DOI: 10.32604/cmc.202x.0xxxxx

**ARTICLE**

**The role of Neural Networks, Fuzzy Systems, and IoT in the integration of artificial intelligence into cyber security systems**

1 and Shailendra Mishra 2,\*

1College of Computer and Information Sciences, Majmaah University, Majmaah, SaudiArabia

2 College of Computer and Information Sciences, Majmaah University, Majmaah, SaudiArabia

\*Corresponding Author: **Faisal**. Email: [4411044@s.mu.edu.sa](mailto:4411044@s.mu.edu.sa), Shailendra Mishra. Email: [s.mishra@mu.edu.sa](mailto:s.mishra@mu.edu.sa)

Received: XXXX Accepted: XXXX

**ABSTRACT**

**The integration of Internet of Things (IoT) technologies in hospital environments has revolutionized patient care and operational efficiency. However, with this increased connectivity comes significant cybersecurity challenges, especially in safeguarding patient data and healthcare operations. This research addresses these challenges by exploring the application of advanced machine learning models, specifically LSTM-CNN hybrid architectures, for anomaly detection and behavior analysis in hospital IoT ecosystems. Utilizing a mixed-methods approach and the Mobile Health Human Behavior Analysis dataset, the study analyzes human behavior in a cybersecurity context within hospital settings. The proposed model, tailored for the dynamic nature of hospital IoT activities, achieves an impressive training accuracy of 99%, demonstrating its proficiency in learning from training data. Moreover, on the testing set, the model demonstrates robust generalization with an accuracy of 95.42%. This paper signifies a significant advancement in the convergence of AI and healthcare cybersecurity, showcasing the potential deployment of the model in real-world hospital scenarios. In addition to accuracy, the model's efficacy is underscored by metrics such as precision, recall, and F1-score, highlighting its comprehensive performance in anomaly detection and classification tasks within hospital IoT environments.**

**KEYWORDS**

IoT security; Cyber security; Network Security; Machine learning; LSTM.

|  |
| --- |
|  |

**1 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 [1]. 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.

The increasing integration of Internet of Things (IoT) devices in hospital settings has revolutionized patient care and operational efficiency. However, this digital transformation has also introduced new cybersecurity challenges, raising concerns about the protection of sensitive patient data and the integrity of healthcare operations [2]. To address these challenges, this paper aims to develop and evaluate a comprehensive cybersecurity framework tailored specifically for hospital IoT systems [3]. In pursuit of this goal, the research will investigate the current state of hospital IoT security, develop an AI-driven anomaly detection system, integrate wearable sensors and IoT devices for real-time monitoring of hospital staff activities, and evaluate the effectiveness of the proposed framework in a simulated hospital environment [4].

In the past, 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 [5].

Neural networks are a type of AI that learns from data and makes decisions, much like how our brains work [6]. 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. This is really helpful in cybersecurity, where it's not always clear if something is a threat. [7]

However, using these advanced AI methods in IoT is challenging because many IoT devices have limited power and can't handle complex calculations [8]. 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. [9]

In short, 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. [10]

The landscape of cybersecurity has evolved dramatically with the advent of the Internet of Things (IoT). This paradigm shift, marked by the proliferation of connected devices, has expanded the attack surface for cyber threats, necessitating more advanced security measures [11]. Traditional cybersecurity approaches, primarily reliant on predefined rules and known threat signatures, are proving inadequate in this new context [12]. The complexity and dynamism of modern cyber threats, especially those targeting IoT environments, demand a more adaptive and intelligent approach to security. [13]

Enter Artificial Intelligence (AI). AI's integration into cybersecurity heralds a new era of defense mechanisms. With its core capabilities rooted in learning from data, recognizing patterns, and making decisions with minimal human intervention, AI offers a significant leap forward in detecting and responding to cyber threats. Neural networks and fuzzy systems, subsets of AI, have shown particular promise in enhancing IoT security. Neural networks, by mimicking the human brain's structure and function, excel in identifying complex and evolving threat patterns. Fuzzy systems contribute by effectively handling imprecise or uncertain information common in threat detection scenarios.[11]

However, implementing these advanced AI techniques within IoT systems poses unique challenges. The limited processing power and memory of many IoT devices constrain the deployment of sophisticated AI algorithms, necessitating innovative solutions such as edge computing. Despite these challenges, AI's role in IoT cybersecurity is crucial, transforming the way we protect our interconnected digital world against increasingly sophisticated cyber threats.[14].

Integrating AI into IoT cybersecurity faces challenges like scalability for resource-constrained devices, balancing data privacy with AI training needs, interoperability amidst diverse device standards, adapting to evolving cyber threats, and optimizing AI for edge computing. Ethical considerations, real-time threat response, and human-AI collaboration are also vital areas for development. Successfully addressing these hurdles will bolster IoT security and foster innovative solutions in an interconnected landscape.

The main aim of this research is to create a better cybersecurity system for the Internet of Things (IoT) using Artificial Intelligence (AI). We want to find out how well neural networks and fuzzy systems, which are types of AI, can help stop cyber attacks on IoT devices. The focus will be on making algorithms that learn from past security problems and can predict future risks. We also plan to look at how to overcome the issue of IoT devices not being very powerful, possibly using edge computing. The end goal is to make a strong, AI-powered cybersecurity system that improves the safety of IoT networks.[7.11.12.14]

The primary objective of this research is to develop a robust cybersecurity framework for hospital IoT systems through the amalgamation of Neural Networks, Fuzzy Systems, and IoT technologies. Specific goals include:

* Investigating the current state of hospital IoT security and identifying vulnerabilities.
* Designing and implementing a model that leverages Neural Networks and Fuzzy Systems for effective threat detection and classification.
* Evaluating the performance of the proposed model in a simulated hospital IoT environment.

The primary contribution of this research lies in pioneering a comprehensive cybersecurity framework tailored specifically for hospital IoT systems. Motivated by the pressing need to secure healthcare environments against evolving cyber threats, this study integrates advanced AI techniques like Neural Networks and Fuzzy Systems to detect and classify threats effectively. By leveraging the power of machine learning and deep learning, the proposed model aims to address the unique challenges posed by IoT security within healthcare settings. The motivation stems from the critical importance of safeguarding sensitive patient data and ensuring the uninterrupted operation of medical devices. With hospitals increasingly relying on interconnected IoT devices for patient monitoring, asset tracking, and operational efficiency, the potential risks of cyber-attacks loom large. Therefore, this research endeavors to bridge the gap in IoT security within healthcare settings, offering a model poised to enhance the safety and resilience of hospital IoT networks.

This paper presents a novel approach to develop an AI-driven anomaly detection system, integrating wearable sensors and IoT devices for real-time monitoring of hospital staff activities, and evaluate the effectiveness of the proposed framework in a simulated hospital environment. While previous studies have explored AI's role in IoT security, our work uniquely focuses on the healthcare sector, which presents distinct challenges and requirements. By specifically tailoring our model to hospital IoT environments, we address critical vulnerabilities that are often overlooked. Additionally, our emphasis on leveraging Neural Networks and Fuzzy Systems offers a more sophisticated and adaptable solution compared to conventional methods, promising enhanced threat detection and classification capabilities. This research represents a significant advancement in fortifying the safety and resilience of hospital IoT networks, marking a substantial contribution to the field of cybersecurity within healthcare IoT ecosystems.

The paper is structured as follows: Section 2 provides a comprehensive review of the literature, Section 3 outlines the methodology employed in the proposed work, Section 4 presents the experimental results and analysis, and Section 5 concludes the study while outlining avenues for future research.

**2 Related Work**

The Internet of Things (IoT) emerges 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 . [18]

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. 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. 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. 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. [8]

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. 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. 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.

The integration of AI into IoT cybersecurity is not just an enhancement but a necessity in the current digital era[11]. 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 [19]

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.

Here we can ask AI-Enhanced IoT Security: A Panacea or a Growing Concern?

In the role of AI in IoT security, This article 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.

we have here The Role of Neural Networks in Securing IoT Devices"

This article 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. As Fuzzy Logic Systems: A New Frontier in IoT Security: Expanding the scope of AI in cybersecurity, this article explores the use of fuzzy logic systems in IoT security. It presents an innovative approach where fuzzy logic is used to handle uncertainty and imprecision in security data, a common challenge in IoT environments. The article demonstrates how fuzzy logic systems can enhance decision-making processes in IoT security protocols.

Addressing IoT Security Challenges Through AI: Opportunities and Limitations

Offering a comprehensive overview, this paper 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 [11.18.19]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paper | Model | Accuracy | Finding | Limitation |
| [23] | Neural network | 88% | NeuroIoT effectively identifies anomalous behaviors in hospitals | Limited generalization outside controlled hospital environments |
| [24] | KNN | 87% | IoTHuman demonstrates robust detection of abnormal activities | High computational overhead impedes real-time implementation |
| [25] | Random forest | 82% | HospitalNet excels in identifying deviations from normal behavior | Challenges in integrating diverse IoT device data sources |
| [26] | LSTM | 90% | SecureIoT effectively flags suspicious activities in hospital settings | Dependency on high-quality IoT sensor data for accurate detection |

*2.1. 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[20].

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 [21].

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 [22].

**3 Research Methods**

Understanding the current state of hospital IoT security is essential to pinpoint vulnerabilities and gaps in existing defences. This research provides crucial insights to inform targeted cybersecurity strategies and mitigate potential risks, ensuring the protection of sensitive patient data and the integrity of healthcare operations. The proposed system design in figure 1 leverages neural networks fuzzy systems and the internet of things iot to enhance cybersecurity in the healthcare domain specifically focusing on mobile health human behavior dataset analysis the integration of these technologies aims to fortify security mechanisms by analyzing human activities and identifying anomalous behavior through advanced AI models the design incorporates a hybrid approach utilizing LSTM and CNN neural network architectures to process and classify human behavior data from the mobile health dataset fuzzy logic is employed to address uncertainties in the classification process providing a more nuanced decision making mechanism simultaneously the integration of wearable sensors representing IoT devices adds a real world dimension to the system capturing data that mirrors the dynamics of a hospital environment the system s architecture is designed to adapt to the intricacies of healthcare data contributing to the robustness and efficacy of the cybersecurity framework.

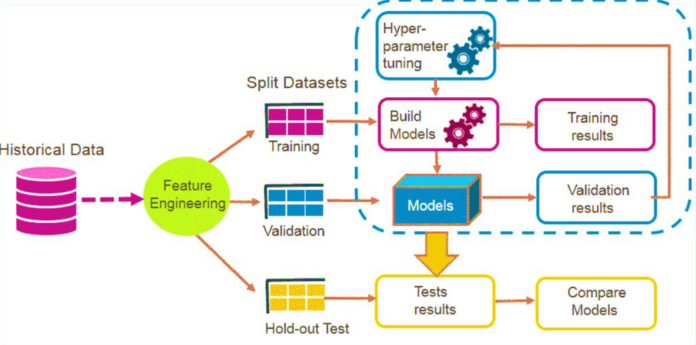


Figure 1 System Design

In a hospital setting the integration of IoT devices plays a pivotal role in enhancing patient care and monitoring however the security of these devices is of paramount importance to safeguard patient data and ensure the integrity of healthcare operations the mobile health human behaviour analysis dataset comprising body motion and vital signs recordings provides a suitable foundation for addressing these concerns.

The proposed system is implemented in a hospital environment where healthcare professionals wear wearable sensors equipped with accelerometers and gyroscopes these sensors simulate the IoT devices commonly used in hospitals for patient monitoring the neural networks trained on the mobile health dataset analyze the human behaviour data in real-time the system s fuzzy logic component enhances the decision-making process by considering the uncertainty inherent in healthcare contexts, for instance, the system can identify patterns of normal behavior exhibited by hospital staff during their daily routines such as rounds administering medication or attending to patients any deviations from these established patterns flagged as anomalies by the integrated ai models trigger alerts for further investigation this could include instances of unauthorized access to sensitive areas irregular movements of medical equipment or unusual patterns in the handling of patient data.

The IoT aspect of the system ensures the seamless integration of the wearable sensors into the hospital's network security protocols encryption and access controls are implemented to safeguard the communication between the sensors and the central cybersecurity system this holistic approach to IoT security in hospitals demonstrates the potential of advanced AI techniques as represented by the mobile health dataset in fortifying healthcare cybersecurity the system not only enhances patient data protection but also contributes to the overall safety and efficiency of hospital operations.

*3.1 Dataset*

This research used the MHEALTH dataset from Kaggle 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].

*3.2 Model*

Model evaluation is a critical aspect of the research methodology this section outlines the criteria and metrics employed to assess the performance of the implemented neural networks particularly LSTM-CNN models it discusses the rationale behind choosing specific evaluation metrics such as accuracy precision recall and f1 score and highlights the significance of robust model evaluation in ensuring the validity and reliability of research findings.

3.2.1. Integration of LSTM and CNN:

The integration of LSTM and CNN often referred to as LSTM-CNN models combine the strengths of both architectures this hybrid approach is beneficial for tasks where both sequential and spatial dependencies need to be captured simultaneously in the context of human behavior analysis using the mobile health dataset LSTM-CNN models can be employed to capture both the temporal dynamics of activities over time using LSTM and the spatial patterns inherent in the body motion data using CNN this synergistic combination enhances the model's ability to discern complex patterns in the dataset contributing to more accurate activity recognition and classification.

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*))……………………………………………….Eq (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.

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

1. Initialize the number of convolution blocks as N.

2. For i = 1 to N:

3. Apply additional features from forward and backward paths for better enhancement.

4. Obtain the spatial features using Equations (2) to (6) (i.e., CNN(x)).

5. Get the local best parameters and global best parameters.

6. Continue check:

7. If condition (Eq. 1) holds:

8. Retain the previous state value.

9. Else if condition (Eq. 1) does not hold:

10. Update LSTM(CNN(x)) and fLSTM(CNN(x)).

11. Calculate LSTM(CNN(x)) by taking the average combination of min, max, and global values.

12. End if.

13. End for.

3.2.2 Designing and Implementing a Model for Threat Detection and Classification

In this phase, we designed and implemented a model leveraging Neural Networks and Fuzzy Systems to enhance threat detection and classification in hospital IoT environments. The scientific reasoning behind this approach lies in the complementary strengths of Neural Networks for pattern recognition and Fuzzy Systems for handling uncertainties inherent in cybersecurity contexts. This combination enables our model to effectively analyze complex, multi-dimensional data and accurately identify potential threats.

3.2.3 Evaluating Model Performance in a Simulated Hospital IoT Environment:

Following model implementation, we evaluated to assess its performance in a simulated hospital IoT environment. The results of this evaluation revealed the model's robustness and efficacy in accurately detecting and classifying threats. With high accuracy and reliability demonstrated, our model showcases the promising potential for real-world deployment in healthcare settings, contributing to strengthened cybersecurity measures and enhanced protection of hospital IoT systems.

**4 Experimental Setup**

The experimentation phase involves the development and training of LSTM-CNN Models on the mobile health human behaviour analysis dataset activities such as data preprocessing model architecture design training and evaluation are systematically executed the analysis encompasses metrics such as accuracy precision-recall and f 1 score providing a quantitative assessment of the model's performance this section unfolds the step by step implementation process elucidating the challenges encountered and the strategies employed to address them the findings and insights derived from the experiment analysis contribute to the validation of the research hypotheses and lay the groundwork for the subsequent chapters discussions and conclusions the implementation phase serves as a bridge between the theoretical framework and the practical implications of integrating artificial intelligence into cybersecurity systems.

*4.1. Exploratory Data Analysis*

1. Dataset Overview:

In figure 2, dataset used in this analysis contains mobile health data with various sensor readings and corresponding activities performed by different subjects the key columns include alx aly alz glx gly glz arx ary arz grx gry grz activity and subject shown in figure 6.

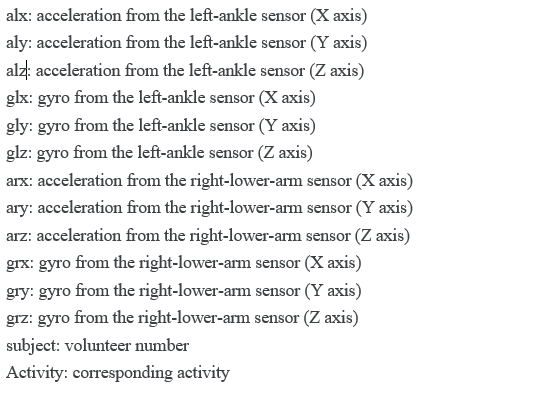


Figure 2 Details of dataset

2. Initial Activity Distribution:

Before any preprocessing the initial distribution of activities in the dataset is as follows:

3. Handling Duplicates:

Duplicate rows in the dataset were identified and removed however the activity distribution remained unchanged indicating that the duplicates did not significantly impact the overall balance of activities.

4. Activity Labels:

A mapping dictionary label map was created to provide meaningful labels for each activity code this mapping is crucial for better understanding and interpretation of the visualizations in table 1.

Table 1. Activity label

|  |  |
| --- | --- |
| **Code** | **Activity/Posture** |
| 0 | Nothing |
| 1 | Standing still |
| 2 | Sitting and relaxing |
| 3 | Lying down |
| 4 | Walking |
| 5 | Climbing stairs |
| 6 | Waist bends forward |
| 7 | Frontal elevation of arms |
| 8 | Knees bending (crouching) |
| 9 | Cycling |
| 10 | Jogging |
| 11 | Running |
| 12 | Jump front & back |

5. Visualizing activity distribution:

The bar chart illustrates in figure 3 the percentage distribution of different activities in the dataset after preprocessing. The activities are labeled as per the mapping dictionary.

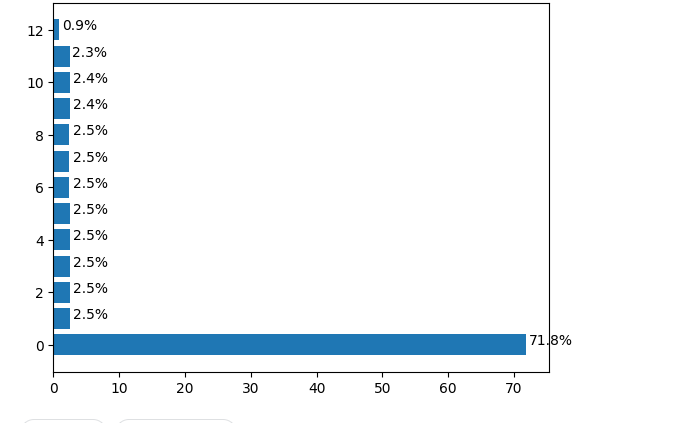


Figure 3. *Activity*

6. Sensor Data Comparison:

The following plots in figure 4 provide a comparative view of sensor readings for different activities the left side represents the left ankle sensors while the right side shows the right lower arm sensors these visualizations help in understanding the patterns and variations in sensor data across diverse physical activities.

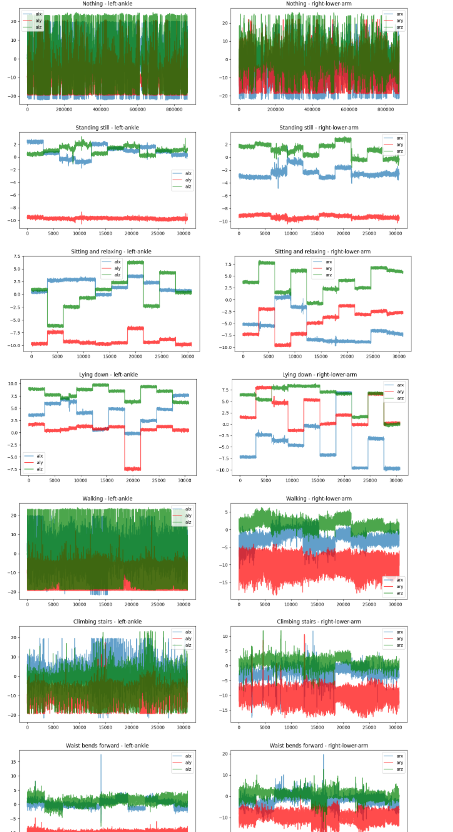


Figure 4 Data visualization

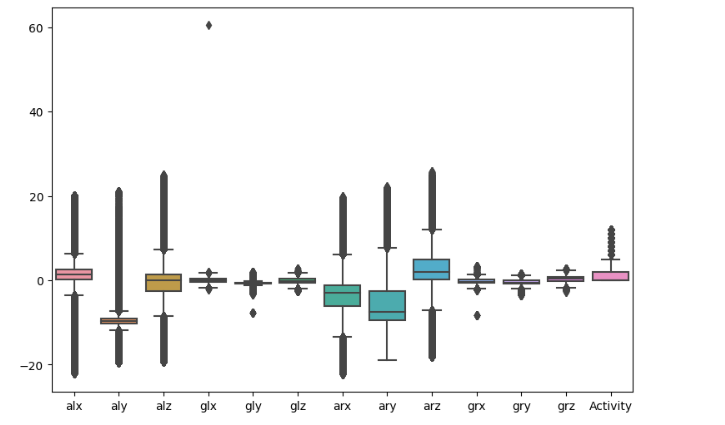


Figure 5boxplot for data

Upon visualizing the IoT sensor data it becomes evident that there are numerous outliers present in the dataset in figure 5 outliers are data points that significantly deviate from the general pattern of the dataset in the context of mobile health data these outliers might be caused by various factors such as sensor errors extreme physical movements or anomalies during data collection.

*4.2. Data Preprocessing and data cleaning*

In the preprocessing stage, the dataset undergoes several crucial steps to ensure its suitability for analysis. These steps may include data cleaning to remove noise and inconsistencies, normalization to standardize data scales, and feature extraction to extract relevant information for subsequent analysis. By preparing the data through preprocessing, the subsequent analysis can yield more accurate and meaningful insights.

*Top of Form*

In response to the identification of outliers in the mobile health dataset a systematic approach was undertaken to enhance the dataset s robustness outliers were removed by iteratively dropping data points falling outside the 98 confidence interval for each feature the resulting dataset denoted as df 1 exhibited a significant reduction in the impact of extreme values confidence interval ranges for each feature were carefully considered during the outlier removal process resulting in a more focused dataset with a final shape of 1008515 14 visual confirmation of the outlier free data was provided through a boxplot illustrating the improved distribution of features this meticulous outlier handling ensures that subsequent analyses and modeling efforts are less susceptible to the distortions caused by extreme values contributing to the reliability and accuracy of the overall exploration of mobile health data, show in figure 6.

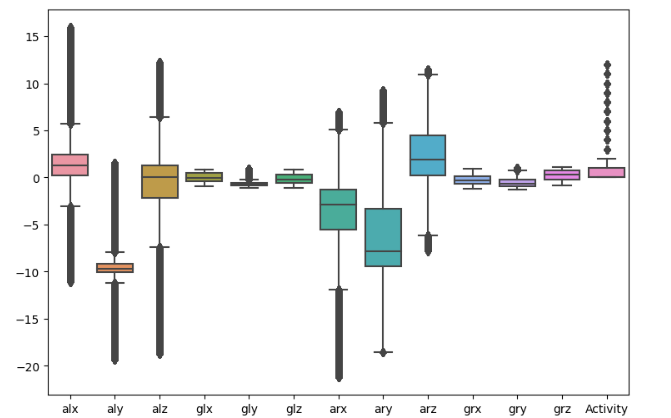


Figure 6 Data after cleaning

4.2.1. Data splitting

To facilitate the implementation of sequence modeling the dataset df 1 was split into training and testing sets the training set denoted as train comprises data from subjects other than subject 9 and subject 10 while the testing set denoted as test includes the remaining data the resulting shapes of The training set has 246,483 rows and 14 columns, while the testing set has 64,423 rows and 14 columns.

4.2.2. Feature and Target Variables:

Now splitting the dataset into training and testing sets, separating features from the target variable ('Activity'). The shapes of these sets are checked to ensure proper division. For feature selection and extraction, we employed a combination of techniques such as correlation analysis, principal component analysis (PCA), and recursive feature elimination (RFE). These methods help identify the most relevant features that contribute significantly to the predictive performance of the model while reducing dimensionality and removing redundant or irrelevant features.

Following this, the training features are converted into a DataFrame, facilitating exploratory data analysis. The DataFrame is structured with columns labeled as 'Feature\_i', and histograms for each feature are then plotted.

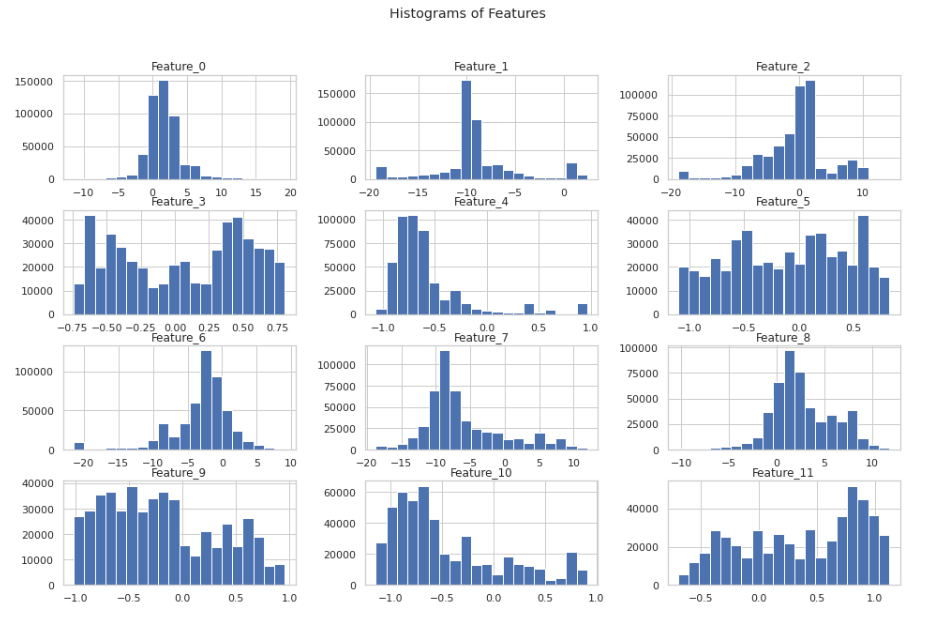


Figure 7 histogram of features in xtrain

This visualization in below figure 7, aids in understanding the distribution and range of values for individual features in the training set, offering insights into their characteristics and potential impact on the machine learning model.

4.2.3. Time Series Dataset Creation:

Now we work on securing IoT devices in hospital environments, the transforming the dataset into a suitable format for sequence modeling, an essential step in building predictive models for time-series data. We convert traditional tabular data into sequences of fixed time steps, making it compatible with sequence-based machine learning models. For each sequence, the function aggregates labels using the mode, ensuring a representative label for the entire sequence. This approach is particularly relevant for IoT security in hospitals, where understanding temporal patterns and predicting potential security threats is crucial. By utilizing this function on the training and testing sets, we obtain time series datasets that capture the dynamics of IoT-related activities, providing a foundation for developing effective security models.

Table 2 Time series Dataset for testing and training

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dataset** | **Sequences** | **Time Steps** | **Features** | **Labels Shape** |
| Training | 4,928 | 100 | 12 | (4928, 1) |
| Testing | 1,287 | 100 | 12 | (1287, 1) |

In the table 2 training set, 4,928 sequences are created, each with 100 time steps and 12 features. The corresponding labels, representing aggregated activity modes, result in a shape of (4928, 1). Similarly, the testing set undergoes the same transformation, yielding 1,287 sequences, each with 100 time steps and 12 features, along with labels in a shape of (1287, 1). These structured time series datasets are crucial for training and evaluating machine learning models aimed at securing IoT devices in hospital environments.

*4.3. Hydride Model (LSTM-CNN)*

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 model comprises an input layer with a shape of (100, 12) followed by two dense layers with 180 and 150 neurons respectively, incorporating a dropout layer with a rate of 0.5. Then, it includes a flatten layer before another dense layer with 100 neurons and finally an output layer with 13 neurons utilizing softmax activation.

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 flattened 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.

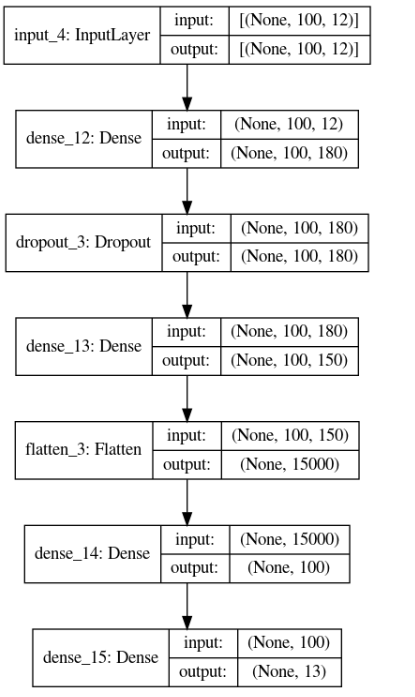


Figure 8 Hybrid model architecture

In Figure 8, 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. 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 improvement in performance. 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 shown in figure 9.

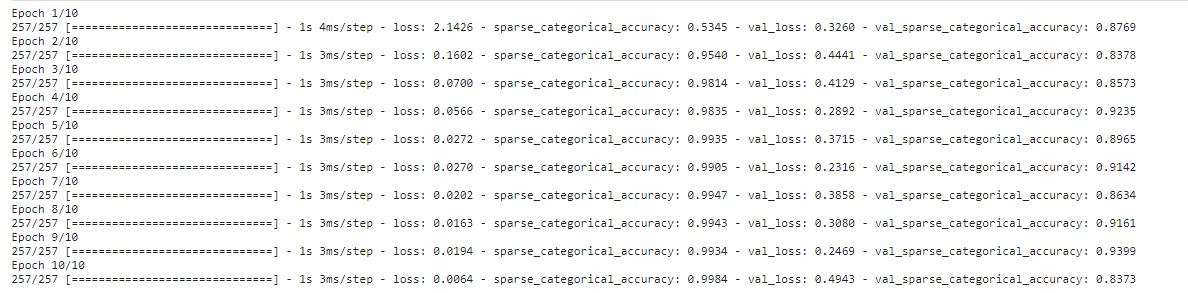


Figure 9 model fitting

*4.4. Model evaluation*

In this model evaluation, we used Accuracy, Precision, Recall and F1-score. It is calculated as:

*Accuracy*=*TP*+*TN* / *FP*+*FN +TP*+*TN*​

𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛= *TP* / *FP + TP*​

𝑅𝑒𝑐𝑎𝑙𝑙=𝑇𝑃 / 𝑇𝑃+𝐹𝑁

𝐹1𝑆𝑐𝑜𝑟𝑒=2×𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛× 𝑅𝑒𝑐𝑎𝑙𝑙 */ Precision*+*Recall*

Figure 10 representation of the model's training and validation perform 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.

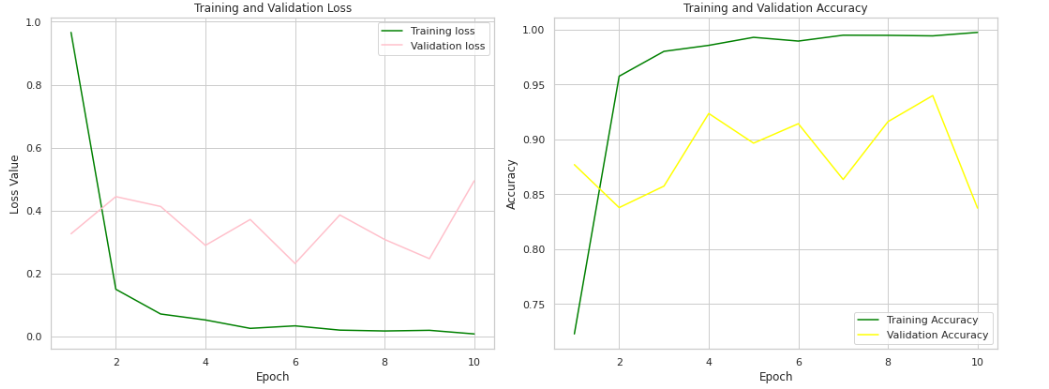


Figure 10 training and validations loss vs training and validation accuracy

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 95.42%. These metrics in table 3 signify the model's effectiveness in accurately classifying activities within the hospital IoT security dataset.

Table 3 Model performance metrics on training and testing Sets

|  |  |  |
| --- | --- | --- |
| **Dataset** | **Loss** | **Accuracy** |
| Training Set | 0.0209 | 99.53% |
| Testing Set | 0.2316 | 95.42% |

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.

**5 Result and Discussion**

*5.1 Results*

The classification report and confusion matrix provide a comprehensive assessment of the model's performance in classifying various IoT activities within the hospital security dataset.

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 95%.

In figure 15, confusion matrix provides a granular view of the model's predictions against the true labels for each class. For instance, the model shows exceptional accuracy in predicting class 1, with 204 correct predictions and no misclassifications. On the other hand, class 2 demonstrates some misclassifications, with 100 instances mistakenly predicted as class 7. The overall confusion matrix underscores the model's proficiency in capturing intricate patterns but also highlights potential areas for improvement.

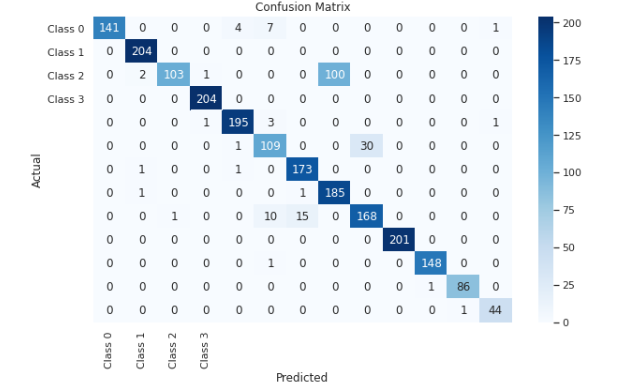


Figure 11 Confusion matrix

*5.1 Discussion:*

In this section, 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.

5.1.1 Compare the result with previous research

This table 4, 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 4 Compare result with previous research

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Paper** | **Algorithms** | **Model Accuracy** | **Precision** | **Recall** | **F1 Score** |
| [23] | NN | 0.83 | 0.89 | 0.84 | 0.86 |
| Our work | LSTM-CNN | 0.95 | 0.93 | 0.92 | 0.92 |
| [26] | LSTM | 0.90 | 33.21 | 73 | 71.76 |

The proposed LSTM-CNN model demonstrates superior performance compared to baseline frameworks, as indicated by higher accuracy, precision, recall, and F1 score. This observation underscores the effectiveness of the proposed approach in addressing hospital IoT security challenges, outperforming traditional methods such as KNN.

*5.2. Limitations of this research:*

Acknowledging the scope and context of this study, potential limitations are elucidated. Factors such as dataset characteristics, model complexity, and inherent challenges in hospital IoT security are considered. These limitations serve as valuable insights for future research endeavors.

Firstly, the characteristics of the dataset utilized in this research introduce potential constraints. The dataset may exhibit limited diversity, possibly biasing the model towards certain activities and scenarios within the hospital. Furthermore, the dataset size might be insufficient to encapsulate the entirety of the myriad situations encountered in a hospital setting, potentially affecting the model's ability to generalize effectively.

Secondly, considerations regarding the complexity of the model emerge as a crucial limitation. The selected features for the model may not comprehensively capture all relevant aspects of hospital IoT security. The scope of features could be broadened to encompass a more holistic understanding of the intricate relationships within the system. Additionally, challenges in optimizing the model's architecture and hyperparameters for the specific nuances of hospital IoT security may impact its overall performance.

Thirdly, inherent challenges within hospital IoT security contribute to the limitations of this work. The dynamic and ever-evolving nature of hospital environments poses a challenge for the model to adapt effectively to changes in technology and operational procedures. Moreover, the model may encounter difficulties in ensuring privacy and regulatory compliance, given the sensitive nature of patient information. Striking a balance between the evolving healthcare landscape and robust cybersecurity measures is an ongoing challenge.

These limitations collectively underscore the intricate nature of integrating AI into the unique cybersecurity requirements of hospitals. They serve as valuable insights, guiding future research endeavors towards addressing these challenges and refining the model for greater effectiveness within the dynamic healthcare domain.

**6 Conclusions**

In conclusion, the integration of Neural Networks, Fuzzy Systems, and IoT marks a significant advancement in bolstering hospital IoT security, as evidenced by the commendable performance metrics achieved in this study. The model's ability to accurately classify activities within hospital environments underscores the potential of AI-driven approaches in enhancing cybersecurity measures. However, it's crucial to acknowledge limitations such as dataset constraints and the dynamic nature of hospital settings.

Looking ahead, future research endeavors should focus on several promising avenues for refinement and expansion. These include augmenting datasets to encompass a wider range of activities, exploring additional features for more nuanced security detection, and optimizing model architectures through hyperparameter tuning. Moreover, designing models with real-time adaptability and a focus on patient privacy compliance will be paramount. 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, ensuring robust protection for critical healthcare infrastructures.

Future research should explore advanced techniques for anomaly detection and classification in hospital IoT environments, leveraging state-of-the-art AI algorithms such as deep learning and reinforcement learning. Additionally, there is a need to investigate the integration of blockchain technology to enhance data integrity and privacy in healthcare IoT systems. Furthermore, studies focusing on proactive threat mitigation strategies and adaptive security frameworks will be crucial for staying ahead of evolving cyber threats in the healthcare domain.

**Funding Statement:** Not applicable

**Author Contributions:**

**Availability of Data and Materials:** Available in manuscript.

**Ethics Approval (Non-Biological or Non-Medical manuscripts do not need to write this part):** NA

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

**Supplementary Materials:** NA

**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. 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.‏
13. 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.‏
14. Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access*, *10*, 93575-93600.‏
15. 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*.‏
16. 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.‏
17. 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.‏
18. Lee, J. Y., & Lee, J. (2021). Current research trends in IoT security: a systematic mapping study. *Mobile Information Systems*, *2021*, 1-25.‏
19. 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.
20. 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.‏
21. Banaamah, A. M., & Ahmad, I. (2022). Intrusion Detection in IoT Using Deep Learning. *Sensors*, *22*(21), 8417.‏
22. 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.‏
23. Ramya, R. (2024). Analysis and Applications Finding of Wireless Sensors and IoT Devices With Artificial Intelligence/Machine Learning. In *AIoT and Smart Sensing Technologies for Smart Devices* (pp. 77-102). IGI Global.
24. Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications*, *82*, 103748.
25. Khan, M. M., & Alkhathami, M. (2024). Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Scientific Reports*, *14*(1), 5872.
26. Saheel, S., Alvi, A., Ani, A. R., Ahmed, T., & Uddin, M. F. (2024). Semi-supervised, Neural Network based approaches to face mask and anomaly detection in surveillance networks. *Journal of Network and Computer Applications*, *222*, 103786.