IRSTI 28.23.15

10.51889/2959-5894.2026.93.1.016

G.I. Beissenova[1], R.D. Ospanova[2], U.B. Balgymbekova[2], G.M. Abdrakhmanoava[2], A.N. Zhidebayeva[3*]

[1]Mukhtar Auezov South Kazakhstan University, Shymkent, Kazakhstan
[2]Central Asian Innovative University, Shymkent, Kazakhstan
[3]Peoples Friendship University named after Academician A. Kuatbekov, Shymkent, Kazakhstan
[*]*e-mail:* aziza_68.kz@mail.ru

NEURAL NETWORK – BASED SECURITY FRAMEWORK FOR IOT DEVICES

Abstract

The research article demonstrates that current IT advancements include the rapid growth of the Internet of Things (IoT). The Internet of Things allows tangible elements to be integrated into digital frameworks. A complex infrastructure of smart sensors, sensor networks, home appliances, industrial controllers, and medical devices automates processes, improves management, and enables new services. The Internet of Things affects energy, transportation, manufacturing, healthcare, and education. The research demonstrates the effectiveness of a machine learning model for classifying normal and anomalous data in IoT systems. To evaluate the performance of our proposed model, we used an open-source BoT-IoT dataset for the IoT environment. 80 percent of the dataset used for the study was used for model training, while 20 percent was implemented in testing mode. Classification metrics, including precision, recall, and F1-score, approach 1.0, indicating high accuracy with a 100% classification rate. The model, particularly the Random Forest, successfully identifies anomalies in network behavior and triggers alarms when threats are detected. It highlights the advantages of using deep neural networks for malware detection in IoT environments, which can analyze both static binary files and dynamic process behaviors. These models adapt to new threats, enhancing security measures in a landscape where traditional methods fall short.

Keywords: IOT, information technologies, artificial intelligence, anomaly detection, CNN, LSTM.

Г.И. Бейсенова[1], Р.Д. Оспанова[2], У.Б. Балгимбекова[2], Г.М. Абдрахманова[2], А.Н. Жидебаева[3]
[1]М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент қ., Қазақстан,
[2]Орталық Азия инновациялық университеті, Шымкент қ., Қазақстан,
[3]Академик А.Қуатбеков атындағы Халықтар достығы университеті, Шымкент қ., Қазақстан

ЗАТТАР ИНТЕРНЕТІ ҚҰРЫЛҒЫЛАРЫН ҚОРҒАУДА НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚОЛДАНУ

Аңдатпа

Ұсынылып отырған зерттеу мақаласында қазіргі IT жетістіктеріне заттар интернетінің (IoT) жылдам өсуіндегі жетістіктер туралы баяндалады. Заттар интернеті материалдық элементтерді сандық құрылымдарға біріктіруге мүмкіндік береді. Ақылды сенсорлардың, сенсорлық желілердің, тұрмыстық техниканың, өнеркәсіптік контроллерлердің және медициналық құрылғылардың күрделі инфрақұрылымы процестерді автоматтандырады, басқаруды жақсартады және жаңа қызметтерді ұсынады. Заттар интернетін пайдалану энергетикаға, көлікке, өндіріске, денсаулық сақтауға және білім беруге әсер етеді. Зерттеу жұмысының мақсаты - заттар интернеті (IoT) жүйелеріндегі қалыпты және аномальды деректерді жіктеуде машиналық оқыту моделінің тиімділігін көрсетеді. Ұсынып отырған модельіміздің өнімділігін бағалау үшін IoT ортасына арналған ашық қолжетімді BoT-IoT деректер жиыны пайдаланылды. Зерттеуге пайдаланылған деректер қорының 80 пайызы модельді оқытуға пайдаланылса, 20 пайызы тестілеу режимінде жүзеге асырылды. Зерттеудің нәтижесі дәлдік (precision), еске түсіру(recall) және F1 ұпайын қоса алғанда, жіктеу көрсеткіштері 1.0 тәсілі, 100% жіктеу деңгейімен жоғары дәлдікті көрсетеді. Модель, әсіресе кездейсоқ орман (Random Forest), желілік мінез-құлықтағы ауытқуларды сәтті анықтайды, қауіптер анықталған кезде дабылдарды іске қосады. Сондай -ақ, IoT орталарында зиянды бағдарламаларды анықтау үшін терең нейрондық желілерді пайдаланудың артықшылықтарын атап көрсетеді, олар статикалық екілік файлдарды да,

динамикалық процестердің мінез-құлқын да талдай алады. Бұл модельдер жаңа қауіптерге бейімделеді, дәстүрлі әдістер жетіспейтін жағдайда қауіпсіздік шараларын күшейтеді.

Түйін сөздер: IOT, ақпараттық технологиялар, жасанды интеллект, аномалияларды анықтау, CNN, LSTM.

Г.И. Бейсенова[1], Р.Д. Оспанова[2], У.Б. Балгимбекова[2], Г.М. Абдрахманова[2], А.Н. Жидебаева[3]
[1]Южно-Казахстанский университет имени М.Ауэзова, г.Шымкент, Казахстан,
[2]Центрально-Азиатский инновационный университет, г.Шымкент, Казахстан
[3]Университет дружбы народов имени академика А.Куатбекова, г.Шымкент, Казахстан

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ЗАЩИТЫ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация

В представленной исследовательской работе рассматривается стремительный рост Интернета вещей (IoT) в современных ИТ-разработках. Интернет вещей позволяет интегрировать физические элементы в цифровые структуры. Сложная инфраструктура интеллектуальных датчиков, сенсорных сетей, бытовой техники, промышленных контроллеров и медицинских устройств автоматизирует процессы, улучшает управление и предоставляет новые услуги. Использование Интернета вещей затрагивает энергетику, транспорт, производство, здравоохранение и образование. Цель исследовательской работы – продемонстрировать эффективность модели машинного обучения в классификации нормальных и аномальных данных в системах Интернета вещей (IoT). Для оценки производительности предложенной нами модели мы использовали открытый набор данных BoT-IoT для среды Интернета вещей. 80 процентов набора данных, использованного в исследовании, было использовано для обучения модели, а 20 процентов – в тестовом режиме. Результаты исследования показывают, что метрики классификации, включая точность, полноту и F1-меру, демонстрируют высокую точность с коэффициентом классификации 1,0, особенно модель Random Forest, успешно выявляющая аномалии в поведении сети и запускающая оповещения при обнаружении угроз. Также подчеркиваются преимущества использования глубоких нейронных сетей для обнаружения вредоносного ПО в средах IoT, которые могут анализировать как статические бинарные файлы, так и поведение динамических процессов. Эти модели адаптируются к новым угрозам, усиливая меры безопасности там, где традиционные методы терпят неудачу.

Ключевые слова: Интернет вещей (IoT), информационные технологии, искусственный интеллект, обнаружение аномалий, CNN, LSTM

Introduction

The swift proliferation of the Internet of Things (IoT) is a hallmark of the current phase of technological advancement. The Internet of Things facilitates the incorporation of tangible elements into a cohesive digital framework. Smart sensors, sensor networks, home appliances, industrial controllers, and medical devices form a complex infrastructure that supports process automation, improves operational efficiency, and enables the development of new services. The energy, transportation, manufacturing, healthcare, and education sectors are substantially influenced by the extensive use of the IoT.

According to international analytical agencies, the number of connected IoT devices is increasing rapidly, with projections indicating it will surpass tens of billions in the coming years. Alongside the tremendous potential they offer to society and the economy, these processes also raise significant concerns about information security. A heterogeneous array of devices employing various protocols in a dispersed setting may be a potential target for cybercriminals. The primary dangers include the proliferation of viruses, distributed denial-of-service (DDoS) attacks that inundate servers with traffic from multiple sources, unauthorized remote access, and the alteration or disclosure of sensitive information.

Firewalls, rule-based intrusion detection systems, cryptographic algorithms, and traffic filtering exemplify classic security methods that remain integral to security architecture. Nonetheless, the ever-evolving nature of digital threats undermines the effectiveness of such initiatives. To circumvent security measures, adversaries employ creative approaches, including deploying botnets that leverage

IoT devices and exploiting vulnerabilities in software and hardware platforms. Consequently, standard methods are frequently inadequate for the rapid identification and mitigation of attacks.

In these situations, artificial intelligence (AI) approaches, especially neural networks, are gaining prominence. This is because they have shown considerable efficacy in classification, forecasting, and analysis of extensive data streams. The use of neural network models facilitates a shift from static restrictions to intelligent adaptive systems capable of identifying previously unnoticed hazards. The precise detection of anomalies is facilitated by the creation of standard activity profiles, the examination of device behavioral traits, and the real-time monitoring of network data.

Neural networks are employed in various essential areas of IoT infrastructure security. They can identify deviations from standard device activity patterns, facilitating intelligent anomaly detection. Secondly, deep machine learning models can classify both malware and network packets, rendering them more reliable than signature-based methods for attack detection. Thirdly, neural networks are employed in multi-factor authentication systems that process biometric data. This diminishes the probability of unauthorized access to equipment [1-2].

Numerous challenges complicate the application of neural networks for cybersecurity within the IoT. This encompasses the significant computational complexity of algorithms, the need for large training datasets, and the difficulty in interpreting model outputs. Hybrid architectures, including convolutional and recurrent neural networks, are widely used because they maintain real-time system performance while achieving high accuracy in attack detection. Consequently, one might argue that neural networks are increasingly vital tools for safeguarding IoT devices and networks. Their implementation introduces new opportunities for advancing adaptive and intelligent cyber defense systems, enabling responses to a rapidly evolving threat landscape [3]. This article examines the role of neural networks in enhancing the security of the IoT and evaluates the practical implications of their use in this domain.

Research Methodology

Recent research in information security demonstrates that neural networks are essential to advancing intelligent security solutions in IoT frameworks. Their use arises from the ability to analyze vast data streams, identify hidden patterns, and adjust to changing circumstances, significantly improving the effectiveness of combating cyber-attacks. Unlike traditional methods that rely on fixed rules or signature databases, neural network methodologies deliver adaptive responses to emerging threat vectors, thereby providing superior protection. This study examines the principal areas of neural network application in IoT device security [4].

The work used the open-source BoT-IoT dataset to identify anomalies in IoT devices. The dataset, which can be downloaded from Bot-IoT_Dataset – OneDrive, includes both normal and malicious traffic on IoT networks. This dataset was generated by modeling real network traffic and includes both normal and anomalous activities.

The BoT-IoT dataset includes various types of cyberattacks, including:

a) Distributed Denial of Service (DDoS) attacks,
b) Botnet activity, malicious actions, and suspicious network traffic patterns.

Each data item in the dataset is labeled, meaning that each item is assigned to a corresponding class (normal or anomaly). This creates a favorable environment for training and evaluating machine learning models.

During the research work, the data was pre-processed: unnecessary labels were removed and the data was normalized. In addition, the dataset was divided into training and testing sets (for example, 80% - training, 20% - testing).

Identification of anomalies

Anomaly detection, the process of identifying deviations from the normative behavior of systems or devices, is essential for IoT security. Neural networks, especially autoencoders and recurrent architectures such as LSTMs, have demonstrated considerable effectiveness in this field. They can assess network traffic, sensor telemetry, and device behavioral profiles instantaneously.

Figure 1 shows anomaly detection results from the Random Forest algorithm.

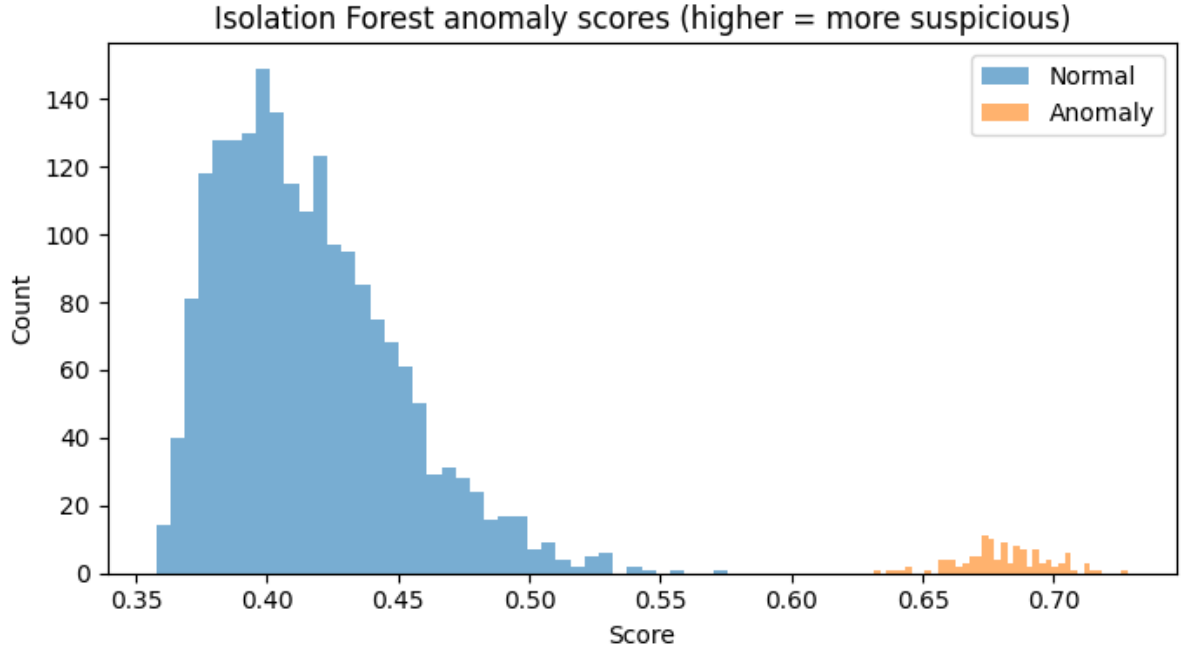

Figure 1. Distribution of abnormal and normal data by points

The upper section displays classification metrics:

a) The precision, recall, and F1-score for both the "Normal" and "Anomaly" classes approach 1.0, signifying nearly flawless data differentiation.

b) The confusion matrix indicates that the model accurately categorized 2000 objects as normal and 120 as anomalous, with minimal errors.

c) The classification accuracy achieved was 100%.

d) The histogram of the anomalous score distribution is presented below.

e) The blue hue signifies standard observations, with values between 0.35 and 0.55.

f) The orange anomalies are strongly delineated and fall within the 0.60–0.70 range.

g) A higher "score" indicates greater suspicion over the object.

h) The graph indicates that the Random Forest model proficiently identifies assaults and failures in IoT systems, as their distributions rarely intersect.

This method enables the identification of aberrant behavior, including substantial increases in network packets, access to atypical resources, changes in temporal patterns, or unauthorized access attempts [5]. Upon identifying an anomaly, the system independently triggers alarms or initiates protocols to prevent suspicious activity. The advantage resides in the neural network's ability to identify previously undetected dangers that lack observable indicators, which is especially vital in the context of rapidly evolving attacks.

Malware detection

Neural networks are used to classify malware that can compromise IoT devices via network protocols, updates, or firmware vulnerabilities. Unlike traditional signature-based methods, deep neural networks (DNNs, CNNs) can identify advanced characteristics in program code or network packets, distinguishing between benign and malicious activities.

These models utilize both static analysis, which scrutinizes binary files and their architectures, and dynamic analysis, which observes process behavior in real time. Extensive research indicates that deep architectures can significantly improve malware detection accuracy and reduce false-positive rates. This is especially vital in the IoT landscape, where the widespread implementation of devices and their limited computational capacities render traditional security measures ineffective [6].

Adaptive safeguarding

The principal benefit of neural networks is their ability to learn and adapt. Unlike static security systems that operate according to predetermined protocols, neural network models can be improved and adapted to respond to emerging threats. Training may occur on centralized servers or via distributed or federated learning, which is especially pertinent for the IoT, as data is stored across multiple devices.

The figure 2 depicts the calibration of biometric verification thresholds based on cosine similarity.

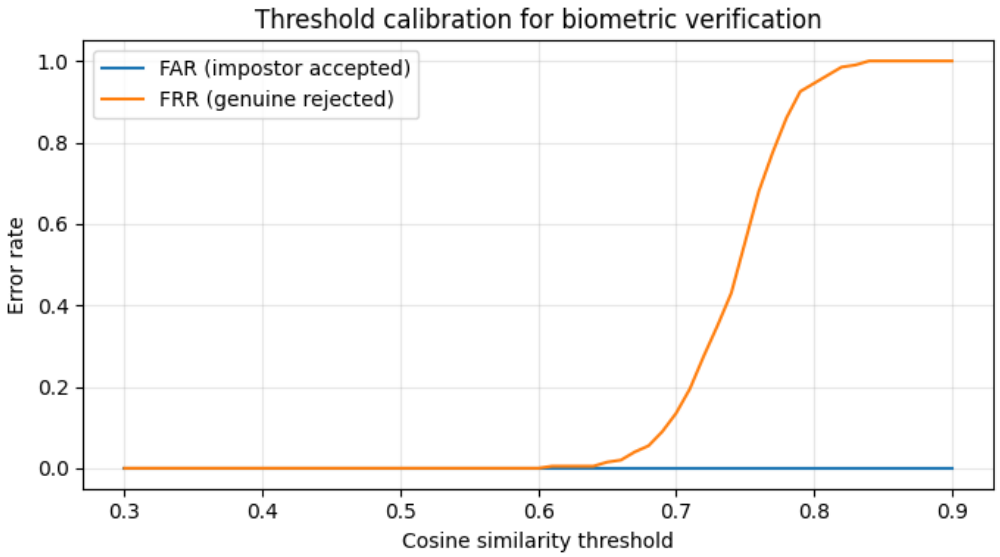

Figure 2. Biometric verification threshold calibration chart

The X-axis represents cosine similarity threshold values, and the Y-axis denotes the error rate. The blue FAR (False Acceptance Rate) indicator signifies the probability of erroneously accepting a "impostor" (unauthorized user). The orange FRR indication signifies the probability of erroneously rejecting a legitimate user.

The graph indicates that false acceptance is infrequent at low threshold levels; however, it increases significantly above 0.7, as evidenced by the rise in the FRR indicator. This indicates that stringent thresholds elevate rejections, even for authorized users [7].

Achieving a balance between security and convenience requires selecting the optimal cosine similarity threshold. The suggested threshold range is 0.65–0.7, which optimally balances a low false acceptance rate (FAR) and a moderate false rejection rate (FRR) to maintain the dependability of biometric identification systems in the IoT context.

Adaptability improves system resilience against novel attacks, including modified versions of existing exploits, zero-day vulnerabilities, and advanced targeted assaults. Furthermore, the application of transfer learning techniques enables the swift adaptation of pre-trained models to new contexts, hence minimizing resource and time costs.

Intelligent Authentication

The authentication procedure for users and devices is a vulnerability inside the IoT framework. The security provided by conventional systems, such as passwords or personal identification numbers (PIN codes), is insufficient. In this context, there is significant activity in developing neural network-based techniques utilizing biometric characteristics [8].

Convolutional neural networks (CNNs) exhibit a significant level of precision in tasks involving the identification of faces, fingerprints, and irises. Recurrent neural networks are used to examine vocal attributes and user behavior dynamics. The likelihood of unauthorized access to IoT devices is markedly reduced when multi-factor authentication, leveraging multiple biometric characteristics concurrently, is implemented [9].

Consequently, neural networks provide a multi-tiered protection for IoT devices, encompassing traffic analysis and monitoring as well as sophisticated user identification. Adaptive cyber protection measures can be implemented to withstand various threats. Nonetheless, it is crucial to acknowledge concurrent drawbacks, including increased computational complexity, the need for high-quality training data, and the challenge of interpretability [10-11]. Nonetheless, advances in hardware accelerators, the introduction of innovative model optimization techniques, and the rise of Explainable Artificial Intelligence (AI) are progressively mitigating these issues [12].

Results of the study

An experiment employed a hybrid model combining convolutional neural networks (CNN) and bidirectional recurrent LSTM networks to evaluate IoT network data. The study evaluated the model's capacity to categorize system states (normal vs. anomalous) and to discern data behavior patterns at different processing stages.

Examination of input temporal series

The initial graph (Figure 1, upper panel) illustrates packets per second and outbound traffic derived from the time series mimicking IoT device network settings. It should be noted that the values are stochastic and exhibit moderate variability, characteristic of actual network dynamics. Although local variations and bursts are observable, they may signify atypical behavior. The data's initial condition is shown prior to the neural network's feature extraction.

Feature Extraction Using CNN

The second panel of Figure 1 illustrates the channel-averaged activations of the CNN convolutional layer. The convolutional filters attenuate the signal and emphasize temporal variations in traffic intensity. CNNs can identify localized patterns, such as transient activity surges or anomalous packet distributions. These attributes supply the model's recurrent block.

Consequently, the CNN decreases data dimensionality while enhancing information density. The incremental increase in average activation over time indicates the extraction of features relevant to classification.

Temporal Dependencies and Bidirectional Long Short-Term Memory

The third panel of Figure 1 illustrates the dynamics of the BiLSTM hidden states. The normative values of the concealed vectors progressively rise, culminating towards the conclusion of the sequence. Data accumulation over many time steps indicates that BiLSTM models effectively capture long-term dependencies. CNN emphasizes local patterns, but LSTM analyzes global context, which is crucial in network traffic analysis, where abnormalities may develop gradually.

Concealed activations at the sequence's conclusion may suggest that the network acquires knowledge of aberrant characteristics. These dynamics reinforce the notion that recurrent networks are crucial for identifying intricate and protracted anomalies.

Classification outcomes

The model quantifies prediction confidence instead of rendering a binary decision. This attribute is advantageous in IoT systems, as it enables administrators to use probabilistic predictions to establish adaptive thresholds for monitoring and active response.

Significance and utilization

The findings indicate that the hybrid CNN + BiLSTM architecture can address two issues concurrently:

a) CNN local analysis for identifying short-term traffic surges.
b) Global LSTM analysis incorporates long-term dependencies and the buildup of anomalies.

This approach effectively identifies intricate attacks, encompassing concealed or "slow" anomalies that conventional methods fail to detect. Hybrid methods diminish false positives and enhance the reliability of IoT security.

The figure 3 shows visualizing the model's functionality (CNN activations and LSTM hidden states) helps researchers understand the patterns the network recognizes and their influence on the final decision. This links these systems with Explainable AI, which is essential in cybersecurity.

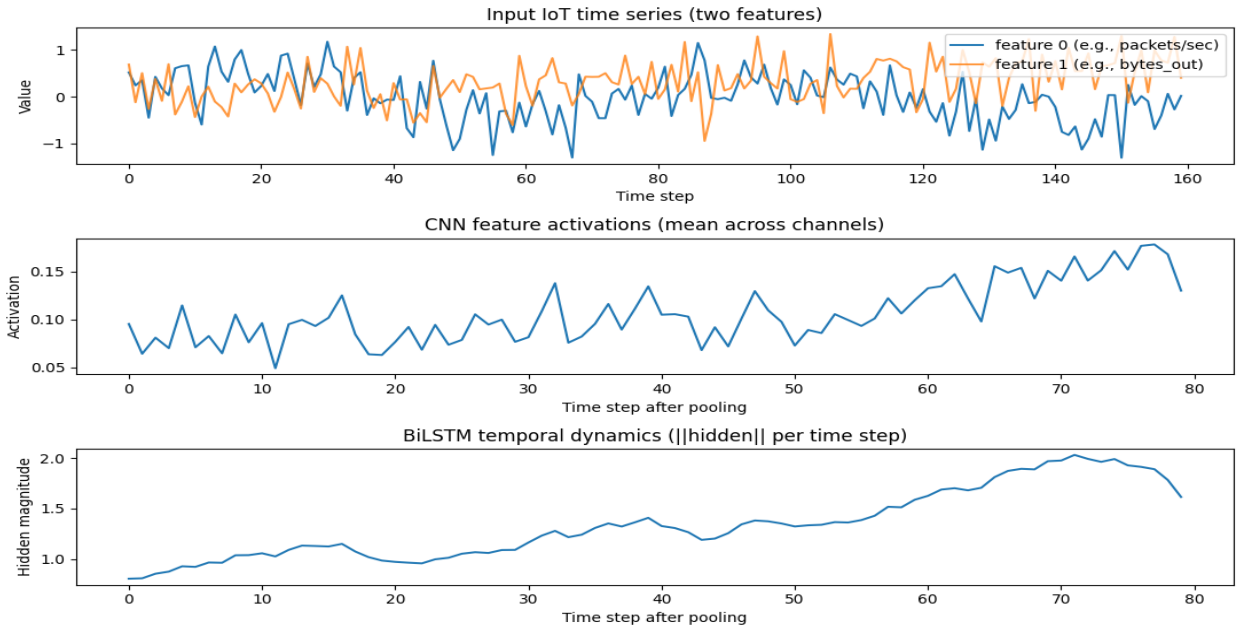

Figure 3. Hybrid CNN–BiLSTM model temporal dynamics visualization

The trials demonstrate that the hybrid CNN + BiLSTM model can identify anomalies in IoT traffic. The model emphasized significant traits, accounted for temporal context, and produced dependable probabilistic predictions. The displayed outcomes validate the architectural selection and provide enhanced optimization, including attention methods and more representative feature sets.

The figure 4 depicts the probability distribution of the hybrid CNN + BiLSTM model for binary classification of "norm/anomaly."

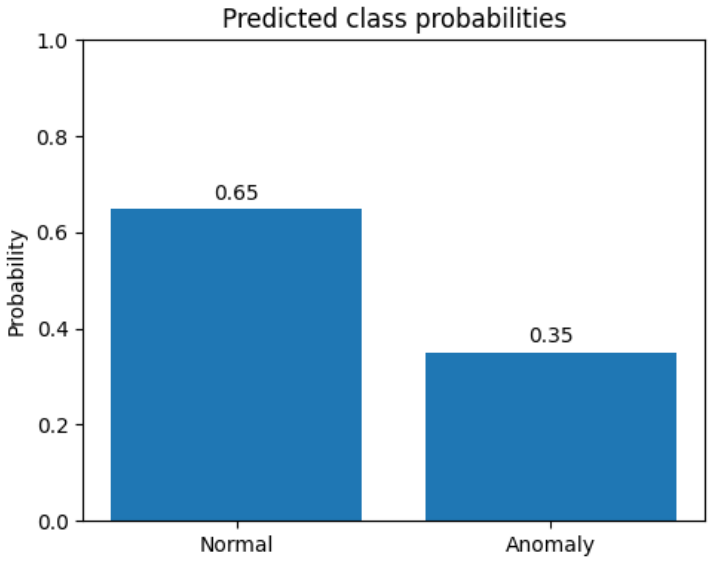

Figure 4. Distribution of prediction probabilities of the hybrid CNN–BiLSTM models

The model's confidence in the case's classification is indicated by the bar's height. The likelihood of the "Norm" class was 65%, whereas that of the "Anomaly" class was 35%. This outcome indicates that the model renders both categorical and probabilistic determinations, enabling the evaluation of a network event's "suspiciousness."

The analysis of these results is essential for IoT system applications. For instance:

a) Should the threshold of 70–80% be surpassed, the system will obstruct dubious activities. Events exhibiting an anomaly probability between 30% and 50% may be classified as "doubtful" and forwarded to the administrator for additional examination.

b) Probabilistic inference facilitates adaptable system modifications to meet particular security demands: essential infrastructures employ rigid thresholds, whereas residential IoT devices utilize more lenient thresholds.

c) The graph indicates that CNN + BiLSTM can effectively detect anomalies and evaluate decision confidence, which is essential in unpredictable and noisy network data.

Discussion

The research indicated that neural networks hold significant potential for cybersecurity in the Internet of Things. The increasing prevalence of connected devices and the complexity of network interaction design pose new challenges for intelligent, adaptive security measures. Deep learning addresses challenges that conventional technologies could not resolve.

Anomaly detection is effective in neural networks. Convolutional neural networks (CNNs) identify local patterns and transient network traffic surges, whereas recurrent neural networks (LSTMs, BiLSTMs) address long-term dependencies and variations in device behavior. These techniques in hybrid models provide thorough data analysis, enhancing the identification of attacks, even concealed or gradual irregularities.

Secondly, neural network techniques have demonstrated efficacy in classifying harmful code and analyzing network traffic. Deep learning models can generalize from experience, detect novel dangers, and minimize false positives, unlike signature systems. This is essential given the rapid release of new exploits and the evolution of attacks.

Third, the study emphasizes the use of sophisticated authentication systems. Biometric neural network models (voice, facial, behavioral) can enhance the trustworthiness of IoT devices and reduce unauthorized access. Multi-factor authentication enhances security by integrating biometrics, behavioral attributes, and contextual elements.

Conclusion

Nonetheless, prevailing constraints must be acknowledged. Significant computing expenses, extensive training datasets, and opaque decision-making processes persist as challenges. To deploy models in the IoT ecosystem, structures must be optimized, algorithmic resource consumption must be minimized, and explainable AI methodologies must be established. Federated and distributed learning minimize data transmission and the risk of exposing confidential information.

In summary, neural networks are establishing a novel paradigm for IoT cybersecurity. Their implementation enables intelligent security systems to adapt to a rapidly evolving threat environment, detect novel anomalies, and maintain user confidence. Consequently, deep learning techniques for IoT must be developed and incorporated to establish a sustainable and reliable digital ecosystem within the framework of global digitalization.

References

[1]Mu, X., & Antwi-Afari, M. F. (2024). The applications of IoTin industrial management: a science mapping review. International Journal of Production Research, 62(5), 1928-1952.

[2]Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., & Mani, L. (2024). Gravitating towards internet of things: Prospective applications, challenges, and solutions of using IoT. International Journal of Religion, 5(2), 436-451.

[3]Bekualykyzy, B. G., Zhakypkyzy, Z. A., Nurbolat, T., Alimhan, K., Sherzod, T., & Smakhulovna, S. G. (2024, May). Control of nonlinear system by means of feedback using the Python-control library. In 2024

IEEE 4th International Conference on Smart Information Systems and Technologies (SIST) (pp. 164-168). IEEE.

[4]Rath, K. C., Khang, A., & Roy, D. (2024). The role of IoTtechnology in Industry 4.0 economy. In Advanced IoT technologies and applications in the industry 4.0 digital economy (pp. 1-28). CRC Press.

[5]Belessova, D., Ibashova, A., Zhidebayeva, A., Shaimerdenova, G., & Nakhipova, V. (2024). The impact of "scratch" on student engagement and academic performance in primary schools. Open Education Studies, 6(1), 20220228.

[6]Hashem, I. A., Siddiqa, A., Alaba, F. A., Bilal, M., & Alhashmi, S. M. (2024). Distributed intelligence for IoT-based smart cities: A survey. Neural Computing and Applications, 36(27), 16621-16656.

[7]Makhanova, Z., Beissenova, G., Madiyarova, A., Chazhabayeva, M., Mambetaliyeva, G., Suimenova, M., ... & Baiburin, A. (2024). A Deep Residual Network Designed for Detecting Cracks in Buildings of Historical Significance. International Journal of Advanced Computer Science & Applications, 15(5).

[8]Erhueh, O. V., Elete, T., Akano, O. A., Nwakile, C., & Hanson, E. (2024). Application of IoTin energy infrastructure: Lessons for the future of operations and maintenance. Comprehensive Research and Reviews in Science and Technology, 2(2), 28-54.

[9]Belessova, D., Ibashova, A., Bosova, L., & Shaimerdenova, G. (2023). Digital learning ecosystem: Current state, prospects, and hurdles. Open Education Studies, 5(1), 20220179.

[10] Prince, N. U., Al Mamun, M. A., Olajide, A. O., Khan, O. U., Akeem, A. B., & Sani, A. I. (2024). IEEE Standards and Deep Learning Techniques for Securing IoTDevices Against Cyber Attacks. Journal of Computational Analysis & Applications, 33(7).

[11] Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-4). IEEE.

[12] Illakya, T., Keerthana, B., Murugan, K., Venkatesh, P., Manikandan, M., & Maran, K. (2024, April). The role of the internet of things in the telecom sector. In 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT) (pp. 1-5). IEEE.