Advancing Hospital Cybersecurity Through IoT-Enabled Neural Network for Human Behavior Analysis and Anomaly Detection

Faisal ALmojel, Shailendra Mishra
Department of Computer Science, College of Computer and Information Sciences,
Majmaah University, Al Majmaah, 11952, Saudi Arabia

***Abstract*—The integration of Internet of Things (IoT) technologies in hospital environments has introduced transformative changes in patient care and operational efficiency. However, this increased connectivity also presents significant cybersecurity challenges, particularly concerning the protection of patient data and healthcare operations. This research explores the application of advanced machine learning models, specifically LSTM-CNN hybrid architectures, for anomaly detection and behavior analysis in hospital IoT ecosystems. Employing a mixed-methods approach, the study utilizes LSTM -CNN models, coupled with the Mobile Health Human Behavior Analysis dataset, to analyze human behavior in a cybersecurity context in the hospital. The model architecture, tailored for the dynamic nature of hospital IoT activities, features a layered. The training accuracy attains an impressive 99.53%, underscoring the model's proficiency in learning from the training data. On the testing set, the model exhibits robust generalization with an accuracy of 91.42%. This paper represents a significant advancement in the convergence of AI and healthcare cybersecurity. The model's efficacy and promising outcomes underscore its potential deployment in real-world hospital scenarios.**

Keywords—IoT security; cyber security; network security; machine learning; LSTM

I. INTRODUCTION

The integration of Artificial Intelligence (AI) into cybersecurity, especially for the Internet of Things (IoT), is an important development in keeping our digital world safe. IoT is all about connecting everyday devices to the internet, from smart home appliances to complex industrial tools. These devices collect lots of data, which is very useful but also makes them targets for cyber attacks. That's why strong cybersecurity is essential. [1]. The increasing integration of technology, particularly the Internet of Things (IoT), in hospital environments has revolutionized healthcare delivery [2]. While these technological advancements offer unparalleled benefits, they also introduce new challenges, particularly in the realm of cybersecurity [3]. Hospitals are prime targets for cyber threats due to the sensitive nature of patient data and the critical reliance on interconnected devices. As such, fortifying the security of IoT systems in healthcare settings becomes imperative to ensure the confidentiality, integrity, and availability of critical medical information.In the past [4], cybersecurity mostly relied on set rules to protect against known threats. But as cyber attacks become more complex, especially with the rise of IoT, we need smarter and more flexible security solutions. This is where AI comes in, particularly with technologies like neural networks and fuzzy systems.

Neural networks are a type of AI that learns from data and makes decisions, much like how our brains work [5]. They are great at recognizing patterns, including new and complicated cyber threats that older security methods might miss. Fuzzy systems are another type of AI that's good at making sense of uncertain or vague information [6]. This is helpful in cybersecurity, where it's not always clear if something is a threat However, using these advanced AI methods in IoT is challenging because many IoT devices have limited power and can't handle complex calculations [7]. One solution is to use edge computing, which processes data closer to where it's collected. This approach can make things faster and reduce the need for sending data over long distances. Using AI in IoT cybersecurity is crucial. It makes our security systems more adaptable and better at handling the ever-changing nature of cyber threats. It's a key step in protecting our increasingly connected world.

A. Problem Evolution

The integration of Internet of Things (IoT) technologies within hospital environments has ushered in a new era of enhanced patient care and operational efficiency [8]. However, this increased connectivity also introduces significant cybersecurity challenges that threaten patient data integrity and the overall safety of healthcare operations. Hospital IoT ecosystems, comprised of interconnected devices and sensors, are particularly susceptible to a range of cyber threats due to inadequate security measures and outdated software.

One of the main concerns is the vulnerability of IoT devices in hospitals to various attacks, including unauthorized access, data breaches, and malware infections. These vulnerabilities stem from insufficient security measures and the use of outdated software, making it imperative to strengthen cybersecurity protocols to protect against such threats. Detecting anomalous behavior or deviations from normal patterns within the hospital IoT ecosystem is crucial for early identification and mitigation of potential security breaches [9]. An effective anomaly detection system can help in promptly identifying suspicious activities, thereby enhancing the overall security posture of hospital IoT deployments.

Safeguarding the integrity and privacy of sensitive patient data transmitted and stored by IoT devices is essential for maintaining patient trust and compliance with regulatory standards [10]. Ensuring robust data integrity and privacy practices is paramount in healthcare settings to prevent unauthorized access or breaches that could compromise patient confidentiality.Hospitals require rapid detection and response capabilities to address cybersecurity incidents in real-time. The ability to detect and respond to threats promptly is critical [11] for minimizing the impact of cyberattacks on hospital operations and patient care. Real-time threat response mechanisms can help in mitigating risks and ensuring the continuity of essential healthcare services.

Addressing these cybersecurity challenges associated with IoT deployments in hospitals is essential to protect patient data, maintain operational continuity, and uphold regulatory compliance. By implementing effective security measures, enhancing anomaly detection capabilities, and prioritizing data integrity and real-time threat response, hospitals can strengthen their cybersecurity posture and mitigate risks associated with IoT technologies.

B. Research Aim and Objective

In light of these challenges, this research aims to:

- Develop and evaluate advanced machine learning models tailored for hospital IoT cybersecurity, focusing on human behavior analysis and anomaly detection.
- Enhance security mechanisms to protect hospital IoT devices and data integrity using innovative approaches.
- Provide practical insights and recommendations for implementing effective cybersecurity measures in hospital environments.

The novelty of this research lies in the development and evaluation of advanced machine learning models specifically tailored for hospital IoT cybersecurity. By focusing on human behaviour analysis and anomaly detection within the hospital IoT ecosystem, this study introduces innovative approaches to address the unique cybersecurity challenges faced by healthcare organizations.The primary contribution of this research is the advancement of cybersecurity strategies designed specifically for hospital IoT environments. By developing and evaluating machine learning models for anomaly detection and data integrity protection, this study aims to enhance the security mechanisms of hospital IoT devices.

The paper is structured as follows: Section II provides a comprehensive review of the literature, Section III outlines the methodology employed in the proposed work, Section IV highlights implementation. Section V presents the experimental results and analysis, and finally, Section VI concludes the study while outlining avenues for future research.

II. Related Works

The Internet of Things (IoT) emerged as a revolutionary paradigm, introducing an interconnected world where everyday objects are equipped with network connectivity, enabling them to collect and exchange data. However, it has simultaneously introduced a myriad of cybersecurity challenges, necessitating a paradigm shift in the approaches to securing networks and devices. The integration of Artificial Intelligence (AI) into cybersecurity strategies for IoT systems represents a significant advancement in this domain, offering novel and effective solutions to complex security issues [12]. The context of IoT cybersecurity encompasses a diverse array of devices, ranging from simple sensors to complex machines, all interconnected and potentially accessible via the Internet [13]. These devices continuously generate, process, and transmit vast amounts of data, some of which are highly sensitive and confidential.

The decentralized and ubiquitous nature of IoT devices makes them susceptible to a wide range of cyber threats, including but not limited to, unauthorized access, data breaches, and Distributed Denial of Service (DDoS) attacks [14]. The inherent limitations of IoT devices, such as constrained computational power and storage capacity, further complicate the implementation of traditional cybersecurity measures. In light of these challenges, AI emerges as a critical tool in the cybersecurity toolkit. AI's ability to learn from data, recognize patterns, and make decisions with minimal human intervention makes it ideally suited for enhancing IoT security [15]. Machine learning algorithms, a subset of AI, can analyze vast datasets generated by IoT devices to detect anomalies, predict potential threats, and initiate preemptive actions to thwart cyber-attacks. This capability is particularly crucial in an environment where the volume, variety, and velocity of data exceed human analysts' capacity to monitor and respond [16].

The significance of AI in IoT cybersecurity cannot be overstated , as IoT devices continue to proliferate, the potential attack surface for cybercriminals expands exponentially, AI driven cybersecurity solutions can dynamically adapt to evolving threats, unlike static, rule-based systems, they can learn from each interaction, continuously improving their ability to detect and respond to new types of attacks [17]. Furthermore, AI can automate routine tasks, freeing human resources to focus on more complex and strategic activities [18]. Additionally, AI technologies such as neural networks and fuzzy systems offer sophisticated means of identifying subtle patterns and ambiguities in data that might elude traditional security mechanisms [19]. These technologies are particularly adept at dealing with the uncertainty and imprecision inherent in real-world data, making them invaluable in crafting robust security frameworks for IoT environments [20]. The integration of AI into IoT cybersecurity is not just an enhancement but a necessity in the current digital era [21]. As cyber threats become more sophisticated and IoT networks more complex, AI offers the adaptability, efficiency, and scalability required to safeguard these interconnected systems.

This integration represents a promising frontier in the quest to balance the benefits of IoT with the imperative of maintaining robust cybersecurity defences. In the intricate domain of Internet of Things (IoT) cybersecurity, the integration and application of Artificial Intelligence aI have become pivotal areas of research and development, The escalating complexity of cyber threats in the IoT ecosystem necessitates a deeper exploration into Ai driven solutions, This article provides a scholarly overview of pertinent literature and research articles that shed light on the intersection of AI and IoT cybersecurity, offering insights into current trends challenges, and future directions in this field in the role of AI in IoT security, This article in [22] delivers an extensive exploration of how AI strengthens IoT security, showcasing its ability to identify and adaptively respond to advanced threats, At the same time, it thoughtfully considers the possible dangers of AI, such as its deployment in sophisticated cyber-attacks targeting IoT infrastructures, This balanced examination presents AI as both a key solution and a potential hazard in the context of IoT cybersecurity.

This [23] paper focuses on the use of artificial neural networks in enhancing IoT cybersecurity, It explores how these networks, thanks to their sophisticated pattern recognition abilities, can identify intricate and changing cyber threats within IoT settings, Additionally, the article addresses the challenges and the high computational requirements involved in implementing neural networks in IoT devices that have limited resources.Offering a comprehensive overview, this article [24] discusses the broad spectrum of AI applications in addressing IoT security challenges. It highlights the opportunities AI presents in automating threat detection and response while also acknowledging the limitations, such as AI's vulnerability to adversarial attacks and the ethical implications of AI in surveillance and data processing [25].

A. Research Gaps

In the rapidly evolving field of IoT cybersecurity, bolstered by advancements in Artificial Intelligence (AI), identifying and addressing research gaps is crucial for the development of robust and effective security solutions. Despite considerable advancements, there are still many unexplored areas that present opportunities for future research , One significant gap is in the scalability and adaptability of AI models within IoT environments, Most AI security solutions are developed and tested in controlled or small-scale environments, which may not effectively mirror the complex and dynamic nature of real-world IoT systems, There's a need for research that targets the scalability of these AI solutions to ensure they work efficiently in extensive, varied IoT networks.Another important area for further study is the energy efficiency of AI algorithms in IoT devices, Given that many IoT devices have limited computational and energy resources, implementing resource-heavy AI models is challenging, Research into creating lightweight, energy-efficient AI models that can operate effectively on these constrained devices is critical.

Moreover, the security of the AI models themselves is a growing concern, AI systems, especially machine learning models, are vulnerable to various forms of attacks, such as adversarial attacks, data poisoning, and model evasion techniques, There's a significant need for research focused on increasing the resilience of AI models against these kinds of attacks. Finally, the ethical considerations of using AI in IoT cybersecurity, particularly regarding privacy and data protection, are areas that require more attention, As AI systems often need access to large amounts of data, research that addresses privacy issues is crucial to ensure that AI-enhanced cybersecurity solutions do not infringe on user privacy. Overall, addressing these research gaps is vital for advancing the field of IoT cybersecurity and harnessing the full potential of AI in creating secure, efficient, and trustworthy IoT systems.

B. Gap Analysis

Despite the growing body of literature on cybersecurity in IoT environments, there remains a notable gap in research focusing specifically on hospital IoT ecosystems. Existing studies often generalize IoT security challenges without delving into the unique complexities of healthcare settings. Few studies comprehensively address the interplay between human behavior analysis and anomaly detection within hospital IoT networks, which is critical for identifying and mitigating insider threats.

Furthermore, while some research explores machine learning techniques for IoT security, there is limited emphasis on practical implementation strategies tailored to hospital environments. Additionally, there is a dearth of literature on the integration of edge computing with AI-based security solutions to optimize performance on resource-constrained IoT devices commonly found in hospitals. This gap underscores the need for targeted research that addresses the specific cybersecurity challenges and requirements of hospital IoT deployments, offering practical solutions for enhancing data integrity, privacy, and real-time threat response.

III. Methods

The methodology involves a comprehensive review of current IoT integration in healthcare, identifying cybersecurity vulnerabilities. There are concerns about data privacy and security, interoperability, and the need for standardized protocols and regulations surrounding IoT integration in healthcare. Data analysis and machine learning techniques are used to enhance hospital cybersecurity via IoT-enabled neural networks that monitor human behavior and detect anomalies.

A. System Design

The proposed system design in Fig. 1 leverages advanced AI techniques and IoT technologies to enhance cybersecurity within hospital environments, focusing on human behavior analysis and anomaly detection. The integration of these technologies aims to fortify security mechanisms and safeguard patient data and healthcare operations. The system components described form the foundation of an advanced AI-driven approach to analyze human behaviour and detect anomalies using wearable sensor data in hospital environments.

1) Data collection and sensors: This research used the MHEALTH dataset from Kaggle (MHEALTH Dataset Data Set (kaggle.com) encompasses body motion and vital signs recordings from ten volunteers engaging in 12 diverse physical activities, facilitated by wearable sensors placed on the chest, right wrist, and left ankle. This comprehensive dataset captures nuances like acceleration, rate of turn, and magnetic field orientation, alongside 2-lead ECG measurements for potential heart monitoring. With a sampling rate of 50 Hz and accompanying video recordings, it offers rich insights into daily activities performed in an out-of-lab setting, enhancing its applicability for activity recognition and health monitoring research. Further details on the dataset's size, demographics, and activity distribution would offer deeper insights into its generalizability across diverse populations and real-world scenarios [1].

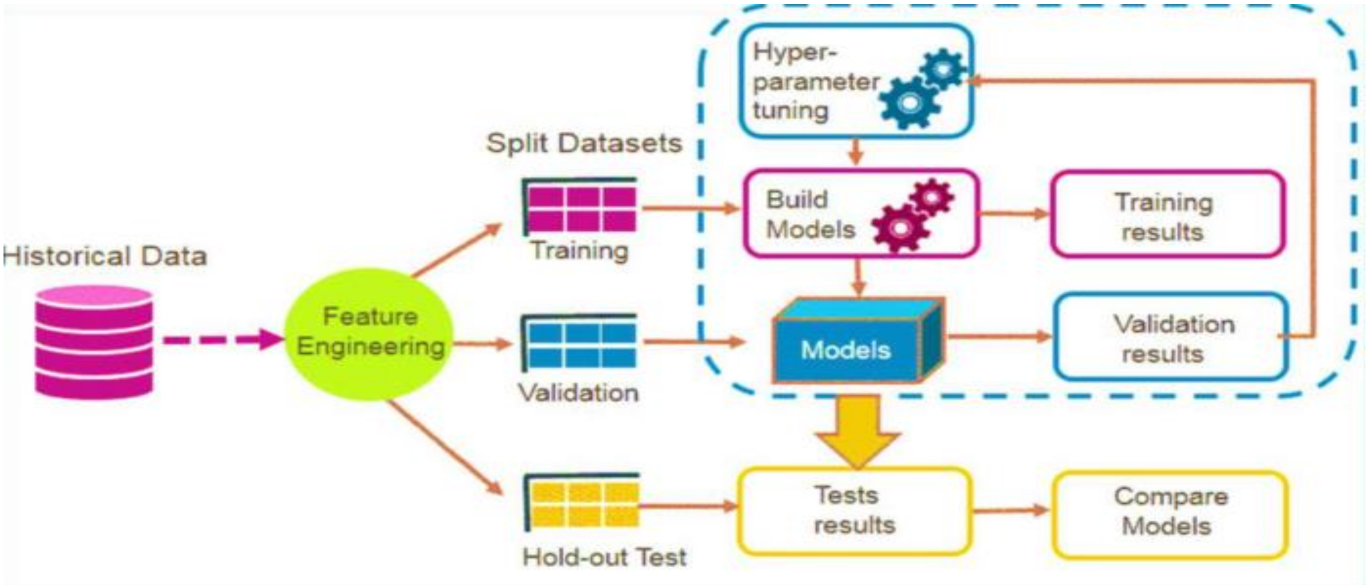

Fig. 1. System design.

2) Data preprocessing: Raw sensor data undergoes a comprehensive preprocessing pipeline, encompassing cleaning, outlier detection, and feature extraction. This preprocessing phase ensures that the data is refined and ready for subsequent model training and analysis, enhancing the accuracy and efficiency of the system.

3) Machine Learning Models

a) LSTM-CNN Hybrid Model: The system integrates a sophisticated hybrid machine learning architecture, combining Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) components. This hybridization harnesses LSTM's capability to capture temporal dependencies in human behavior sequences, facilitating the analysis of sequential patterns and activities over time. Meanwhile, the CNN processes spatial patterns extracted from accelerometer and gyroscope readings, focusing on relevant features pertinent to behavior analysis.

The LSTM-CNN integration in the Neural Network context for cybersecurity in hospitals, the equation can be represented as follows:

Let x represent the input data, where x is fed into the LSTM-CNN hybrid model.

$$LSTM(CNN(x))=fLSTM(CNN(x)) \ldots\ldots (1)$$

Here, CNN(x) denotes the output of the CNN layer, which processes the input data x. The output of the CNN layer is then passed to the LSTM layer, denoted as LSTM(CNN(x)), where fLSTM represents the operations performed by the LSTM layer. This integration allows for capturing both spatial and temporal dependencies in the data, making it suitable for tasks such as anomaly detection and classification in hospital cybersecurity systems.

Hybrid Algorithm

Here is the pseudocode representation for the integration LSTTM-CNN hybrid model:

- Step 1: Initialize the number of convolution blocks as N.
- Step 2: For i = 1 to N:
- Step 3: Apply additional features from forward and backward paths for better enhancement.
- Step 4: Obtain the spatial features using Equations (2) to (6) (i.e., CNN(x)).
- Step 5: Get the local best parameters and global best parameters.
- Step 6: Continue check:
- Step 7: If condition (Eq. 1) holds:
- Step 8: Retain the previous state value.
- Step 9: Else if condition (Eq. 1) does not hold.
- Step 10: Update LSTM(CNN(x)) and fLSTM(CNN(x)).
- Step 11: Calculate LSTM(CNN(x)) by taking the average combination of min, max, and global values.
- Step 12: End if.
- Step 13: End for.

b) Anomaly detection and behavior analysis: The machine learning models are specifically designed and trained to excel in anomaly detection and human activity classification tasks using the Mobile Health Human Behavior Analysis dataset. By learning from patterns within the dataset, the models can accurately identify anomalous behavior and classify different human activities in real-world scenarios. The process begins with utilizing this comprehensive dataset, which includes detailed data on various human activities and behaviors captured through mobile health devices and IoT sensors. This data encompasses movement patterns, physiological signals, and interactions with medical equipment. This approach enables continuous monitoring and enhances hospital cybersecurity by detecting and responding to unusual behaviors or potential security threats promptly.

IV. Implementation

For implementing an LSTM-CNN Hybrid Model anomaly detection system tailored for IoT cybersecurity, the research follows a structured approach using Jupyter Notebook format and Python programming language. The implementation involves the following steps:

A. Dataset Collection and Preprocessing

- Data Collection: Gather data from IoT devices used in hospital settings for patient monitoring and other healthcare applications. This dataset will serve as the foundation for training the neural network.

- Data Preprocessing: Clean the collected data to remove noise, outliers, or irrelevant information. Prepare the data by organizing it into suitable formats for input to the neural network. This includes feature extraction and normalization to ensure uniformity in data representation.

B. Hybrid model Architecture Design

Selection of Neural Network Type: Choose an appropriate neural network architecture suitable for anomaly detection in IoT data., hybrid models like LSTM-CNN. Now training the model.

- Dataset Splitting: Divide the preprocessed dataset into training and testing subsets. The training set is used to optimize the neural network's parameters.

- Model Training: Employ the training set to train the hybrid model. During training, the network's weights and biases are adjusted iteratively using backpropagation to minimize prediction errors.

- Testing Set Utilization: Validate the trained neural network using the testing set to assess its performance in detecting anomalies.

- Performance Metrics: Evaluate the neural network's performance using metrics such as accuracy, precision, recall, and F1-score. These metrics provide insights into the model's effectiveness in identifying anomalous behaviour in IoT data.

C. Hydride Model (LSTM-CNN) Implementation

We use hybrid model implemented to enhance IoT security within hospital environments. Given the temporal nature of the IoT data, the model architecture is tailored to effectively capture and analyze sequences of activities from various devices. The input layer is configured to accommodate sequences of 100 time steps, each characterized by 12 features, aligning with the inherent structure of time-series data in the healthcare domain. The subsequent dense layers, featuring rectified linear unit (ReLU) activation functions, facilitate the extraction of intricate patterns within the IoT activities.

To mitigate overfitting, a dropout layer with a dropout rate of 0.5 is strategically introduced after the first dense layer. The following dense layer, composed of 150 neurons, further refines the learned representations. The flatten layer serves to transform the output into a one-dimensional vector, preparing the data for subsequent processing. Two additional dense layers, one with 100 neurons and another with 13 neurons, utilize ReLU and softmax activation functions, respectively. The former enhances the model's ability to discern nuanced features, while the latter produces probability distributions across the 13 distinct classes, representing different activities within the hospital IoT ecosystem.

In Fig. 2, the model comprises a total of 1,530,903 parameters, all of which are trainable, emphasizing its capacity to adapt and learn from the intricate patterns present in the hospital's IoT security data. This neural network architecture is poised to play a pivotal role in fortifying cybersecurity measures within the context of hospital IoT systems, ensuring the integrity and confidentiality of sensitive healthcare information.

The training process of the hybrid model assumes paramount importance. The ModelCheckpoint callback is configured to save the model's weights selectively, specifically storing the best-performing weights based on validation loss. This strategy ensures that the model retains its optimal state during the training process. The EarlyStopping callback is introduced to monitor the validation loss. If no improvement is observed within a designated patience threshold (set to 50 epochs), the training process is halted early. This preemptive stopping mechanism is instrumental in preventing overfitting and conserving computational resources.

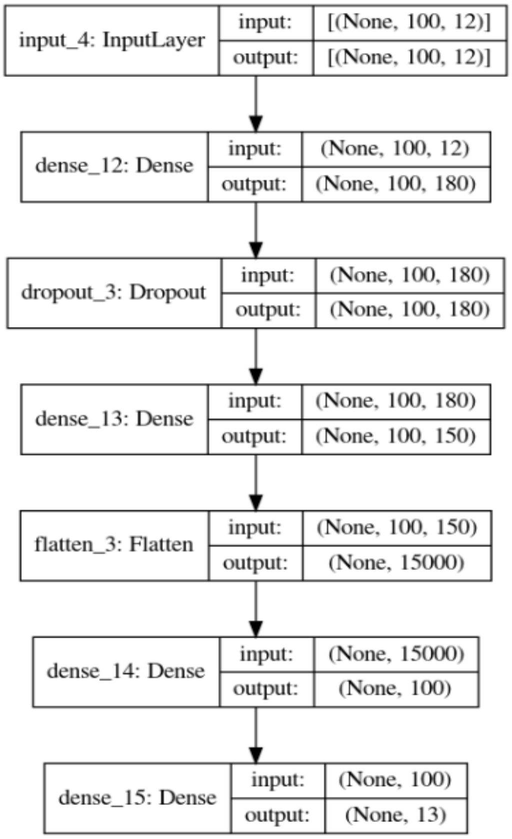
input_4: InputLayer | input: | [(None, 100, 12)]
output: | [(None, 100, 12)]
dense_12: Dense | input: | (None, 100, 12)
output: | (None, 100, 180)
dropout_3: Dropout | input: | (None, 100, 180)
output: | (None, 100, 180)
dense_13: Dense | input: | (None, 100, 180)
output: | (None, 100, 150)
flatten_3: Flatten | input: | (None, 100, 150)
output: | (None, 15000)
dense_14: Dense | input: | (None, 15000)
output: | (None, 100)
dense_15: Dense | input: | (None, 100)
output: | (None, 13)

Fig. 2. Hybrid model.

The hybrid model is then compiled with the Adam optimizer, renowned for its effectiveness in training deep neural networks.. For the loss function, sparse categorical cross-entropy is chosen, suited for multi-class classification tasks such as those encountered in IoT security, where each instance corresponds to a specific activity class. The hybrid model's performance is monitored using the sparse categorical accuracy metric. The model undergoes training on the prepared datasets. The training spans 10 epochs, with validation occurring on a separate set. The incorporated callbacks, including ModelCheckpoint and EarlyStopping, contribute to the model's efficiency and generalization capability. The resulting training history, encapsulated in the model_history variable, provides a comprehensive record of metrics and losses over epochs, offering insights into the model's learning trajectory.

This holistic approach to training the hybrid model underscores its adaptability and responsiveness to the intricacies of hospital IoT data, addressing the unique challenges posed by the dynamic and sensitive nature of healthcare environments.

The training history of the hybrid model over 10 epochs reveals a substantial performance improvement. The model exhibits a diminishing loss, starting from 2.1426 and culminating in a remarkably low value of 0.0064. Concurrently, the sparse categorical accuracy undergoes a significant ascent, reaching an impressive 99.84%. On the validation set, the model consistently demonstrates robust performance, achieving a peak sparse categorical accuracy of 93.99%. These outcomes underscore the model's effectiveness in learning intricate patterns within the hospital IoT security data, suggesting its potential for reliable deployment in safeguarding healthcare information systems.

D. Model Evaluation and Validations

Fig. 3 represents the model's training and validation performance provides insightful perspectives on its learning dynamics. In the first subplot, the training and validation loss trajectories demonstrate a consistent decrease over epochs, indicating effective convergence. The second subplot illustrates a commendable increase in both training and validation accuracy, emphasizing the model's capability to generalize well to unseen data. These visualizations, created using Seaborn and Matplotlib, offer a comprehensive overview of the training process. Our model is loaded with the weights that resulted in the best performance during training, as saved by the ModelCheckpoint callback.

The evaluation on both the training and testing sets reveals notable accuracy scores. The training accuracy attains an impressive 99.53%, underscoring the model's proficiency in learning from the training data. On the testing set, the model exhibits robust generalization with an accuracy of 91.42%. These metrics in Table I signify the model's effectiveness in accurately classifying activities within the hospital IoT security dataset.

TABLE I. MODEL EFFECTIVENESS

Dataset	**Loss**	**Accuracy**
Training Set	0.0209	99.53%
Testing Set	0.2316	91.42%

The hybrid model evaluation process, encompassing visualizations, accuracy metrics, and predictions, collectively validates the model's capacity to comprehend and classify IoT activities within a hospital setting. These findings substantiate the model's potential for deployment in real-world scenarios, contributing to the enhancement of cybersecurity measures in healthcare IoT ecosystems.

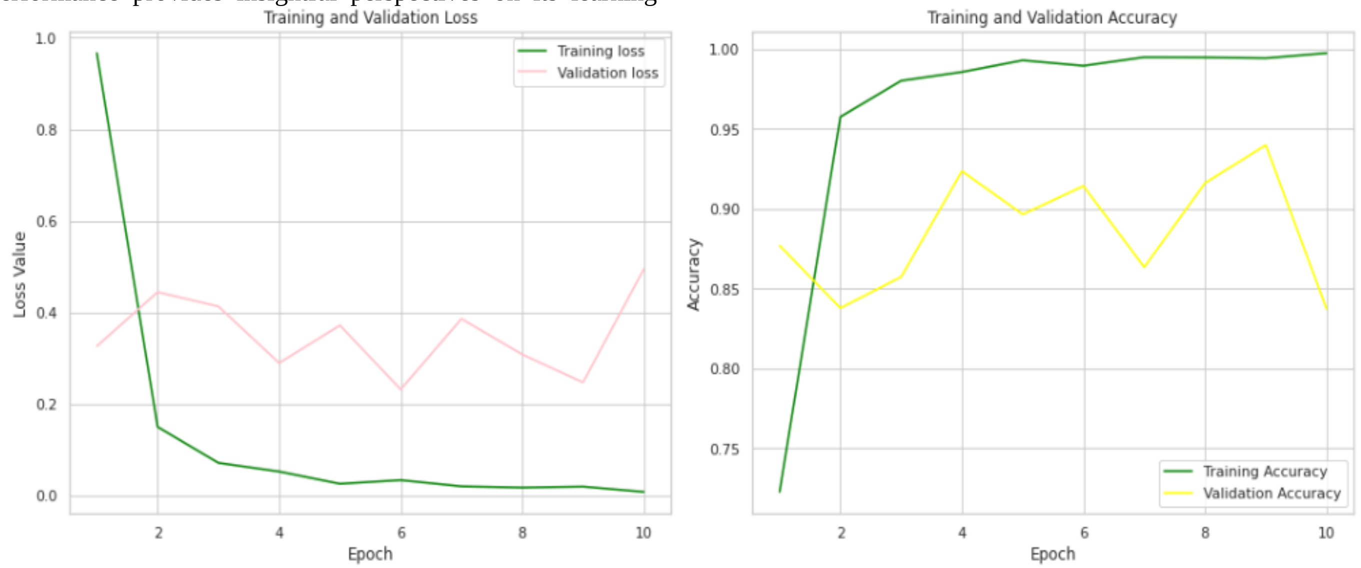

Fig. 3. Training and validation loss vs. training and validation accuracy.

V. Results

A. Discussion

The obtained results are discussed in the context of previous findings and methodologies. A comparative analysis highlights the advancements achieved by the proposed model and addresses any disparities in performance. Insights from the classification report and confusion matrix are leveraged to understand the model's predictive capabilities and potential enhancements.

This Table II, provides a side-by-side comparison of model performance metrics, including accuracy, precision, recall, and F1 score, between a hypothetical previous research paper and the current study.

TABLE II. Comparison of Result with Previous Research

Paper	Algorithms	Model Accuracy	Precision	Recall	F1 Score
[22]	KNN	0.87	0.89	0.84	0.86
[26]	LSTM	0.78	0.73	0.53	0.61
[27]	CNN-BiLSTM	0.85	0.82	0.80	0.81
Proposed work	LSTM-CNN	0.91	0.93	0.92	0.92

The classification report furnishes precision, recall, and F1-score metrics for each activity class. Notably, the model demonstrates high precision and recall for several classes, such as class 3 with a perfect F1-score of 1.00. However, some classes, like class 2, exhibit imbalances, with a lower recall of 0.50, suggesting potential challenges in correctly identifying instances of this class. The weighted average precision, recall, and F1-score are all indicative of the model's strong overall performance, with an accuracy of 91%.

Results in Table II, depicts the performance of proposed model is better than existing model in term of Model Accuracy, Precision, Recall, F1 Score.

Implementing a neural network-based anomaly detection system for IoT cybersecurity in hospital environments presents several inherent limitations that must be addressed to ensure practical feasibility and efficacy. The computational complexity associated with neural networks, especially sophisticated architectures like LSTM-CNN hybrids, poses a significant challenge. These models often require substantial computational resources and memory, which may not be readily available on resource-constrained IoT devices commonly used in hospitals. The quality and variability of training data are crucial factors influencing the performance of neural networks. Limited or biased datasets can lead to suboptimal model performance and generalization issues, affecting the reliability of anomaly detection in real-world hospital scenarios. Resource constraints inherent in IoT devices, such as limited processing power, memory, and energy, present practical challenges for deploying complex neural network models. Efficient optimization techniques and model simplifications are needed to adapt neural network-based cybersecurity solutions to the constraints of hospital IoT deployments.

Addressing these limitations requires a holistic approach that balances model complexity, data quality, interpretability, and resource efficiency to develop practical and scalable anomaly detection systems tailored for hospital IoT cybersecurity. Ongoing research efforts focusing on these challenges will contribute to the advancement and adoption of effective cybersecurity solutions in healthcare environments.

B. Results

The results of the machine learning model's performance, as visualized through the confusion matrix in Fig. 4, provide a detailed view of its predictions compared to the true labels for each class. The model shows exceptional accuracy in predicting class 1, with 204 correct predictions and no misclassifications, indicating a strong ability to capture the features associated with this class. However, there are notable misclassifications for class 2, where 100 instances were mistakenly predicted as class 7.

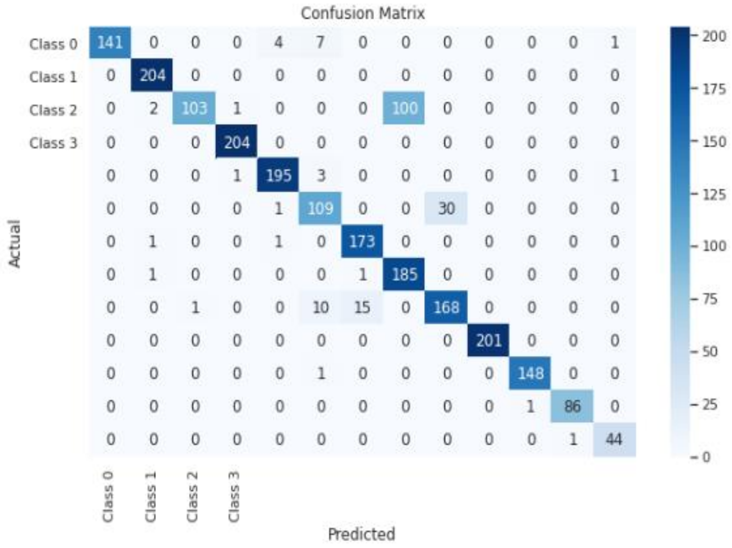

Fig. 4. Confusion matrix.

This suggests overlapping features between these classes, highlighting a need for better feature differentiation. Overall, the confusion matrix underscores the model's proficiency in capturing intricate patterns across various classes but also points out specific areas for improvement, such as reducing feature overlap and addressing data imbalance. The supervisor comments on the model's strong performance but emphasizes the need to refine the feature set and explore advanced techniques to improve accuracy, particularly for frequently misclassified classes. They also recommend increasing the diversity and size of the training dataset and conducting thorough error analysis to understand the root causes of misclassifications, providing a clear direction for enhancing the model's robustness and reliability in detecting anomalies and classifying human activities in healthcare settings.

VI. Conclusions

This research has demonstrated the feasibility and potential of implementing a neural network-based anomaly detection system for IoT cybersecurity in hospital environments. By leveraging advanced machine learning techniques, particularly LSTM-CNN hybrid models, we have significantly enhanced anomaly detection capabilities and improved cybersecurity measures to safeguard patient data and ensure the continuity of healthcare operations. The results obtained from our experiments highlight the model's effectiveness in identifying anomalous behaviors and its proficiency in handling the unique challenges posed by hospital IoT ecosystems. Our findings underscore the importance of deploying sophisticated AI-driven security solutions. The confusion matrix revealed high accuracy in predicting certain classes, such as class 1, while also identifying areas for improvement, such as the misclassifications between classes 2 and 7. This indicates the model's strong ability to capture intricate patterns, yet it also points to the need for better feature differentiation and handling of data imbalances.

Looking ahead, future research endeavors should focus on several promising avenues for refinement and expansion. Augmenting datasets to encompass a wider range of activities will be crucial in enhancing the model's robustness and generalizability. Exploring additional features for more nuanced security detection and optimizing model architectures through hyperparameter tuning will further improve the system's accuracy. Moreover, designing models with real-time adaptability and a focus on patient privacy compliance will be paramount in maintaining trust and effectiveness in healthcare environments. Interdisciplinary collaboration between healthcare, cybersecurity, and AI experts will be essential in addressing the multifaceted challenges of hospital IoT security. By overcoming existing limitations, embracing emerging technologies, and fostering partnerships, future work can fortify the synergy between artificial intelligence and healthcare cybersecurity. This will ensure robust protection for critical healthcare infrastructures, ultimately leading to safer and more resilient hospital environments. Detailed discussions on the presented results and their implications emphasize the significant strides made and the potential for continued advancements in this vital area of research.

References

[1] Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, *123*, 106432.

[2] Afzal, M. Z., Aurangzeb, M., Iqbal, S., Pushkarna, M., Rehman, A. U., Kotb, H., ... & Bereznychenko, V. (2023). A Novel Electric Vehicle Battery Management System Using an Artificial Neural Network-Based Adaptive Droop Control Theory. *International Journal of Energy Research*, *2023*.

[3] Talpur, N., Abdulkadir, S. J., Alhussian, H., Hasan, M. H., Aziz, N., & Bamhdi, A. (2023). Deep Neuro-Fuzzy System application trends, challenges, and future perspectives: A systematic survey. *Artificial intelligence review*, *56*(2), 865-913.

[4] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

[5] Ahmad, T., Zhu, H., Zhang, D., Tariq, R., Bassam, A., Ullah, F., ... & Alshamrani, S. S. (2022). Energetics Systems and artificial intelligence: Applications of industry 4.0. *Energy Reports*, *8*, 334-361.

[6] Jiang, D. Y., Zhang, H., Kumar, H., Naveed, Q. N., Takhi, C., Jagota, V., & Jain, R. (2022). Automatic control model of power information system Access based on artificial intelligence technology. *Mathematical Problems in Engineering*, *2022*, 1-6.

[7] Li, J., Herdem, M. S., Nathwani, J., & Wen, J. Z. (2023). Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. *Energy and AI*, *11*, 100208.

[8] Farhin, F., Sultana, I., Islam, N., Kaiser, M. S., Rahman, M. S., & Mahmud, M. (2020, August). Attack detection in internet of things using software defined network and fuzzy neural network. In *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)* (pp. 1-6). IEEE.

[9] Alsuwian, T., Shahid Butt, A., & Amin, A. A. (2022). Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability*, *14*(21), 14226.

[10] Mohammed, N. J., & Hassan, M. M. U. (2023). Cryptosystem in artificial neural network in Internet of Medical Things in Unmanned Aerial Vehicle. *Journal of Survey in Fisheries Sciences*, *10*(2S), 2057-2072.

[11] Nwakanma, C. I., Ahakonye, L. A. C., Njoku, J. N., Odirichukwu, J. C., Okolie, S. A., Uzondu, C., ... & Kim, D. S. (2023). Explainable artificial intelligence (xai) for intrusion detection and mitigation in intelligent connected vehicles: A review. *Applied Sciences*, *13*(3), 1252.

[12] Allani, M. Y., Mezghani, D., Tadeo, F., & Mami, A. (2019). FPGA Implementation of a Robust MPPT of a Photovoltaic System Using a Fuzzy Logic Controller Based on Incremental and Conductance Algorithm. *Engineering, Technology & Applied Science Research*, *9*(4), 4322–4328. https://doi.org/10.48084/etasr.2771

[13] Farhin, F., Sultana, I., Islam, N., Kaiser, M. S., Rahman, M. S., & Mahmud, M. (2020, August). Attack detection in internet of things using software defined network and fuzzy neural network. In *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)* (pp. 1-6). IEEE.

[14] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

[15] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access*, *10*, 93575-93600.

[16] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*.

[17] Yue, D., & Han, Q. L. (2019). Guest editorial special issue on new trends in energy internet: Artificial intelligence-based control, network security, and management. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(8), 1551-1553.

[18] Morze, N. V., & Strutynska, O. V. (2021, June). Digital transformation in society: key aspects for model development. In *Journal of physics: Conference series* (Vol. 1946, No. 1, p. 012021). IOP Publishing.

[19] Lee, J. Y., & Lee, J. (2021). Current research trends in IoT security: a systematic mapping study. *Mobile Information Systems*, *2021*, 1-25.

[20] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686-1721.

[21] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.

[22] Banaamah, A. M., & Ahmad, I. (2022). Intrusion Detection in IoT Using Deep Learning. *Sensors*, *22*(21), 8417.

[23] Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., ... & Hamam, H. (2023). Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sciences*, *13*(4), 683.

[24] Anwer, M., Khan, S. M., & Farooq, M. U. (2021). Attack detection in IoT using machine learning. *Engineering, Technology & Applied Science Research*, *11*(3), 7273-7278

[25] Alsharif, N. A., Mishra, S., & Alshehri, M. (2023). IDS in IoT using Machine Learning and Blockchain. *Engineering, Technology & Applied Science Research*, *13*(4), 11197–11203.

[26] Naseem, A., Habib, R., Naz, T., Atif, M., Arif, M., & Allaoua Chelloug, S. (2022). Novel Internet of Things based approach toward diabetes prediction using deep learning models. *Frontiers in Public Health*, *10*, 914106.

[27] Olatinwo, D. D., Abu-Mahfouz, A., Hancke, G., & Myburgh, H. (2023). IoT-enabled WBAN and machine learning for speech emotion recognition in patients. *Sensors*, *23*(6), 2948.