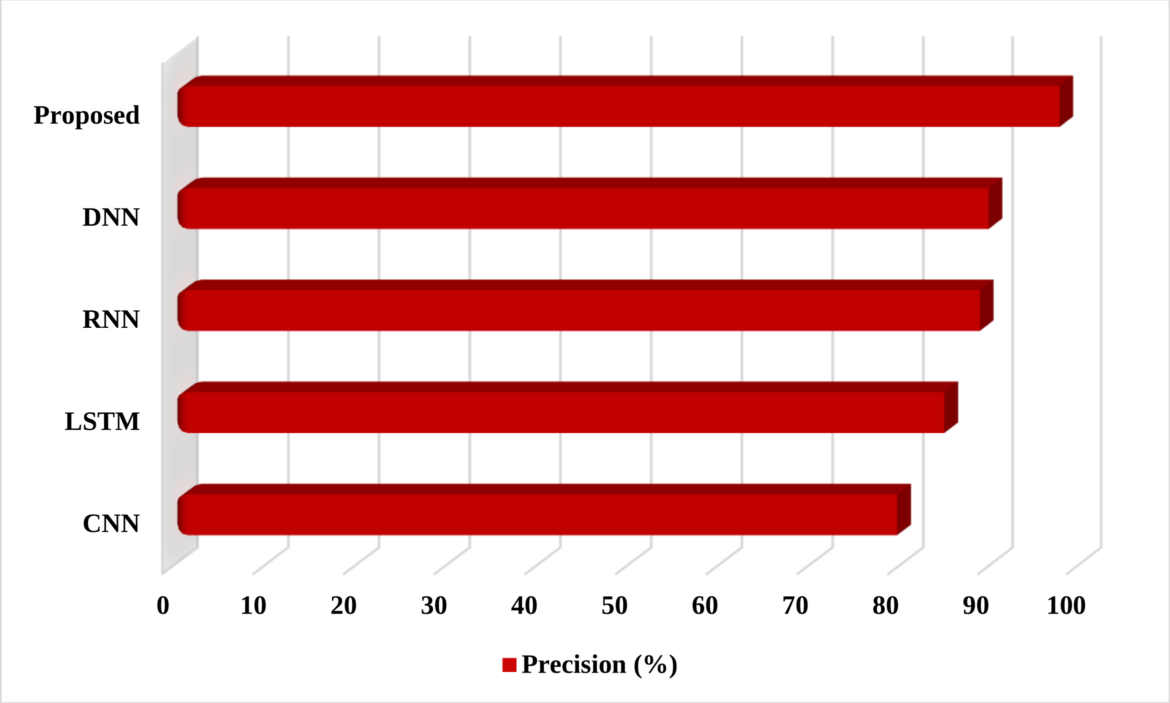

Fig .3. Precision comparison

The Fig 3 shows the precision comparison among CNN, LSTM, RNN, DNN, and the Proposed RNN-LSTM Framework. Precision is an important attribute in IoT security for minimizing false positives where benign actions are mistakenly identified as malicious. Among these, the proposed RNN-LSTM model significantly performs better than the state-of-the-art models. The performances of CNN and LSTM are slightly lower in terms of precision due to the fact that they might misclassify some patterns either by overfitting the spatial data or not capturing the long-term dependency sufficiently.

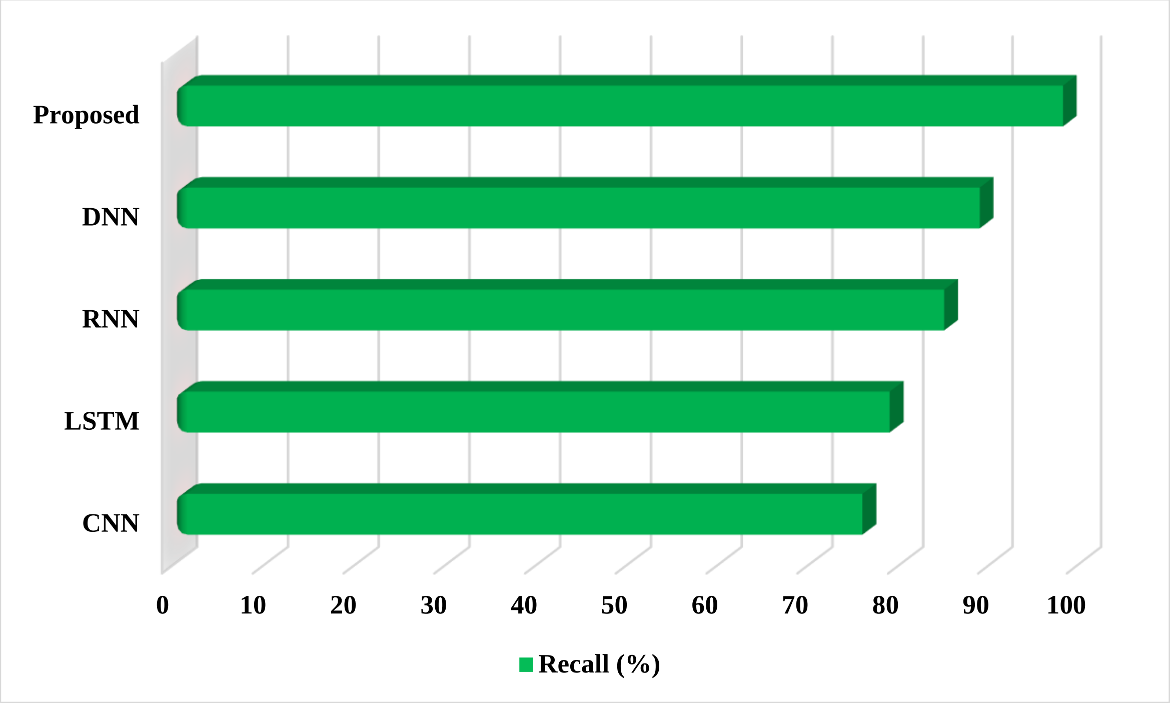

Fig .4. Recall comparison

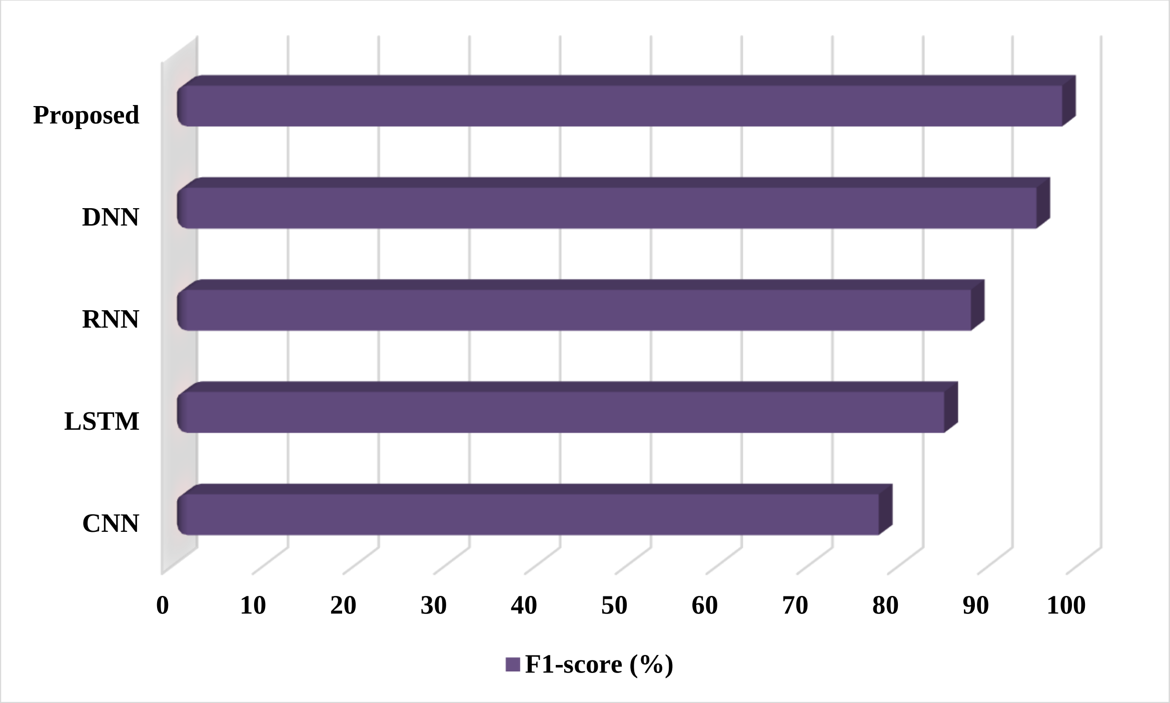

Fig .5. F1-score comparison

While RNNs are much better at processing sequences, they are not that good at retaining long-term information, which reduces precision. Combining RNN's sequence processing with the memory retention provided by the LSTM in the proposed model empowers it for higher precisions and thereby reduces unnecessary alarms in IoT healthcare systems where any disruption due to false alerts can make operations critical.

As shown in Fig 4, the outcome would be that hardly any critical threat can get overlooked this way, thus reinforcing the security integrity of such sensitive systems. Fig. 5 depicts the F1-score comparison, which is a balance between precision and recall; hence, it gives the holistic view of model overall performance in the detection of IoT security threats. While several IoT security applications demonstrated the performance of CNN, LSTM, RNN, and DNN models, none of the techniques solely provided the same level of balance between precision and recall as that obtained in the proposed RNN-LSTM framework.

Furthermore, the highest F1-score proved that this model was able to handle both false positives and false negatives with the highest level of efficiency. In this way, balancing in such healthcare environments becomes necessary, as the aftermath of undetected threats and even false alarms is grave. Basically, with the proposed model improved in F1-score, one is guaranteed overall reliability and capability not only in detecting the maximum amount of threats but also in maintaining the required accuracy and precision for an effective and reliable IoT security system.

5. CONCLUSION

The conclusion of this paper identifies and highlights the effectiveness and importance of the proposed security framework, RNN-LSTM-based, in IoT systems, particularly in healthcare; the more the proliferation of IoT devices increases, the more new vulnerabilities are introduced. This framework proposal overcomes the drawback of traditional techniques in security through an unprecedented integration of RNNs and LSTM units, allowing the analysis of time-series data in both immediate and developing threats. In contrast, the results returned by the proposed framework outshine the traditional models, CNN, RNN, LSTM, and DNN, based on critical metrics of accuracy, precision, recall, and F1-score. This would imply that the proposed framework can learn very subtle time-dependent anomalies with minimal false positives and false negatives.

This work insists on continuous threat monitoring and the need for dynamic models toward adapting to the IoT data streams in real time. The proposed framework elegantly avoids the problem of the vanishing gradient common in RNNs by embedding LSTM's capability of learning long-term dependencies, hence turning out to be more capable of detecting complex, cunning attacks that might go unnoticed by traditional approaches. The results and comparisons in this work have clearly indicated that the proposed RNN-LSTM-based model outperforms those from previous methods by a large margin. Thus, it assures a highly dependable security solution for critical IoT applications, such as healthcare, which demand both accuracy and timeliness in threat detection.

Funding

No institutional affiliations or sponsorship agreements are mentioned in the paper, indicating a lack of external funding.

Conflicts Of Interest

The author's affiliations, financial relationships, or personal interests do not present any conflicts in the research.

Acknowledgment

The author acknowledges the institution for the intellectual resources and academic guidance that significantly enriched this research.

References

[1] R. Zgheib, S. Kristiansen, E. Conchon, T. Plageman, V. Goebel, and R. Bastide, "A scalable semantic framework for IoT healthcare applications," Journal of Ambient Intelligence and Humanized Computing, vol. 14, pp. 4883-4901, 2023.

[2] A. Atadoga, T. T. Omaghomi, O. A. Elufioye, I. P. Odilibe, A. I. Daraojimba, and O. R. Owolabi, "Internet of Things (IoT) in healthcare: A systematic review of use cases and benefits," International Journal of Science and Research Archive, vol. 11, pp. 1511-1517, 2024.

[3] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, et al., "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," Internet of Things, vol. 22, p. 100721, 2023.

[4] S. Yazdanpanah, S. S. Chaeikar, and A. Jolfaei, "Monitoring the security of audio biomedical signals communications in wearable IoT healthcare," Digital Communications and Networks, vol. 9, pp. 393-399, 2023.

[5] R. Salama, F. Al-Turjman, P. Chaudhary, and S. P. Yadav, "(Benefits of Internet of Things (IoT) Applications in Health care-An Overview)," in 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), 2023, pp. 778-784.

[6] K. Sahinbas and F. O. Catak, "Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems," in Interpretable Cognitive Internet of Things for Healthcare, ed: Springer, 2023, pp. 57-72.

[7] S. Dharmadhikari, A. Kausar, M. Deore, N. S. Kittad, V. Bhagavan, and R. Krishnamoorthy, "IOT based healthcare monitoring system for smart city applications," in Human-Assisted Intelligent Computing: Modeling, simulations and applications, ed: IOP Publishing Bristol, UK, 2023, pp. 28-1-28-18.

[8] K. H. Almotairi, "Application of internet of things in healthcare domain," Journal of Umm Al-Qura University for Engineering and Architecture, vol. 14, pp. 1-12, 2023.

[9] B. G. Mohammed and D. S. Hasan, "Smart Healthcare Monitoring System Using IoT," Int. J. Interact. Mob. Technol., vol. 17, pp. 141-152, 2023.

[10] M. Bokharaei Nia, M. Afshar Kazemi, C. Valmohammadi, and G. Abbaspour, "Wearable IoT intelligent recommender framework for a smarter healthcare approach," Library Hi Tech, vol. 41, pp. 1238-1261, 2023.

[11] H. Verma, N. Chauhan, and L. K. Awasthi, "A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns," Computer Science Review, vol. 50, p. 100591, 2023.

[12] A. Balasundaram, S. Routray, A. Prabu, P. Krishnan, P. P. Malla, and M. Maiti, "Internet of Things (IoT)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care," IEEE Internet of Things Journal, vol. 10, pp. 18563-18570, 2023.

[13] N. Yathiraju and A. Mohapatra, "The Implications of IoT in the Modern Healthcare Industry post COVID-19," International Journal of Smart Sensor and Adhoc Network, vol. 3, 2023.

[14] S. M. K. Sistla and B. K. Konidena, "IoT-Edge Healthcare Solutions Empowered by Machine Learning," Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), vol. 2, pp. 126-135, 2023.

[15] K. Mehta, S. Gaur, S. Maheshwari, H. Chugh, and M. Anibhushan Kumar, "Big Data Analytics Cloud based Smart IoT Healthcare Network," in 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), 2023, pp. 437-443.