International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume 14 Issue 02 Year 2022 Page 222:233

Cyber Physical System Based Smart Healthcare System with Federated Deep Learning Architectures with Data Analytics

Dadang Hermawan[1*], Ni Made Dewi Kansa Putri[2] and Lucky Kartanto[3]

[1,2]Institut Teknologi Dan Bisnis STIKOM Bali, Indonesia
[3]Universitas Widya Kartika, Indonesia
[1]dh6996301@gmail.com, [2]nimadewi@outlook.com, [3]luckykartantol@gmail.com
https://orcid.org/0000-0002-9935-8090, https://orcid.org/0000-0001-6888-7216
https://orcid.org/0000-0001-7809-3866
[*]Corresponding Author: Dadang Hermawan

Article History

Received: 24 June 2022
Revised: 28 July 2022
Accepted: 22 August 2022

Abstract

Data shared between hospitals and patients using mobile and wearable Internet of Medical Things (IoMT) devices raises privacy concerns due to the methods used in training. the development of the Internet of Medical Things (IoMT) and related technologies and the most current advances in these areas The Internet of Medical Things and other recent technological advancements have transformed the traditional healthcare system into a smart one. improvement in computing power and the spread of information have transformed the healthcare system into a high-tech, data-driven operation. On the other hand, mobile and wearable IoMT devices present privacy concerns regarding the data transmitted between hospitals and end users because of the way in which artificial intelligence is trained (AI-centralized). In terms of machine learning (AI-centralized). Devices connected to the IoMT network transmit highly confidential information that could be intercepted by adversaries. Due to the portability of electronic health record data for clinical research made possible by medical cyber-physical systems, the rate at which new scientific discoveries can be made has increased. While AI helps improve medical informatics, the current methods of centralised data training and insecure data storage management risk exposing private medical information to unapproved foreign organisations. New avenues for protecting users' privacy in IoMT without requiring access to their data have been opened by the federated learning (FL) distributive AI paradigm. FL safeguards user privacy by concealing all but gradients during training. DeepFed is a novel Federated Deep Learning approach presented in this research for the purpose of detecting cyber threats to intelligent healthcare CPSs.

Keywords: Cyber-physical system; Internet of Medical Things; remote health monitoring; Deep learning

1. Introduction

The Internet of Medical Things (IoMT) has improved human well-being and quality of life by improving healthcare management, oversight, and procedure [1]. This has resulted in healthcare systems that are more personalised, user-centric, precise, and ubiquitous in nature. Internet of Medical Things (IoMT) devices are commonly utilised for continuous monitoring of healthcare traffic as part of the smart healthcare system. Using an AI-enabled framework, a variety of cutting-edge intelligent healthcare solutions are becoming a reality, including disease prediction and remote health monitoring [2]. Applications like holographic communication, telesurgery, H2H, and QoL services will form the foundation of future healthcare systems. Particularly demanding will be the real-time and granularity of performance needed for telesurgery and holographic communication. Existing wireless designs like 5G are unable to accommodate intelligent healthcare applications because of poor data rates. There is high anticipation that the 6G will play a decisive role in removing the communication constraints of the current wireless architecture and so radically improving the current healthcare system.

Methods for managing the flow of patients in and out of healthcare facilities have traditionally employed a centralised artificial intelligence framework on the cloud or a data centre. As a result of the proliferation of IoMT devices and the large amount of health communications, concerns about the scalability [3] of modern smart healthcare systems' centralised architecture are emerging. Furthermore, patients' safety and privacy are seriously threatened because data learning systems rely heavily on centralised servers, which are themselves vulnerable to a wide range of security flaws. Intruders and adversaries, for example, can compromise IoMT devices in order to change the patient's stored data, which could have fatal consequences. Furthermore, the health traffic distribution across diverse and extensive healthcare systems may make the centralised AI architecture for future adaptive healthcare systems unworkable. A decentralised AI-based platform that supports scalable and privacy-preserving healthcare applications is necessary for the successful implementation of intelligent healthcare systems.

Cyber-physical systems (CPSs) include things like autonomous transportation networks, smart grids, and gas pipeline networks in an industrial setting and are sometimes referred to as complex, large-scale, heterogeneous Internet-of-Things and geographically-dispersed, ([4]. Together with pre-existing industrial control systems (ICS) and AI, industrial CPSs are encased in intelligent networking and computing technologies such as cloud computing, network function virtualization, 5G (and beyond), and software-defined networking (SDN) (AI). It is expected that industrial CPSs will facilitate improved network resource allocation [5], greater remote access, the promotion of intelligent services, the facilitation of big data analytics, and the enabling of big data analytics.

There is little doubt about the benefits of industrial CPSs, but the advances made in this area have not been without risk. Inadequate precautions have been taken for the safety of existing industrial infrastructures, leaving them open to several threats. The fast convergence of modern networking and computing technologies has generated new vulnerability that may be leveraged throughout software-based terminals, networks, applications, and the cloud, significantly expanding the threat environment. More than 30 power substations in Ukraine were knocked offline by the Black Energy malware-based cyber-attack in December 2015, leaving about 230 thousand people without electricity for one to six hours. Stuxnet, which attacked Iran's nuclear power plant, VPN Filter, which attacked supervisory control and data acquisition (SCADA) protocols, and unauthorised entry at Australia's Maroochy sewage facility are all examples of industrial CPS cyber events. These incidents provide evidence that state-sponsored or affiliated actors will continue to focus on industrial CPSs soon. According to the 2016 ICS-CERT Annual Assessment Report from the U.S. Department of Homeland Security, "rapid increases in the connectivity of operational technology through the Internet of Things raise new challenges for control system security," and "cybersecurity is essential to the safe and reliable operation of control systems," according to the NIST Guide to ICS security from the U.S. Department of Commerce. [6]

In recent years, cutting-edge research has focused on AI-related intrusion detection methods to address industrial CPS-related cybersecurity challenges. Qiu et al. [7] established a deep Q-learning-based solution for reducing cyber-risks in software-defined industrial IoT connections in 2019. Ismail et al. [8] investigated electricity theft attacks in smart grid CPSs and created a deep learning-based intrusion detection solution to detect such breaches by the beginning of 2020.

In order to detect a wide range of cyber threats against industrial CPSs, we develop a novel deep learning model based on convolutional neural networks (CNNs) and gated recurrent units (GRUs). In addition, we create a new federated learning architecture that protects the privacy of many individual owners while they collaborate on a unified intrusion detection model for industrial CPSs. We further protect the model's parameters during training by creating a secure data transmission protocol based on Paillier.

What follows is a brief outline of how the rest of the article is structured. Section 2 provides a thorough analysis of relevant literature. Section 3 provides an overview of the Federated Deep Learning technique's proposed framework, as well as a description of its primary components and features. In Section 4, we reveal the results of a thorough performance investigation of the Federated Deep Learning approach framework, and we compare these findings to those of previous relevant research. Finally, the article finishes with a section that outlines the way forward for this type of research.

2. Literature Survey

Xu et al. (Lee et al., 2020) [9] created a Certificate less Signature Scheme (CLS) for the medical cyber-physical system that is based on the NTRU lattice. As a result of its usage of tiny integer solutions on NTRU grids, the latter has been shown to be secure against quantum attacks. Based on security studies and performance evaluations, our proposed method provides quantum attack resilience at significantly reduced coordination and measurement costs compared to two leading quantum resiliency systems. However, once quantum computers are widely available, strategies for quantum survival will need to be formulated.

Kumar et al. [10] provide a method for data normalisation that takes into consideration the heterogeneity of the data, which is produced by the data being collected from several institutions using various computed tomography (CT) scanners. The data was heterogeneous since it was acquired from a number of institutions using a range of computed tomography (CT) scanners.

Using a variety of network traffic features and an improved Adaboost algorithm, Dan Tang and co-workers (Tang et al. 2020) [11] proposed a method for detecting LDoS assaults. (MF-Adaboost). In order to collect data on network traffic and quantify various components, they design a network feature collection. The computing function will prioritise the most important data in network traffic in order to lower the total quantity of data transmitted over the network. The list of components is used to fine-tune the detection algorithm's training process and choose the most relevant classification features. The Adaboost method, a machine learning classification strategy, is used in this approach. Their findings suggest that their system is able to detect LDoS attacks.

Mcghin et al. [12] propose introducing federated learning into the technique of attaining consensus on the block chain network as part of the process. This would be done as a part of the procedure. Because of this, it will be feasible to use the computer labour that is required to reach consensus for federated training as well, which will save both time and money. Federated training will be possible as a result of this.

The investigation that Pokhrel et al. conducted out [13]. The findings of this study demonstrate that different healthcare applications each have their own set of needs, the majority of which are currently not being addressed by a significant proportion of the block chain experiments being studied as part of this study. In addition to that, this study presents an overview of a variety of possible paths of inquiry for research soon.

Lu et al. [14] It has been hypothesised that the distributed ledger technology, could be used as the foundational architecture for a platform that would enable many users to communicate data with one another in a secure manner. This is because block chain is often referred to as the "technology behind bitcoin." The problem of data sharing was turned into a challenge for machine learning after certain aspects of functional logic and safety were incorporated into the equation.

3. Proposed System

Many scholars have studied the literature on IoT security and privacy during the past ten years. [15] Although security concerns have received most of the attention, end-user privacy must also be protected in the present electronic health care systems [16]. By embracing cutting-edge digital technologies like IoT, high-performance computing devices for data storage and analysis, personal health records and more, the modern health-care system has developed into a new field. By using these more effective countermeasures, IoMT has been shown to increase the effectiveness of the healthcare system [17].

Despite these positives, healthcare cybersecurity is still an urgent issue that must be addressed [18]. Unfortunately, cybercriminals regard vulnerable electronic healthcare systems as an easy target due to inadequate information security protection capabilities. If a hacker gains access, they may employ ransomware to cripple the system, steal sensitive medical records to resell, or even extort users for financial gain. Furthermore, it has been shown that the computerised healthcare system has a higher prevalence of attack-able vulnerability spots. One such case of an attacker intercepting an automated insulin pump's operation is [19]. When the security operator looked at the communication protocols, they found this attack. As a result, it is obvious that the risk of the system must be evaluated before adding any security or privacy measures. Modern healthcare systems will now face a serious danger from security and privacy issues, which must be resolved for IoMT systems to work properly. In order to meet future demands, the secure network must also be able to adjust to changes in the healthcare system and meet all system requirements while being limited.

3.1. In IOMT, Privacy Is Important.

In today's world, protecting the network is only half the battle. It is very important for electronic healthcare systems to have their network privacy protected. Here, we'll present a high-level summary of privacy issues and the effective security measures that have been established as a result.

3.1.1. Personal Information:

Large amounts of data are exchanged between multiple networked operating systems in IoMT-based apps, which raises privacy problems. ISO/IEC 27018 and 29100 [20] are only two examples of the many standard protocols developed to address these issues. Information that can be used to identify an individual is called "personally identifiable information" (PII). Currently, user data can be broken down into three broad categories: extremely confidential, general, and aggregate. Sensitive personal information, as its name implies, requires a higher level of privacy protection than generic and statistical data, the likes of which are typically used for surveys and statistical research.

The individual who has full ownership and control over the information is known as the PII owner. On the other hand, a PII associated processor is a business that has been given consent by the person to access and use their personal data for several purposes. However, with the owner's permission, the processor may disclose the data to a third party for some specialised purposes. The contractual processor and third party will both be held accountable if a violation involves the unauthorised use of personal data.

3.2 A Florida-Based Healthcare System's Framework

Incorporating FL into a variety of different architectures is depicted in Figure 1. The generic healthcare system with FL assistance comprises a lot of stages. When designing a healthcare system, the central server must first make several decisions, including which algorithm to use for prediction or classification and which task to perform—which may be medical image processing or some other application requiring human intervention. Also selected are the learning rates and several adjustable ML-related factors.

The central server also chooses which clients will take part in the FL procedure. Once the central server has agreed on the total number of end nodes that will take part in FL, the first models will be delivered to each of those nodes. Model updates are then sent to a centralised repository for aggregation. To this end, the last nodes take data from their immediate surroundings and use it to hone the model. A federated average model, for instance, can be used to assign different values to local model parameters depending on the sample sizes that are available. The modified global model is then sent to the terminal nodes. The desired degree of precision is obtained by a process of iterative and constant learning.

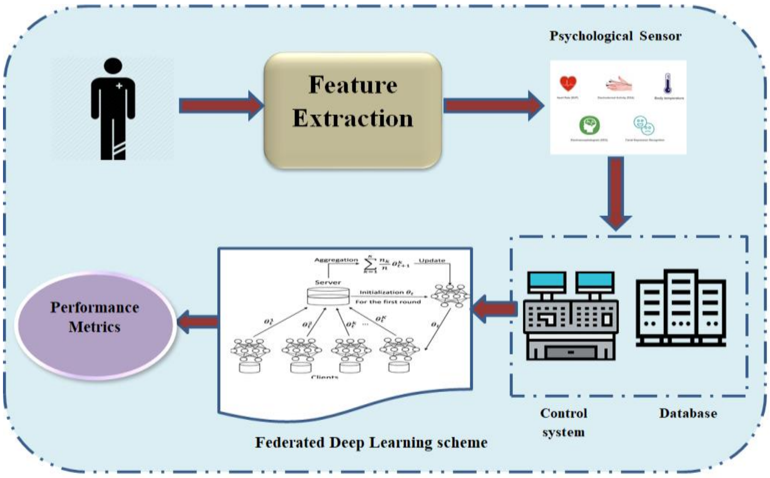

Figure 1: Proposed diagram of Federated Deep Learning scheme method

3.3 Federated Learning: Key Design Aspects

The following changes can be made to the federated machine learning formula

$$\arg_v \min L(p,q,v) = \sum_k p_k L_k(p,q,v) \tag{1}$$

If the decentralised multiuser $(F_1, F_{2,....}F_k)$ scenario is applied for federated learning, k stands for the number of clients and pk is the weight value of the k^{th} client. Any client user can view the current user's dataset $(D_1, D_2, ...D_k)$.

Federated learning is a novel approach to building smart, private, and secure Internet of Things (IoT) gadgets. Here are the main phases of FL-smart healthcare:

Several criteria are used by the centralised processing unit to decide on an analytical objective, such as automated biomedical imaging or motion detection. The FL procedure also involves the selection of a group of participants from a pool of people chosen by the target.

- Educational Workshops and Discussion Groups in Local Communities Once the dataset of knowledgeable users is found, the network will distribute a prototype model to the clients along with an initial global gradient to kick off the distributed training process. Each user can get a rough notion of their model's health by training an own, offline model using their own data. A novel model, v0 G, is created by the server after the training has been configured and it is sent to the users to start dispersed training. Each client k drills a local model using its own data Dk and evaluates an update v_k by mitigating a loss function $F(v_k)$.

$$v_k^* = \arg\min F(v_k), k \in K \tag{2}$$

The loss function for various FL algorithms may differ. A linear regression's loss function F The Federated Learning model can be summarised as follows: $F(v_k) = \frac{1}{2}\left(p_i^T v_k - q_i\right)^2$ by use of a collection of input-output pairs denoted by the letter $\{p_i q_i\}_{i=1}^{K}$. Then, for the sum, all the clients k sends the server their best guess at the latest update v_k.

Using the "model aggregation and download" process, the server collects the most recent data from the chosen clients and downloads it in one fell swoop. When it comes to model averaging, Google's Federated Averaging (FedAvg) technique takes a weighted, element-wise average of the gradient parameters of local models based on the sizes of the client datasets. Clients will then download the revised global model from the server and use it as a basis for updating their own local models during the upcoming training cycle. Specifically, the server calculates and incorporates into the global model, the following client-side model customizations:

$$v_G - \frac{1}{\sum_{k\in K}|D|}\sum_{k=1}^{K}|D|\,v_k \qquad (3)$$

in which the optimization problem to be solved is as follows:

$$(A1):\min_{w\in k}\frac{1}{K}\sum_{k=1}^{K}F(v_k) \qquad (4)$$

subject to (C1): v_1 = v_2 =...= v_k = v_G The success of a FL-based item classification task, for example, is reflected in the loss function F, which characterises the FL method's precision. Also, after each training cycle, the central server and all the individual users will have the same training model for the Federated Learning problem because to the constraint (C1). Once the model is complete, the server will update all users with the latest global version v_G so that they can improve their trained models during the next training session. The process repeats itself until either the required level of precision is reached or the loss function converges.

4. Result and Discussion

4.1. Experimental Setup:

The suggested DeepFed model is executed with the Keras API1 and the federated learning framework is constructed with the Flask framework for Python, which is a lightweight framework. 2 Our research is being showed on a platform running Ubuntu 18.04.3 LTS and outfitted with an Intel Xeon E5-2618L v3 central processor unit and an NVIDIA GeForce RTX 2080TI graphics processing unit (64GB RAM)

4.2. The Performance Metrics

The overall functionality of the proposed technique was determined by analysing the performance of aberrant human activity recognition from a confusion matrix and computing the following performance metrics.

Precision: The ratio of total TP to total component tags is provided for the positive class as (i.e., the sum of TP and FP). For example, PPV stands for Positive Predictive Value. Use the following formula to calculate accuracy:

$$\text{Precision} = \frac{TP}{TP+FP} \qquad (5)$$

F1 Score: The harmonic mean of recall and precision is used as a metric in Equation (6).

$$\text{F1 Score} = \frac{2TP}{2TP+FP+FN} \qquad (6)$$

Accuracy: Accuracy is calculated by dividing the total number of components by the number of components TP and TN. Precision can be calculated using the following equation: (7).

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \qquad (7)$$

Recall Analysis: Divide the number of negative class components by the total number of negative class components to demonstrate this (i.e., the sum of TN and FP). In terms of mathematics, we get the following: in eq (8).

$$\text{Recall} = \frac{TP}{TP+FN} \qquad (8)$$

4.3. Precision

Table 1: Precision Analysis of DeepFed Method with existing system

No of data from dataset	LSTM	RF	RNN	DeepFed
100	76.11	81.46	86.24	90.24
200	77.81	82.25	87.11	91.45
300	78.12	83.44	86.81	93.24
400	79.35	82.87	88.11	94.86
500	80.27	84.11	89.75	95.36

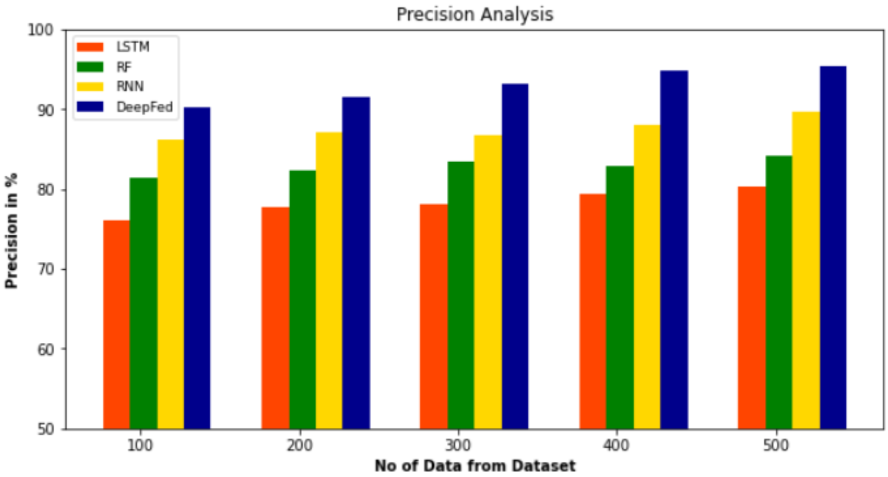

Figure 2: Precision Analysis for DeepFed Method with existing system

Figure. 2 and Table 1 illustrate a comparative precision examination of the DeepFed approach with other existing methods. The figure shows that the deep learning approach has resulted in higher performance with precision. For example, with data 100, the precision value is 90.24% for DeepFed, whereas the LSTM, RF and RNN models have obtained a precision of 76.11%, 81.46% and 86.24%, respectively. However, the DeepFed model has shown maximum performance with different data set size. Similarly, under 500 data, the precision value of DeepFed is 95.36%, while it is 80.27%, 84.11% and 89.75% for LSTM, RF and RNN models, respectively.

4.4. Recall

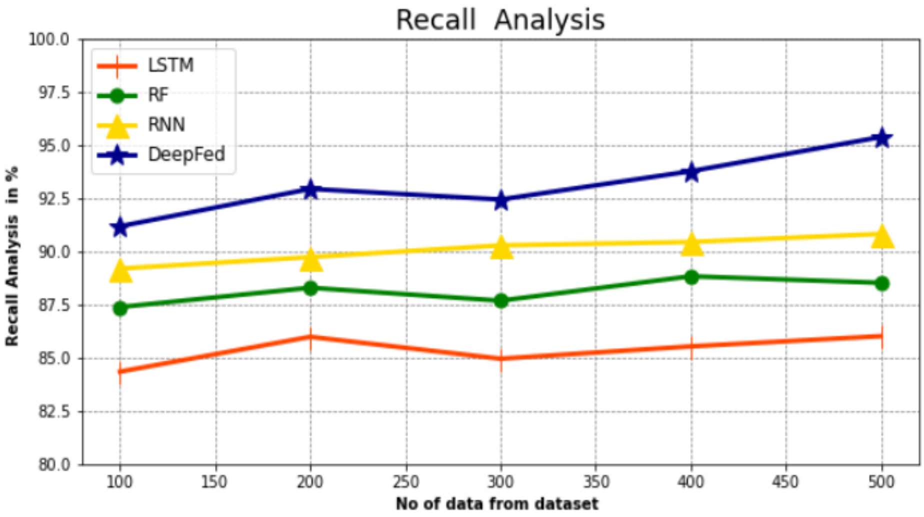

Figure 3: F-Score Analysis for DeepFed Method with existing system

Table 2: Recall Analysis of DeepFed Method with existing system

No of data from dataset	LSTM	RF	RNN	DeepFed
100	84.34	87.38	89.19	91.18
200	85.98	88.29	89.73	92.94
300	84.95	87.68	90.28	92.44
400	85.53	88.83	89.44	93.77
500	86.01	88.52	90.82	95.38

Figure .3 and Table.2 illustrate a comparative recall examination of the DeepFed approach with other existing methods. The figure shows that the deep learning approach has resulted in higher performance with recall. For example, with data 100, the recall value is 91.18% for DeepFed, whereas the LSTM, RF and RNN models have obtained a recall of 84.34%, 87.38% and 89.19%, respectively. However, the DeepFed model has shown maximum performance with different data set size. Similarly, under 500 data, the recall value of DeepFed is 95.38%, while it is 86.01%, 84.11% and 90.82% for LSTM, RF and RNN models, respectively.

4.5. F-Score

Table 3: F-Score Analysis of DeepFed Method with existing system

No of data from dataset	LSTM	RF	RNN	DeepFed
100	89.27	90.86	92.38	93.75
200	88.18	89.43	92.63	94.83
300	89.52	90.52	93.76	95.27
400	89.95	91.98	93.82	95.68
500	88.37	91.54	92.96	96.99

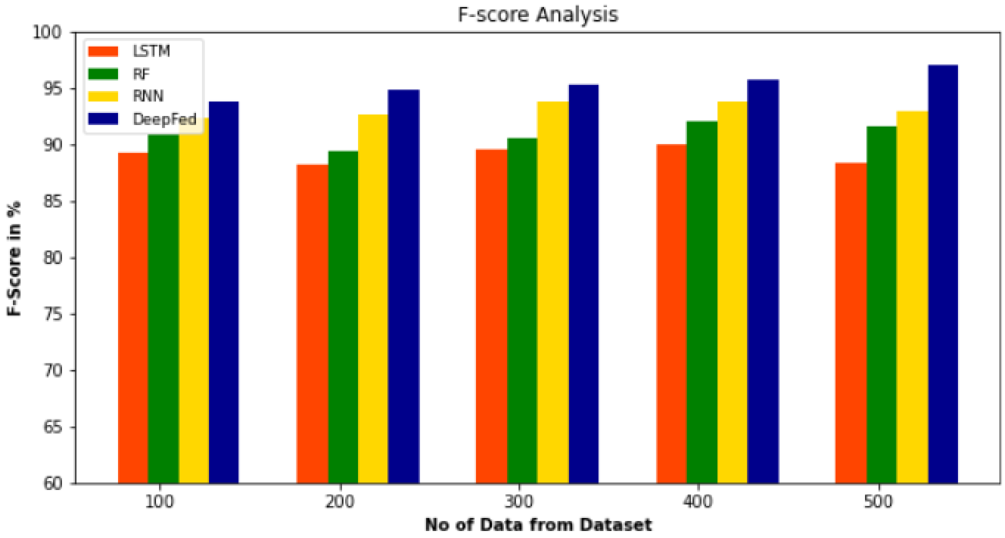

Figure 4: F-Score Analysis for DeepFed Method with existing system

Figure. 4 and Table.3 illustrate a comparative f-score examination of the DeepFed approach with other existing methods. The figure shows that the deep learning approach has resulted in higher performance with f-score. For example, with data 100, the f-score value is 93.75% for DeepFed, whereas the LSTM, RF and RNN models have obtained a f-score of 89.27%, 90.86% and 92.38%, respectively.

However, the DeepFed model has shown maximum performance with different data set size. Similarly, under 500 data, the f-score value of DeepFed is 96.99%, while it is 88.37%, 91.54% and 92.96% for LSTM, RF and RNN models, respectively.

4.4. Accuracy

Table 2: Accuracy Analysis of DeepFed Method with existing system

No of data from dataset	LSTM	RF	RNN	DeepFed
100	81.45	86.24	90.11	93.24
200	81.74	85.36	91.24	93.45
300	82.35	86.48	90.85	94.51
400	83.26	87.11	92.35	95.21
500	84.11	87.24	92.95	96.77

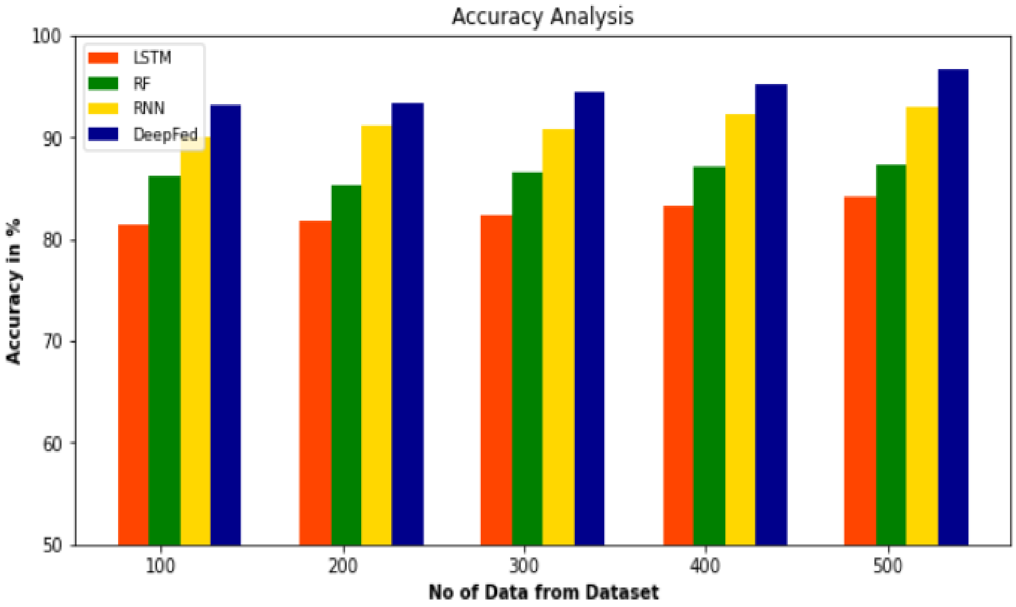

Figure 3: Accuracy Analysis for DeepFed Method with existing system

Figure. 3 and Table 2 illustrate a comparative accuracy examination of the DeepFed approach with other existing methods. The figure shows that the deep learning approach has resulted in higher performance with accuracy. As an illustration, on data 100, DeepFed achieves an accuracy of 93.24%, whereas LSTM, RF and RNN models achieve an accuracy of 81.45%, 86.24% and 90.11%, respectively. When tested with datasets of varying sizes, however, the DeepFed model consistently outperformed the competition. Similarly, under 500 data, the accuracy value of DeepFed is 96.77%, while it is 84.11%, 87.24% and 92.95% for LSTM, RF and RNN models, respectively.

4.5. Execution Time

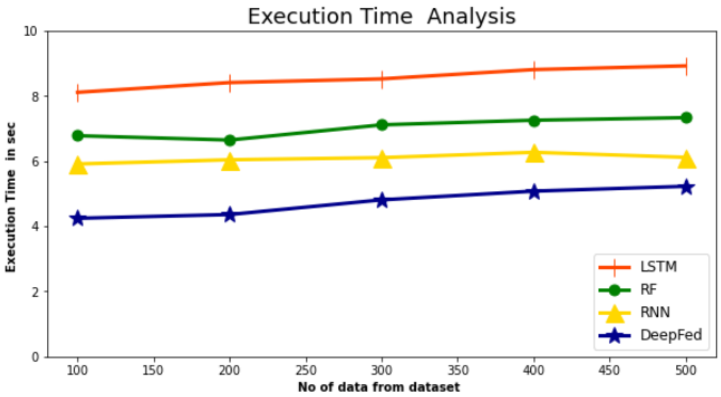

Figure 4: Execution Time Analysis for DeepFed Method with existing system

Table 3: Execution time Analysis for DeepFed Method with existing system

No of data from dataset	LSTM	RF	RNN	DeepFed
100	8.112	6.781	5.913	4.245
200	8.412	6.647	6.041	4.361
300	8.525	7.114	6.107	4.811
400	8.811	7.256	6.271	5.078
500	8.925	7.335	6.117	5.227

The DeepFed technique's Execution Time analysis with existing approaches is described in Tab 3 and Fig 4. The data clearly demonstrates that the DeepFed method surpassed the other techniques in every way. For 100 data, the DeepFed method has taken only 4.245 sec to execute, while the other existing techniques like LSTM, RF and RNN have an execution time of 8.112 sec, 6.781 sec and 5.913 sec, respectively. Similarly, for 500 data, the DeepFed method has an execution time of 5.227 sec while the other existing techniques like LSTM, RF and RNN have 8.925 sec, 7.335 sec and 6.117 sec of execution time, respectively.

5. Conclusion

In this study, we present a method for keeping people's personal health information secure during online data transfers. In this work, we explore the security issues at various levels of cyber-physical systems and the corresponding threat models and provide a high-level overview of the research obstacles associated with developing secure cyber-physical systems. This research analyses the state-of-the-art static and adaptive detection and prevention systems, as well as the limitations of each, to find solutions to these problems. The paper concludes by establishing open research problems for building intelligent CPS security protocols and ML-based security solutions, with the goal of protecting against a wide range of threats found across several layers of the CPS. New avenues for protecting users' privacy in IoMT without requiring access to their data have been opened up by the federated learning (FL) distributive AI paradigm. By only showing gradients during training, FL further protects users' privacy. As part of this research, we introduce DeepFed, a novel Federated Deep Learning approach for discovering cyber threats to smart healthcare CPSs.

References

[1] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, “Trustworthy and intelligent covid-19 diagnostic IOMT through xr and deep-learning-based clinic data access,” IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15 965–15 976, 2021.

[2] R. F. Mansour, A. El Amraoui, I. Nouaouri, V. G. D´ıaz, D. Gupta, and S. Kumar, “Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems,” IEEE Access, vol. 9, pp. 45 137–45 146, 2021.

[3] F. Naeem, M. Tariq, and H. V. Poor, “SDN-enabled energy-efficient routing optimization framework for industrial internet of things,” IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5660–5667, 2020.

[4] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Blockchain and federated learning for privacy-preserved data sharing in industrial IoT,” IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4177–4186, Jun. 2020

[5] B. Li, R. Lu,W.Wang, and K.-K. R. Choo, “Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system,” J. Parallel Distrib. Comput., vol. 103, pp. 32–41, May 2017.

[6] N. Sayfayn and S. Madnick, “Cybersafety analysis of the Maroochy Shire sewage spill,” MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, MIT Management Sloan School, Cambridge, MA, USA, Working Paper CISL 2017-09, vol. 9, May 2017

[7] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, “Blockchain-based software-defined industrial Internet of Things: A dueling deep Q -learning approach,” IEEE Internet Things J., vol. 6, no. 3, pp. 4627–4639, Jun. 2019.

[8] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, “Deep learning detection of electricity theft cyber-attacks in renewable distributed generation,” IEEE Trans. Smart Grid, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.

[9] Lee SJ, Yoo PD, Asyhari AT, Jhi Y, Chermak L, Yeunand CY, Taha K (2020) IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction. IEEE Access 8:65520–65529.

[10] Kumar, Rajesh, et al. "Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging." IEEE Sensors Journal 21.14 (2021): 16301-16314.

[11] Tang D, Tang L, Dai R, Chen J, Li X, Rodrigues JJ (2020) Mfadaboost: Ldos attack detection based on multi-features and improved adaboost’. Futur Gener Comput Syst 106:347–359.

[12] McGhin, T., Choo, K.K.R., Liu, C.Z., He, D.: Blockchain in healthcare applications: Research challenges and opportunities. J. Net. Comput. Appl. 135, 62–75 (2019).

[13] Pokhrel, S.R., Choi, J.: Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. IEEE Transac. Commun. 68(8), 4734–4746 (2020).

[14] Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y.: Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Transac. Industrial Informat. 16(6), 4177–4186 (2019).

[15] A. M. Conforming, “Proposal for a privacy impact assessment manual conforming to iso/iec 29134: 2017,” in Computer Information Systems and Industrial Management: 17th International Conference, CISIM 2018, Olomouc, Czech Republic, September 27-29, 2018, Proceedings, vol. 11127. Springer, 2018, p. 486.

[16] A.Hardhavardhan, R.Partheepan,Ranjan Walia and V.Chandra Shekar Rao, Multilayer Stacked Probabilistic Belief Network-Based Brain Tumor Segmentation and Classification “International Journal of Foundations of Computer Science”, https://doi.org/10.1142/S0129054122420047

[17] Prasanthi Boyapati, Alhassan Alolo Abdul-Rasheed Akeji, Aditya Kumar Singh Pundir, Ranjan Walia, "LSGDM with Biogeography-Based Optimization (BBO) Model for Healthcare Applications", Journal of Healthcare Engineering, vol. 2022 https://doi.org/10.1155/2022/2170839

[18] A. V. R. Mayuri, T. Jackulin, J. L. Aldo Stalin, Varagantham Anitha, "Pigeon Inspired Optimization with Encryption Based Secure Medical Image Management System", Computational Intelligence and Neuroscience, vol. 2022, Article ID 2243827, 13 pages, 2022. https://doi.org/10.1155/2022/2243827.

[19] B. Jaishankar, Santosh Vishwakarma, Aditya Kumar Singh Pundir, Ibrahim Patel, N. Arulkumar, "Blockchain for Securing Healthcare Data Using Squirrel Search Optimization Algorithm", Intelligent Automation & Soft Computing, Vol. 32, No. 3, pp.1815-1829, 2022. DOI: 10.32604/iasc.2022.021822.

[20] F. Alshehri and G. Muhammad, “A comprehensive survey of the internet of things (iot) and ai-based smart healthcare.” IEEE Access, vol. 9, no. January, pp. 3660–3678, 2021

[21] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou and C. Tsatsoulis, “Review of security and privacy for the internet of medical things (iomt),” in 2019 15th international conference on distributed computing in sensor systems (DCOSS). IEEE, 2019, pp. 457–464

[22] M. M. Ogonji, G. Okeyo and J. M. Wafula, “A survey on privacy and security of internet of things,” Computer Science Review, vol. 38, p. 100312, 2020

[23] W. Aman and F. Kausar, “Towards a gatewaybased context-aware and self-adaptive security management model for iot-based ehealth systems,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 1, pp. 280–287, 2019.

[24] Morzelona, R. (2021). Human Visual System Quality Assessment in The Images Using the IQA Model Integrated with Automated Machine Learning Model . Machine Learning

Applications in Engineering Education and Management, 1(1), 13–18. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/5

[25] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider et al., “Iot privacy and security: Challenges and solutions,” Applied Sciences, vol. 10, no. 12, p. 4102, 2020.

[26] Cai, P., “Security threats and measures to protect in wireless sensor networks on an internet of things (IOT) platform”, International Journal of Applied Engineering and Technology, 2(2), p. 73-80, 2020

[27] Efe, A., & Isik, A. (2020). A general view of industry 4.0 revolution from cybersecurity perspective. International Journal of Intelligent Systems and Applications in Engineering, 8(1), 11-20. doi:10.18201/ijisae.2020158884

[28] Alissa, K. A., AlDeeb, B. A., Alshehri, H. A., Dahdouh, S. A., Alsubaie, B. M., Alghamdi, A. M., & Alsmadi, M. K. (2021). Developing a simulated intelligent instrument to measure user behavior toward cybersecurity policies. International Journal of Communication Networks and Information Security, 13(1), 82-91.

[29] Mondal, D., & Patil, S. S. (2022). EEG Signal Classification with Machine Learning model using PCA feature selection with Modified Hilbert transformation for Brain-Computer Interface Application. Machine Learning Applications in Engineering Education and Management, 2(1), 11–19.