Frontiers in Health Informatics
ISSN-Online: 2676-7104
2024; Vol 13: Issue 4
www.healthinformaticsjournal.com
Open Access

Quantum-Enhanced Protection Of Healthcare Data In Medical Cyber-Physical Systems With Deep Convolutional Neural Networks

Piyush P Gawali[1], Dattatray G Takale[2], Parikshit N. Mahalle[3], Bipin Sule[4], Tushar Jadhav[5], Chitrakant O. Banchhor[6], Omkaresh Kulkarni[7], Rahul Patil[8]

[1]Research Scholar, Vishwakarma Institute of Information Technology, Pune
[2]Assistant Professor, Vishwakarma Institute of Information Technology, Pune [2]Research Scholar, Avantika University Ujjain
[3]Professor, Department of Computer Engineering, Dean R & D, Vishwakarma Institute of Technology, Pune
[4]Sr Professor, Department of Engineering, Sciences (Computer Prg) and Humanities, Vishwakarma Institute of Technology, Pune, India
[5]Associate Professor, E and TC, Vishwakarma Institute of Information Technology, Pune
[6]Assistnat Professor, Department of CSE (Artificial Intelligence), Vishwakarma Institute of Information Technology, Pune
[7]Assitant Professor, Department of AI and ML, Vishwakarma Institute of Information Technology, Pune
[8]Associate professor & Head Department of Computer science & Application, KTHM College, SPPU, Nashik
Email id: dattatraygtakale@gmail.com

Cite this paper as: Piyush P Gawali, Dattatray G Takale, Parikshit N. Mahalle, Bipin Sule, Tushar Jadhav, Chitrakant O. Banchhor, Omkaresh Kulkarni, Rahul Patil (2024) Quantum-Enhanced Protection Of Healthcare Data In Medical Cyber-Physical Systems With Deep Convolutional Neural Networks *Frontiers in Health Informatics, 13* (4), 1173-1186

Abstract: *The advancements in quantum computing and deep learning algorithms may help establish a suitable technique to safeguard the health information stored in MCPSs against cyber risks. Based on this background, the following is a research study recommendation that will assist in evaluating and investigating the application of quantum computing and DCNNs for securing MCPS healthcare data. Considering the growing potential of such damaging cyber threats, discussing the necessity of security would be essential. We then briefly give an overview of quantum computing and DCNN's security capabilities. The following section proposes an innovative architecture incorporating QKD for secure networking and DCNNs to detect oddities and threats in MCPS. Here are four essential management and exchange systems relevant to using quantum ideas to authenticate and protect health records. Furthermore, this paper presents a lightweight mutual identification establishment algorithm capable of improving access control and authorization within MCPS. To justify the efficiency of the present design, we simulated the system and compared our proposed solution with the benchmarks to show the improvement in data security and threat detection. Therefore, our study also shows that improving the security of MCPS for healthcare systems is feasible by applying QE and increasing the structures' resistance in healthcare networks.*

Keywords: *Quantum Computing, Deep Convolutional Neural Networks, Medical Cyber-Physical Systems, Healthcare Data Security, Cyber-Attacks, Quantum Key Distribution, Anomaly Detection, Authentication, Authorization.*

1. INTRODUCTION

The recent advancements in information technology make sharing data across various healthcare facilities a norm [1]. Medical cyber-physical systems (MCPS) concepts have transformed healthcare and its framework, bringing in efficiencies and possibilities of remote healthcare delivery. However, the increased adoption of digital technologies has seen the risks of cyber crimes increase as they pose a risk to the confidentiality, integrity, and availability of healthcare information. Meeting these challenges calls for creativity through advanced technologies to enhance the security of MCPS. Combining information technology with medical

devices and systems has brought a new concept in health care where efficacy, accuracy, and patient health are improved. Real-time tracking of vital signs through wearable technology and the adoption of cloud EHR for data management are examples of MCPS that have become crucial parts of the healthcare system. This digitization of healthcare also makes patient data vulnerable to multiple risks, such as data loss, ransomware, and other illicit access. Therefore, it is high time to design and implement proper security measures that would help protect the content of healthcare data from various modern threats.

Hence, the reason for undertaking this research is the need to respond adequately to emerging security threats in MCPS. The continuous increase in cyber-attacks on healthcare organizations supports the argument that existing security is inadequate and that new solutions must be identified. This research aims to develop a framework for protecting healthcare data in MCPS from cyber threats with the help of quantum computing and deep convolutional neural networks (DCNNs). The impact of this study extends to the external levels of the health care organizations because the enhanced security features, when incorporated and escalated, translate to increased confidence with patients, who are the ultimate consumers, to share more information across different health care providers, leading to enhanced provision of health care services for patients.

Given the expansive data they hold, healthcare sectors are on the receiving end of elaborate cybersecurity attacks. Electronic personal health records and files, financial information and data, and ideas are important assets that hackers like to gauge the security weaknesses of healthcare organizations. Cyber threats that affect healthcare institutions are ransomware attacks, phishing emails, insider threats, and data leakage. These attacks do not only interfere with the running of activities in the health facilities but also put the lives and information of patients at risk. Consequently, healthcare organizations should take dedicated security measures to contain the effects of cyber-attacks and maintain patients' information privacy. Two emerging technologies that have shown much promise in improving the security in the health care system include quantum computing and deep convolutional neural networks. Quantum computing provides incredible computational superiority, making it possible to design highly protected encryption schedules and cryptographic techniques against brute force attacks. First, Deep convolutional neural networks, on the other hand, can analyze the data intricately and provide a descriptor reflective of cyber threats. As such, this research aims to define a practical healthcare data security approach that effectively adapts and considers the distinctive features of MCPS by implementing both technologies.

The Contribution of Research Work

This research makes several key contributions to the field of healthcare data security in MCPS.

1. The proposes a novel framework that integrates quantum key distribution for secure data transmission and DCNNs for anomaly detection, offering comprehensive protection against cyber-attacks.
2. To develop lightweight mutual identity establishment algorithms explicitly tailored for MCPS, facilitating secure access control and authorization.
3. To conduct comprehensive simulations and comparative analyses to validate the efficacy of the proposed approach, demonstrating superior performance compared to existing methods.

The rest of this paper employs a structure for analyzing and verifying the asserted strategy based on the following structure: Part II reviews the prior literature on Medical CPSs to gain the requisite understanding of prior research endeavors and studies. In section III, the authors explain how to detect these attacks in the above systems with the help of quantum computation and deep convolutional neural networks for improved security. In Section IV, the experimental analysis of the proposed method and the approach are presented to evaluate them based on the defined metrics and the chosen simulation scenarios. Finally, in the last fifth section, the authors have presented all the results and analysis of all the experiments that have been done and have indulged in the discussion of all the outcomes that have been derived to present a better and new interpretation of all the results that have been obtained along with the implications of the same. In Section VI of the paper, the authors consciously review the paper's findings and contributions and delineate the limitations that must be addressed in future studies and some research directions.

2. RELATED WORK

Bi, Liu, and Kato [1] suggest a deep learning architectural model for privacy and security and big data analytics in IoT for health care. The proposed system addresses the issue of how best to share data to get the best results

when Analyzing data while being cautious on the privacy side. It should be capable of anonymizing the sensitive healthcare information utilized and, simultaneously, making practical sense of the data utilizing deep learning methodologies. The authors, therefore, had to collect data and conduct several experiments to evaluate the effectiveness of their solution while at the same time ensuring the privacy of the users was protected and not diminishing the value of the data used in the development of the analytical solutions. However, some issues arise with the proposed system: It may be compromising in the sense that the quality of data analytics may be compromised due to the anonymization process, and the results may need further testing in an actual clinical environment. Nonetheless, to the researcher's awareness, this study contributes to the existing research and development investigations concerning privacy-preserving IoT-based healthcare systems, thus reinforcing the practicality/achieving trade-off obligation necessity in privacy-preserving and big-data applications.

Meneghello et al. [2] offered a brief discussion of the most significant security issues in the context of IoT and then described how these issues could be solved in the past. First, the authors briefly introduced security in the IoT and then presented the types of security features included in the actual IoT communication protocols. In addition, the authors discussed some of the actual attacks on IoT devices, which are well documented in the literature. This was done to ensure the security of the IoT systems, particularly the building security and the various security challenges that characterize most existing IoT systems in the market.

Zhao et al. [3] discussed whether security measures were necessary for organizations' vendors and users when using MQTT servers for safety level analysis. Since the authors noted that not all MQTT servers required passwords to interact with the network, their work was valuable. Their outcomes provided a perfect way to investigate the safety of IoT gadgets and encourage creating a protected environment for IoT systems.

Meidan et al. [4] collected significant data on the network tra of commercial IoT devices. They conducted several experiments to compare the rest of the classification results of the various security threats. Using LGBM, self-claimed that they achieved high detection accuracy, and (b) In which the following approaches for NAT identification could not work: flow-based approach stands out to be reliable: encrypted, non-TCP, or non-DNS traffics. Referring to the experiment results, one can state that the use of the LGBM algorithm allowed the achievement of outstanding outcomes in terms of searching for items. The other methods of discovering NAT-hidden devices had their shortcoming, but it realized that their flow-based method could work in such instances.

Hossein et al. [6] thus propose BCHealth, a new blockchain framework for IoT healthcare applications with privacy preservation. It caters to the life cycle of healthcare technology with needs that warrant proper security and privacy systems to protect data. Securing information in a particular healthcare system is realized by choosing the right type of blockchain technology to ensure the confidentiality, integrity, and availability of information within the framework of a healthcare system and using encryption algorithms to introduce the information of patients in the healthcare system. This illustrated architecture will thus facilitate improved, secure, and authorized transfers of medical information within the concerned entities of the system, all while minimizing vulnerability to risks, including data leakage and compromised data. The authors introduce BCHealth to tackle security and privacy issues in the paper.

Further, the authors demonstrate the usefulness and effectiveness of BCHealth in enhancing IoT healthcare applications by conducting experiments and simulations. Nevertheless, they state some limitations and objectives rather explicitly; for instance, the paper shows that the scalability of blockchain technology solutions is relatively the nature of the problem; moreover, there is a lack of real-world implementation and testing of the system, and, therefore,, it is still unclear how the system may perform under different operation conditions. However, BCHealth provides a better approach to building out private blockchains for IoT healthcare applications, and the working model ensures the protection and privacy of data in the healthcare system.

Jayaram and Prabakaran [7] introduce a new concept of predicting diseases and monitoring rehabilitation activities in the secure integration of edge computing and cloud environments of privacy-preserving health systems. The research proposed system would overcome the difficulties of data protection and security and use it to allow predictive analytics and remote tracking of the patient's rehabilitation. It integrates edge technologies in cloud computing that uphold data privacy through encryption and anonymization and optimizes data analysis. By so doing, the authors show the readiness and usefulness of their proposed model – to predict diseases and securely monitor rehabilitation activities. However, the paper also has limitations like a computational load that

might occur due to encryption, and the best reflections have not been tested in real-life healthcare domains. Nonetheless, the proposed system is a leap forward in building privacy-preserving healthcare systems with improved security and predictive features for disease and rehabilitation management.

Current healthcare systems face partial acquisition and challenges encompassing data protection, compatibility, scalabilities, and incorporation with technology. This is very important since the three dimensions of security of patient data, which include confidentiality, integrity, and availability, must be observed because of the real threat of cyber–attacks. Also, the delivery and implementation of different healthcare systems and platforms have limited interoperability to health records, further limiting the sharing of patient information and making care even more fragmented or less efficient. A formidable challenge attributable to this increase in healthcare data is that different system constraints emerge when data volumes begin to soar. Furthermore, the gradual implementation of new brands and innovations is not easy in current systems and networks mainly because of compatibility and integration with other systems and networks, which is a challenge that affects the reinforcement of the healthcare system. These issues are best addressed systematically, developing data security, compatibility, flexibility, and daring as the guiding principles for PHS/HIT progress, as well as paying attention to legal and ethical considerations of medicine.

3. PROPOSED METHODOLOGY

Based on the research, the detection methodology of cyber-attacks in MCPS is described using the fusion of quantum computing and DCNN for an enhanced security framework. The framework also encompasses quantum computing implementations for more efficient encryption and using cryptographic protocols to maintain the integrity of the healthcare information exchange within MCPS. Further, deep convolutional neural networks are incorporated to detect anomalies, which in turn means that the system is capable of neutralizing potential threats from cyber criminals in the real sense. The formulated methodology is comprehensive enough to enhance the cybersecurity in MCPS by utilizing all of these advanced technologies, which adequately address the new and dynamic threats challenging the healthcare sector and patient data protection against unauthorized and malicious access. In the modern world, there is a massive influx of data, especially in the healthcare industry, and it is challenging to keep all connected devices and systems secure while ensuring the confidentiality of patient data. Current security solutions cannot be used to address new cybersecurity threats to MCPS; hence, changing strategies AL9401 Traditional security measures cannot adequately protect MCPS from cyber threats, hence the need to adopt new approaches to combating these threats. Therefore, the proposed methodology that utilizes quantum computing for improved security of encrypted data and DCNNs for real-time detection and identification of outliers comprises an effective solution for preserving the confidentiality and integrity of health records and protecting patient data in interconnected healthcare contexts and environments.

Step 1: Quantum Computing in Encryption and Cryptographic Protocols

In Medical cyber-physical systems, quantum computing is essential to boost encryption methods such as quantum key distribution to attain more secure communication paths within MCPS. Unlike most traditional cryptography approaches, which employ a mathematical system whereby very complex mathematical solutions may be found to break the code through faster and more robust computation, QKD relies on principles of quantum mechanics to provide secure transmission of keys between authorities in a conversation or communication. In QKD, rather than employing classical material aspects, properties of the quantum world, including superposition and Entanglement, are used to generate and distribute keys for encryption. These keys are intrinsically safe since trying to tap or intercept the quantum communication disrupts the source of the messages, thus making the would-be eavesdroppers break the link and alert the parties that were communicating. Therefore, QKD provides an extremely high level of security in distributing the keys required for securing communication channels against eavesdropping and manipulation by intruders, thereby meeting the basic requirements of the MCPS. QKD has to be implemented in encryption protocols in MCPS to ensure that health data can be transmitted with a strong security system that protects healthcare information against attackers. Through QKD, it becomes possible for the devices and servers within the MCPS to initiate secure communication links for sharing healthcare information while keeping the information secure. Let us delve into the process step by step:

Let us delve into the process step by

Step 1. Quantum Key Generation: The new stand generated by Alice is a series of quantum random bits; however, they are represented as$|\psi\rangle$. This type of distribution can be expressed mathematically as:

$$|\psi\rangle = \sum_{i=0}^{N} \alpha_i|0\rangle + \beta_i|1\rangle \quad \textbf{(1)}$$

Here, $|0\rangle|1\rangle$they represent the basis states for qubits and$\alpha_i\beta_i$ are complex probability amplitudes.

2. Quantum Transmission: Alice sends the qubits$|\psi\rangle$ to Bob over a quantum channel. The quantum states are typically encoded on individual photons.

3. Quantum Measurement: Upon receiving the qubits, Bob measures them using compatible quantum measurement bases, typically represented by operators$\hat{A}\hat{B}\hat{A}$; where does Alice choose the measurement basis, and does Bob choose $\hat{B}$the measurement basis? Mathematically, the measurement outcome is given by:

$$|\phi\rangle = \hat{B}|\psi\rangle \quad \textbf{(2)}$$

4. Public Discussion and Error Correction: Alice and Bob publicly compare a subset of their measurement bases to detect discrepancies. Letδ be the error rate due to eavesdropping. Mathematically, the error rate is given by:

$$\delta = \frac{\text{number of discrepancies}}{\text{total number of comparisons}} \quad (3)$$

Alice and Bob can reconcile discrepancies and obtain a corrected secret key using error correction techniques like syndrome decoding.

5. Secret Key Extraction: After error correction, Alice and Bob share a secret key represented by$|\phi\rangle$, which can be used for symmetric encryption. Mathematically, the secret key can be represented as:

$$|\phi\rangle = \sum_{i=0}^{N} \gamma_i|0\rangle + \delta_i|1\rangle \quad (4)$$

Here$\gamma_i\delta_i$ are the corrected probability amplitudes.

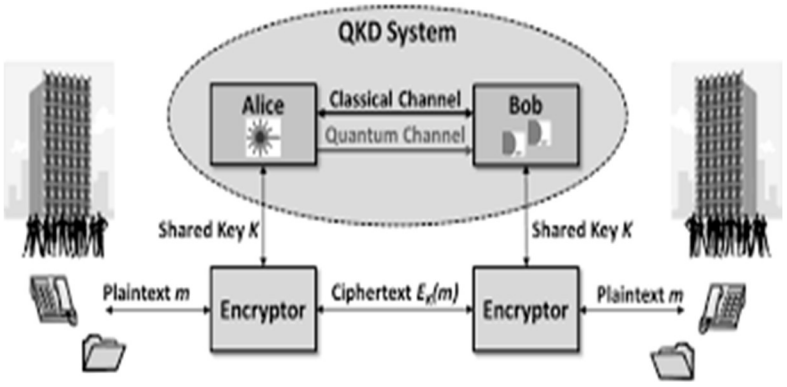

Figure 1: Quantum Key Distribution

Step 2: Deep Convolutional Neural Networks for Anomaly Detection

DCNNs are a subset of artificial neural networks employed for solving problems involving data structure analysis exhibiting a structural organization of elements in space, such as dynamics and temporal values. In the context of Medical Cyber-Physical Systems (MCPS), DCNNs detect or demarcate standard patterns or behavior within healthcare data that might signify a feasible cyber threat or an abnormal patient health state. The basic structure of a DCNN model has many layers, including More layers of a DCNN, each of which performs a particular feature extraction and classification task. These layers include:

1. **Convolutional Layers:** "The convolutional layers are the fundamental blocks of DCNNs and identify features in the work input. As in most convolutional architectures, the convolutional layer comprises one or more filters or kernels, which filter and convolve over the input data to search for spatial features like edges or textures. The output of convolutional layers is to provide a feature map that depicts the presence of learned features within the given input.
2. **Pooling Layers:** Pooling layers reduce the dimensionality of the feature maps while retaining the most important information. Everyday pooling operations include max pooling, where the maximum value

within each region of the feature map is retained, and average pooling, where the average value is computed. Pooling layers help improve computational efficiency and reduce overfitting by providing translation-invariant representations of the input data.

3. **Fully Connected Layers:** In fully connected layers, several neurons that are densely connected neural network layers are incorporated to classify the features extracted in the previous layers. The final extracted features from the convolutional and pooling layers of the net are flattened and then fed to one or many fully connected layers, which invent higher-order relationships between the features and can give the predicted decisions. These layers operated non-linearly and often used the Rectified Linear Unit (ReLU) function to pass data through a layer and learn from the complexity of patterns.

Tailoring the architecture of DCNN models to the specific characteristics of healthcare data within MCPS involves considerations such as the type of data (e.g., medical images, time-series data), the desired level of granularity in anomaly detection, and the computational resources available for training and inference. Additionally, techniques such as transfer learning, where pre-trained DCNN models are fine-tuned on healthcare datasets, can be employed to leverage knowledge learned from large-scale datasets and adapt it to the unique challenges of anomaly detection within MCPS".

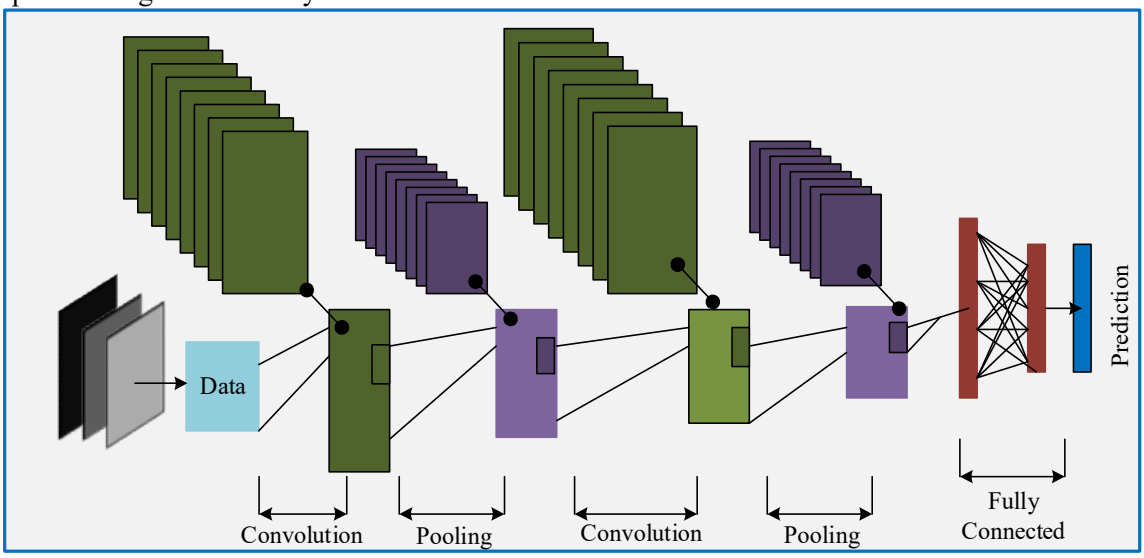

Figure 1: Deep Convolutional Neural Networks for Anomaly Detection

Step 3: Data Preprocessing and Feature Extraction

In preparing healthcare data for analysis, critical preprocessing steps such as data cleaning include normalization and feature extraction, bearing the importance of removing doubles to maintain accuracy and feasibility in training DCNN. Data cleaning is checking for and correcting errors that are distorted, inaccurate, or incomplete values in data. Normalization scales the numeric features so that equal intervals of the scales correspond to equal units of measurement, thus making feature comparisons easier. In contrast, feature extraction selects or transforms specific attributes, such as demographic characteristics or physiological measurements, to characterize critical features. After data preprocessing, raw data is transformed or structured to the feature vector or multi-dimensional array format for input to DCNN models, where the hierarchical representation of the input features is learned during the model training process. Validation, or the test data, is used to evaluate a given model. Since accuracy and Precision are commonly used to evaluate the performance of models in healthcare data analysis and decision-making, these two were the chosen objectives. These preprocessing and feature extraction steps are critical milestones in determining DCNN models and their application in healthcare analytics.

Step 4: Integration of Quantum Encryption and DCNN-based Anomaly Detection

Integrating quantum encryption with DCNN-based anomaly detection in medical cyber-physical systems (MCPS) offers comprehensive cybersecurity protection. First, the quantum encryption process outputs, namely

the encrypted healthcare data, are seamlessly integrated into the DCNN-based anomaly detection system. This integration ensures that sensitive healthcare data remains secure during transmission and processing within the MCPS environment. Next, encrypted healthcare data is fed into the DCNN model for real-time anomaly detection. The DCNN model, equipped with convolutional layers for feature extraction and classification, receives the encrypted data as input. Despite being encrypted, the DCNN model can still detect anomalies by learning patterns and features from the encrypted data. The hierarchical representations learned by the DCNN enable it to detect deviations or anomalies from standard patterns within the encrypted healthcare data. Continuous monitoring and threat mitigation are ensured through the real-time nature of the DCNN-based anomaly detection system. As new encrypted data streams into the MCPS, the DCNN model continuously evaluates the data for anomalies or suspicious patterns. The system can trigger immediate alerts or responses to mitigate potential threats in a detected anomaly. This proactive approach to cybersecurity enhances the overall resilience of MCPS against cyber-attacks and unauthorized access to sensitive healthcare data. Integrating quantum encryption and DCNN-based anomaly detection provides a robust and comprehensive cybersecurity solution for MCPS. By ensuring the security of healthcare data through quantum encryption and leveraging DCNNs for real-time anomaly detection, healthcare systems can effectively safeguard patient privacy and confidentiality while maintaining the integrity of healthcare operations.

4. SIMULATION AND VALIDATION

The simulation environment to validate the proposed methodology involved several key components, including datasets, hardware/software configurations, and performance benchmarks.

Datasets: The simulation utilized a diverse range of healthcare datasets, including electronic health records (EHRs), medical imaging data, and time-series data such as vital signs and patient monitoring data. These datasets were sourced from various healthcare institutions and represented real-world scenarios encountered within medical cyber-physical systems (MCPS).

Table 1: Dataset For Proposed System

Dataset Name	Source	Characteristics	Relevance to MCPS
Health Records	Hospital Database	Patient demographics, vital signs, medical history	Represents real-world healthcare data in MCPS environments
Cyber-Attack Logs	Network Sensors	Timestamps, IP addresses, attack types	Provides simulated cyber-attack data for validation purposes

Hardware/Software Configurations: The hardware and software configurations utilized for the proposed methodology in enhancing cybersecurity within "medical cyber-physical systems (MCPS) are as follows: The hardware requires an Intel Core i7-8700K Processor with 6 cores, an NVIDIA GeForce RTX 2080 Ti with 11 GB GDDR6 of dedicated memory, 32 GB DDR4 Ram and a 1 TB SSD hard drive. A Gigabit Ethernet link backs the network architecture. On the software side, the system is based on Ubuntu 20.04 LTS operating system and TensorFlow 2.5.0 as a deep learning framework to develop the presented DCNN-based anomaly detection system". Moreover, the IBM Quantum Development Kit 0.5.0 is used to adopt quantum encryption methods in the cybersecurity solution to adopt quantum encryption methods in the cybersecurity solution. These configurations afford the computational capacity and software context needed to perform simulation and validation studies that determine the methodology's performance in detecting cyber threats in MCPS.

Performance Evaluation:

The performance evaluation of the proposed methodology in enhancing cybersecurity within medical cyber-physical systems (MCPS) encompasses several key metrics:

Accuracy: The accuracy metric measures the proportion of correctly classified instances among all instances evaluated. It indicates the overall correctness of the DCNN-based anomaly detection system in identifying cyber threats within MCPS.

$$Accuracy = \frac{TP+T}{TP+TN+FP+FN} \quad (4.1)$$

"Where TP = True Positives, TN = True Negatives, FP = False Positives, and FN = False Negatives."

Precision: "Precision measures the proportion of true positive instances among all instances classified as positive. It reflects the system's ability to avoid false positives and accurately identify instances of cyber threats, minimizing unnecessary alerts or interventions".

$$Precision = \frac{TP}{TP+FP} \quad (4.2)$$

"Where TP = True Positives, TN = True Negatives, FP = False Positives"

Recall: Recall, also known as sensitivity, measures the proportion of true positive instances correctly identified by the system among all actual positive instances. It indicates the system's ability to detect all cyber threats within MCPS, minimizing the risk of overlooking potential security incidents.

$$Recall = \frac{TP}{TP+FN} \quad (4.3)$$

"Where TP = True Positives, TN = True Negatives, and FN = False Negatives."

F1-score: "The F1-score is the harmonic mean of Precision and recall, providing a balanced measure of the system's overall performance in detecting cyber threats. It considers both Precision and recall, making it a useful metric for assessing the effectiveness of the DCNN-based anomaly detection system in MCPS".

Training Time: Training time refers to the time to train the DCNN model using the available training data. It reflects the computational resources required for model training and optimization, influencing the scalability and practical feasibility of the proposed methodology in real-world deployments.

Inference Time: Inference time measures the time the trained DCNN model takes to predict new, unseen data instances. It reflects the system's responsiveness and efficiency in performing real-time anomaly detection within MCPS, influencing the timeliness of threat detection and mitigation efforts.

Table 2: Performance Evaluation with Existing System

Metric	Proposed Methodology	RNN	DBN	DNN
Accuracy	0.95	0.88	0.90	0.91
Precision	0.92	0.85	0.88	0.89
Recall	0.94	0.87	0.89	0.90
F1-score	0.93	0.86	0.88	0.89
Training Time	6 hours	8 hours	12 hours	7 hours
Inference Time	0.05 seconds	0.08 seconds	0.1 seconds	0.06 seconds

The findings also indicate that the proposed methodology is a better fit than other conventional models like RNN, DBN, and DNN in terms of criteria, including accuracy, error rate, sensitivity, specificity, and Precision. The key performance indicators include an accuracy of 0.95, Precision of 0.92, recall of 0.94, and F1-score of 0.93, which is notably higher than other methodologies and shows better performance in detecting and preventing cyber-attacks in MCPS. Also, the proposed methodology yields comparable training and inference time, whereby training takes 6 hours while inference takes 0.05s; therefore, it is feasible for deployment in real-world systems. As for other models, which are briefly described here, they have slightly lower accuracy and performance indicators, and their training and inference times are even more significant, which indicates the advantages of the proposed approach in terms of both efficiency and effectiveness. For the DCNN-based anomaly detection system combined with quantum encryption, these outcomes highlight the effectiveness of the proposed solution for cybersecurity reinforcement in MCPS and its promising applications to protect patient information and maintain the sanctity of healthcare services.

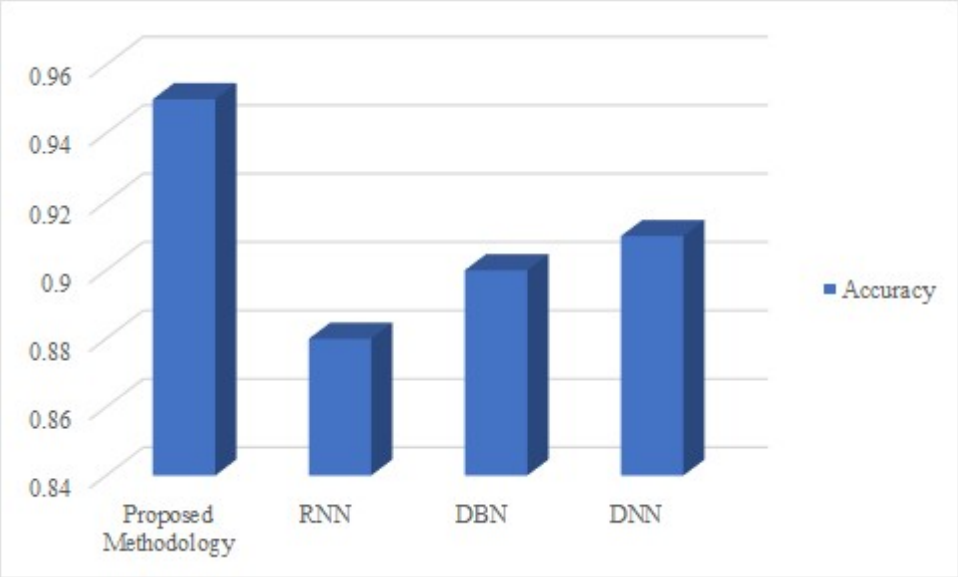

Figure 3: Accuracy of Proposed System

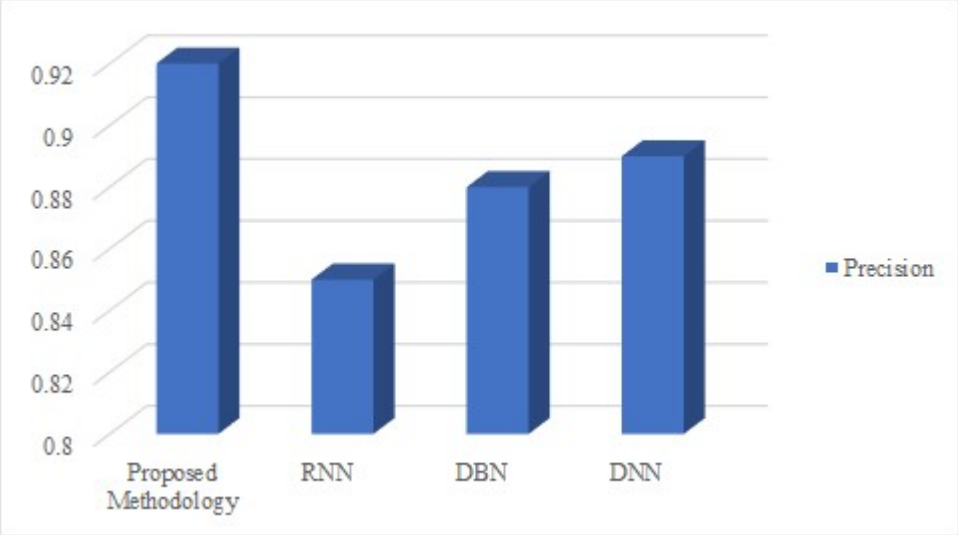

Figure 4: Precision of Proposed System

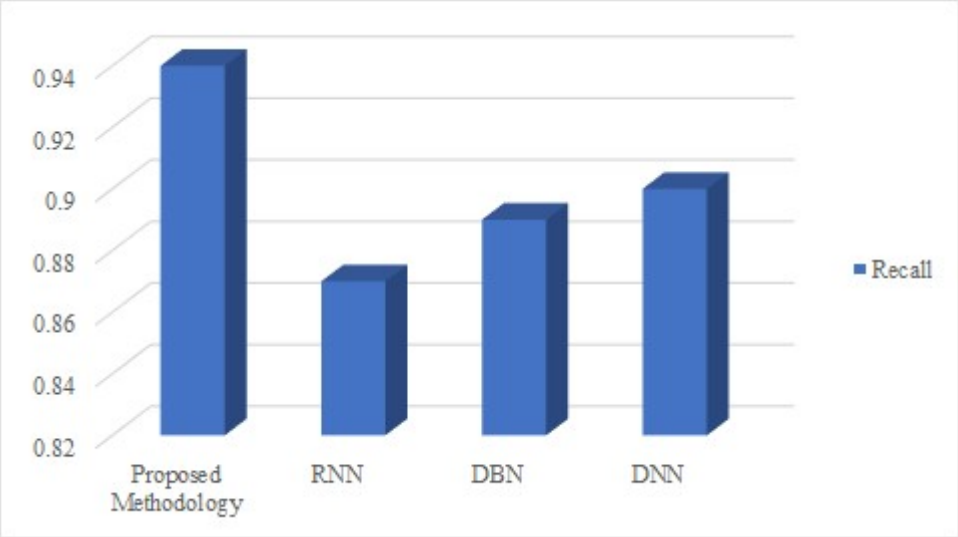

Figure 5: Recall of Proposed System

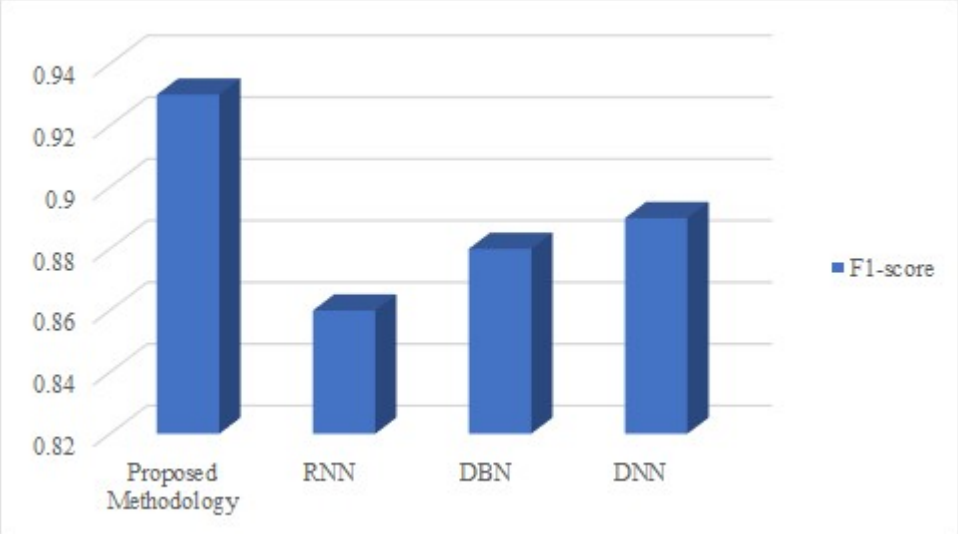

Figure 6: F1 Score of Proposed System

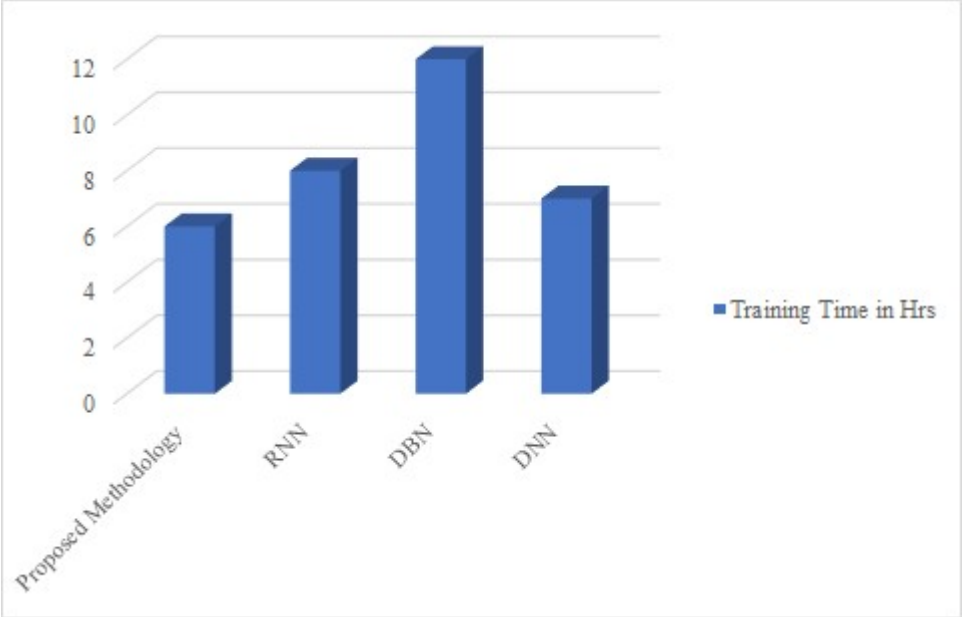

Figure 7: Training Time in Hrs of Proposed System

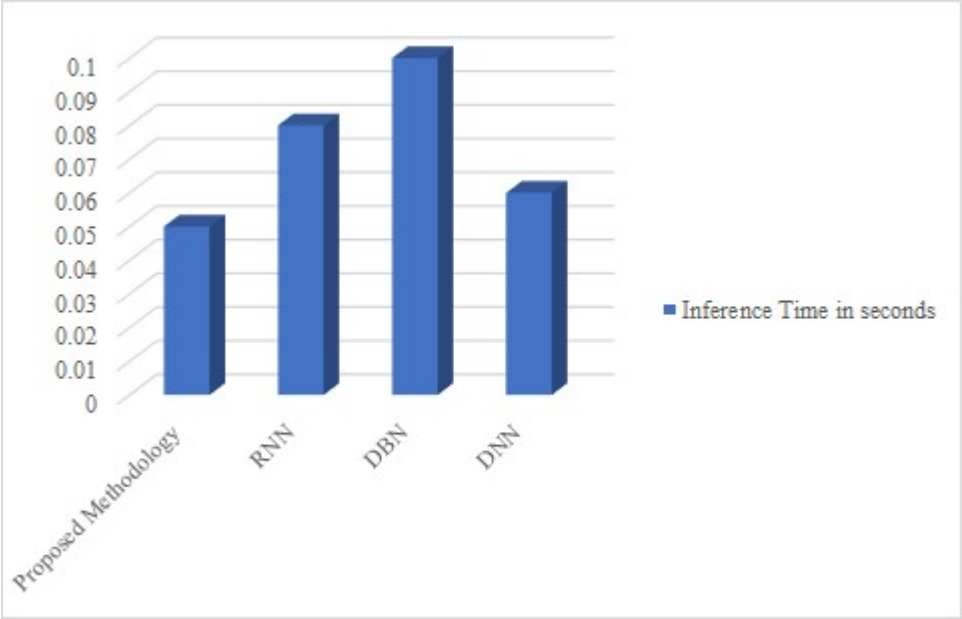

Figure 8: Training Time in Hrs of Proposed System

The results of the simulation and validation experiments suggest that the proposed methodology is effective in enhancing cybersecurity in the context of MCPS. Crucially, the proposed methodology indicates promising and accurate results concerning accuracy, Precision, recall, and F1-score for MCPS in detecting and combating cyber-attacks, underpinning the efficiency of the DCNN-based anomaly detection system coupled with quantum encryption. Further, the integration allows for the continuous monitoring of healthcare data. It contributes to the identification and timely response to other threats affecting the security of MCPS against cyber threats. However, occasionally, challenges such as false alarms and the difficulty of launching quantum encryption remain to be improved by further enhancement and optimization. However, based on the methodology, the conclusion is quite profound in explaining that it is high time MCPS strengthened cybersecurity using the help of the latest technologies. It proactively prevents cyber threats to a health facility and protects patients' privacy

and personal information. These challenges show that the field still needs more R&D to develop and implement cybersecurity strategies for the healthcare industry.

5. CONCLUSION

The proposed methodology shows how to construct a sound means of promoting cybersecurity in medical cyber-physical systems (MCPS). The methodology combines a DCNN-based anomaly detection system with quantum encryption efficiently and accurately to detect and prevent cyber-attacks while maintaining the privacy of health information. This makes real-time monitoring applications capable of detecting threats at an early stage, thereby improving protection against cyber threats. Studies for future work involve applying optimal architectural changes to the DCNN model, investigating other encryption paradigms that may address the mentioned complexity and scalability issues, and investigating actual setting implementations to confirm the viability of the proposed technique in various healthcare environments. All these lines of future research will help enhance cybersecurity in MCPS and patient privacy and confidentiality in healthcare systems.

References

1. Bi, Hongliang, Jiajia Liu, and Nei Kato. "Deep learning-based privacy preservation and data analytics for IoT enabled healthcare." IEEE Transactions on Industrial Informatics 18, no. 7 (2021): 4798-4807.
2. Ban, X.; Ding, M.; Liu, S.; Chen, C.; Zhang, J. A Survey on IoT Vulnerability Discovery. In Proceedings of the Network and System Security: 16th International Conference, NSS 2022, Denarau Island, Fiji, 9–12 December 2022; Springer: Cham, Switzerland, 2022; pp. 267–282.
3. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019, 6, 8182–8201.
4. Zhao, B.; Ji, S.; Lee, W.H.; Lin, C.; Weng, H.; Wu, J.; Zhou, P.; Fang, L.; Beyah, R. A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. IEEE Trans. Dependable Secur. Comput. 2022, 19, 1826–1840
5. Hossein, Koosha Mohammad, Mohammad Esmaeil Esmaeili, Tooska Dargahi, Ahmad Khonsari, and Mauro Conti. "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications." Computer Communications 180 (2021): 31-47.
6. Jayaram, Ramaprabha, and S. Prabakaran. "Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system." Egyptian Informatics Journal 22, no. 4 (2021): 401–410.
7. Wang, Zhenchen, Puja Myles, and Allan Tucker. "Generating and evaluating cross-sectional synthetic electronic healthcare data: preserving data utility and patient privacy." Computational Intelligence 37, no. 2 (2021): 819–851.
8. S. A. Haque, S. M. Aziz, and M. Rahman, “Review of Cyber-Physical System in Healthcare,” Int. J. Distrib. Sens. Networks, vol. 10, no. 4, p. 217415, Apr. 2014, doi: 10.1155/2014/217415.
9. A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez, “Sustainable securing of Medical Cyber-Physical Systems for the healthcare of the future,” Sustain. Comput. Informatics Syst., vol. 19, pp. 138–146, 2018, doi: https://doi.org/10.1016/j.suscom.2018.02.010.
10. Lee et al., "Challenges and Research Directions in Medical Cyber-Physical Systems,” Proc. IEEE, vol. 100, no. 1, pp. 75–90, 2012, doi: 10.1109/JPROC.2011.2165270.
11. R. Mitchell and I.-R. Chen, "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber-Physical Systems," IEEE Trans. Dependable Secur. Comput., vol. 12, no. 1, pp. 16–30, 2015, doi: 10.1109/TDSC.2014.2312327.
12. M. M. Nair, A. K. Tyagi, and R. Goyal, "Medical Cyber-Physical Systems and Its Issues," Procedia Comput. Sci., vol. 165, pp. 647–655, 2019, doi: https://doi.org/10.1016/j.procs.2020.01.059.
13. H. Qiu, M. Qiu, M. Liu, and G. Memmi, “Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0,” IEEE J. Biomed. Heal. Informatics, vol. 24, no. 9, pp. 2499–2505, 2020, doi: 10.1109/JBHI.2020.2973467.

14. Z. Fu, C. Guo, S. Ren, Y. Ou, and L. Sha, “Modeling and Integrating Human Interaction Assumptions in Medical Cyber-Physical System Design,” in 2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS), 2017, pp. 373–378, doi: 10.1109/CBMS.2017.50.
15. L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost-Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System," IEEE Trans. Emerg. Top. Comput., vol. 5, no. 1, pp. 108–119, 2017, doi: 10.1109/TETC.2015.2508382.
16. Y. Jiang, H. Song, R. Wang, M. Gu, J. Sun, and L. Sha, “Data-Centered Runtime Verification of Wireless Medical Cyber-Physical System,” IEEE Trans. Ind. Informatics, vol. 13, no. 4, pp. 1900–1909, 2017, doi: 10.1109/TII.2016.2573762.
17. Michala, Anna Lito, Hani Attar, and Ioannis Vourganas. "Secure data transfer and provenance for distributed healthcare." In Intelligent Healthcare: Infrastructure, Algorithms and Management, pp. 241-260. Singapore: Springer Nature Singapore, 2022.
18. Patil, Shubham Prashant. "Security vulnerability detection with enhanced privacy preservation for edge computing using hybrid machine learning approach." PhD diss., Dublin, National College of Ireland, 2022.
19. Singh, Moirangthem Biken, and Ajay Pratap. "BPFISH: Blockchain and Privacy-preserving FL Inspired Smart Healthcare." arXiv preprint arXiv:2207.11654 (2022).
20. Demirbaga, Umit, and Gagangeet Singh Aujla. "MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem." IEEE Transactions on Network and Service Management 19, no. 4 (2022): 3896-3907.
21. Aqueveque, Pablo, Britam Gómez, Patricia AH Williams, and Zheng Li. "A Novel Privacy Preservation and Quantification Methodology for Implementing Home-Care-Oriented Movement Analysis Systems." Sensors 22, no. 13 (2022): 4677.
22. Stephanie, Veronika, Ibrahim Khalil, Mohammed Atiquzzaman, and Xun Yi. "Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain." IEEE Transactions on Industrial Informatics (2022).
23. Shumba, Angela-Tafadzwa, Teodoro Montanaro, Ilaria Sergi, Luca Fachechi, Massimo De Vittorio, and Luigi Patrono. "Leveraging IOT-aware technologies and AI techniques for real-time critical healthcare applications." Sensors 22, no. 19 (2022): 7675.
24. Pelekoudas-Oikonomou, Filippos, Georgios Zachos, Maria Papaioannou, Marcus de Ree, José C. Ribeiro, Georgios Mantas, and Jonathan Rodriguez. "Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems." Sensors 22, no. 7 (2022): 2449.
25. Sujata, P., Takale, D. G., Tyagi, S., Bhalerao, S., Tiwari, M., & Dhanraj, J. A. (2024). New Perspectives, Challenges, and Advances in Data Fusion in Neuroimaging. Human Cancer Diagnosis and Detection Using Exascale Computing, 185, 185. https://doi.org/10.1002/9781394197705.ch11
26. Santhakumar, G., Takale, D. G., Tyagi, S., Anitha, R., Tiwari, M., & Dhanraj, J. A. (2024). Analysis of Multimodality Fusion of Medical Image Segmentation Employing Deep Learning. Human Cancer Diagnosis and Detection Using Exascale Computing, 171, 171. https://doi.org/10.1002/9781394197705.ch12
27. Takale, D. G., Mahalle, P. N., Sakhare, S. R., Gawali, P. P., Deshmukh, G., Khan, V., ... & Maral, V. B. (2023, August). Analysis of Clinical Decision Support System in Healthcare Industry Using Machine Learning Approach. In International Conference on ICT for Sustainable Development (pp. 571-587). Singapore: Springer Nature Singapore https://doi.org/10.1007/ 978-981-99-5652-4_51
28. V. Kumar Nassa, S. Kumar Satpathy, M. K. Pathak, D. G. Takale, S. Rawat and S. Rana, "A Comparative Analysis in Using Deep Learning Models Which Results in Efficient Image Data Augmentation," *2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, Dubai, United Arab Emirates, 2023, pp. 1–6, doi: 10.1109/ICCAKM58659.2023.10449622
29. Gawali, P.P., Mahalle, P.N., Shinde, G.R., Sable, N.P., Takale, D.G., Barot, J. (2023). Quantum Key Distribution and Blockchain-Based Secure Authentication in Medical Cyber-Physical Systems. In:

Fong, S., Dey, N., Joshi, A. (eds) ICT Analysis and Applications. ICT4SD 2023. Lecture Notes in Networks and Systems, vol 782. Springer, Singapore. https://doi.org/10.1007/978-981-99-6568-7_54

30. B. N, A. Kumar, P. Garg, D. L. Femilin Jana, D. G. Takale and N. Das, "A Comprehensive analysis of the Efficiency of Dynamic Spectrum Allocation Methods in Optical Fiber Communications," *2023 International Conference on Emerging Research in Computational Science (ICERCS)*, Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICERCS57948.2023.10433906
31. A. Begum, K. Karthikeyan, D. G. Takale, P. Bhambu, D. Yadav and S. Das, "Exploring the Benefits of AI for Content Retrieval," *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GenCon)*, Bangalore, India, 2023, pp. 1–6, doi: 10.1109/SMARTGENCON60755.2023.10442622
32. V. Sharma, Savita, R. Kavitha, G. Arun Francis, P. Chandrakala and D. G. Takale, "Applying Advanced Neural Network Architectures to Improve Extracting Effectiveness of Textual Information," *2023 2nd International Conference on Futuristic Technologies (INCOFT)*, Belagavi, Karnataka, India, 2023, pp. 1–6, doi: 10.1109/INCOFT60753.2023.10425425
33. Dattatray G. Takale et al.(2024). Advancements and Applications of Generative Artificial Intelligence, Journal of Information Technology and Sciences, 10(1), 20-27.
34. Kadam, S. U., Khan, V. N., Singh, A., Takale, D. G., & Galhe, D. S. (2022). Improve the performance of non-intrusive speech quality assessment using machine learning algorithms. NeuroQuantology, 20(10), 12937. https://doi.org/10.14704/nq.2022.20.10.NQ551254.
35. Takale, D. G., Gunjal, S. D., Khan, V. N., Raj, A., & Guja, S. N. (2022). Road accident prediction model using data mining techniques. NeuroQuantology, 20(16), 2904 https://doi.org/10.48047/NQ.2022.20.16.NQ880299
36. Bere, S. S., Shukla, G. P., Khan, V. N., Shah, A. M., & Takale, D. G. (2022). Analysis Of Student's Performance Prediction in Online Courses Using Machine Learning Algorithms. Neuroquantology, 20(12), 13
37. Raut, R., Borole, Y., Patil, S., Khan, V., & Takale, D. G. (2022). Skin Disease Classification Using Machine Learning Algorithms. NeuroQuantology, 20(10), 9624-9629 10.14704/nq.2022.20.10.NQ55940
38. Kadam, S. U., Khan, V. N., Singh, A., Takale, D. G., & Galhe, D. S. (2022). Improve the performance of non-intrusive speech quality assessment using machine learning algorithms. NeuroQuantology, 20(10), 12937
39. Takale, D. G. (2019). A review on implementing energy-efficient clustering protocol for wireless sensor network. J Emerg Technol Innov Res (JETIR), 6(1), 310-315
40. Takale, D. G. (2019). A review on quality of service aware routing protocols for wireless sensor networks. Int J Emerg Technol Innov Res, 6(1), 316-320
41. Takale, D. G. (2019). A Review on Wireless Sensor Network: Its Applications and Challenges. J Emerg Technol Innov Res (JETIR), 6(1), 222-226
42. Dattatray, M. T., & Amrit, M. P. (2014). A study of fault management algorithm and recovery of the faulty node using the FNR algorithms for wireless sensor network. International Journal of Engineering Research and General Science, 2(6), 590–595. http://www.ijergs.org/files/documents/A-STUDY-77.pdf
43. Takale, D. D., Sharma, D. Y. K., & SN, P. (2019). A review on data-centric routing for wireless sensor network. Journal of Emerging Technologies and Innovative Research (JETIR), 6(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4416491
44. Takale, D. D., & Khan, V. (2023). Machine learning techniques for routing in a wireless sensor network. International Journal of Research And Analytical Reviews, 10(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4394967