An Intelligent Quantum Cyber-Security Framework for Healthcare Data Management

Kishu Gupta, *Member, IEEE*, Deepika Saxena, *Member, IEEE*, Pooja Rani, Jitendra Kumar, *Senior Member, IEEE*, Aaisha Makkar, *Member, IEEE*, Ashutosh Kumar Singh, *Senior Member, IEEE*, and Chung-Nan Lee, *Member, IEEE*

***Abstract*— Digital healthcare is essential to facilitate consumers to access and disseminate their medical data easily for enhanced medical care services. However, the significant concern with digitalization across healthcare systems necessitates for a prompt, productive, and secure storage facility along with a vigorous communication strategy, to stimulate sensitive digital healthcare data sharing and proactive estimation of malicious entities. In this context, this paper introduces a comprehensive quantum-based framework to overwhelm the potential security and privacy issues for secure healthcare data management. It equips quantum encryption for the secured storage and dispersal of healthcare data over the shared cloud platform by employing quantum encryption. Also, the framework furnishes a quantum feed-forward neural network unit to examine the intention behind the data request before granting access, for proactive estimation of potential data breach. In this way, the proposed framework delivers overall healthcare data management by coupling the advanced and more competent quantum approach with machine learning to safeguard the data storage, access, and prediction of malicious entities in an automated manner. Thus, the proposed IQ-HDM leads to more cooperative and effective healthcare delivery and empowers individuals with adequate custody of their health data. The experimental evaluation and comparison of the proposed IQ-HDM framework with state-of-the-art methods outline a considerable improvement up to 67.6%, in tackling cyber threats related to healthcare data security.**

***Note to Practitioners*—This paper aims to address the issue of digital healthcare data access, which requires both ease and security. Existing research either focuses solely on safe access or on high security, which often comes with high computational challenges. In this paper, we present a comprehensive approach that takes into account various challenges such as secure data storage, efficient data communication, and the prediction of malicious entities. We have developed a mathematical system to portray the overall management of healthcare data. All techniques proposed in this paper have been implemented using quantum computing and have been tested on four healthcare datasets. Initial experimental results suggest that the proposed approach is feasible. Our techniques can be applied to discover malicious entities and understand the behavior of real-life users in healthcare processes.**

***Index Terms*— Automated healthcare data security, malicious entity prediction, quantum encryption, quantum feed forward neural network.**

I. Introduction

DIGITAL transformation of healthcare services allows access to healthcare facilities, across the globe even from far distant, remote, and strategic locations. Cloud computation serves as a base element to roll out this worldwide digital facility by offering outstanding services like storage, computation, investigations, analysis, etc. at a very nominal cost and with remarkable availability. This has attracted healthcare institutions to migrate their data accumulated from diverse medical IoT devices and sensors, over the cloud platform [1], [2], [3]. Cloud service platforms act as the backbone of digital health systems by enabling the digital retrieval of patient data and the extraction of valuable clinical information. As a result, various additional uses have become available, including quality management, healthcare administration, and trans-national research [4], [5]. The adoption of digital infrastructure by healthcare organizations can offer numerous advantages for consumers like doctors, patients, and healthcare services. However, apprehensions regarding the privacy and security of end consumer data is a major challenge across various healthcare institutions [6], [7]. These institutions are required to grant data access among multiple stakeholders, such as researchers, academia, doctors, patients, regulatory bodies,

Manuscript received 20 June 2024; accepted 4 September 2024. This article was recommended for publication by Associate Editor M.-H. Hung and Editor X. Xie upon evaluation of the reviewers' comments. This work was supported by the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan. *(Corresponding author: Deepika Saxena.)*

Kishu Gupta and Chung-Nan Lee are with the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan (e-mail: kishuguptares@gmail.com; cnlee@mail.cse.nsysu.edu.tw).

Deepika Saxena is with the School of Computer Science and Engineering, The University of Aizu, Aizuwakamatsu 965-0006, Japan (e-mail: deepika@u-aizu.ac.jp).

Pooja Rani is with the Department of Computer Applications, National Institute of Technology Kurukshetra, Kurukshetra 136119, India (e-mail: poojavats971993@gmail.com).

Jitendra Kumar is with the Department of Mathematics, Bioinformatics, and Computer Applications, Maulana Azad National Institute of Technology Bhopal, Bhopal 462003, India (e-mail: jitendrakumar@ieee.org).

Aaisha Makkar is with the College of Computer Science and Engineering, University of Derby, DE22 3AW Derby, U.K. (e-mail: a.makkar@derby.ac.uk).

Ashutosh Kumar Singh is with the Department of Computer Science and Engineering, Indian Institute of Information Technology Bhopal, Bhopal 462003, India, and also with the Department of Computer Science, University of Economics and Human Sciences, 01-043 Warsaw, Poland (e-mail: ashutosh@iiitbhopal.ac.in).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TASE.2024.3456209.

Digital Object Identifier 10.1109/TASE.2024.3456209

etc., for different usages [8], [9], [10], [11]. Sharing of this crucial and sensitive data in digital infrastructure is essential for medical growth, but it is highly susceptible to data breaches, security, and privacy issues. According to a survey, healthcare data breaches have consistently trended upward and doubled in the last three years [12]. Moreover, according to the Global Threat Report 2023, for more than 2500 adversaries there is a 112% increase in the cyber threat-related eCrimes, compared to 2021 [13]. Furthermore, a study highlights the privacy security concerns related to Electronic Health Records (EHRs) [14]. Any mal-intentional exposure of crucial medical data to some unauthorized party may induce direct financial loss, reputation damage, operational downtime, legal actions and massive harm to overall growth of the organization's [15], [16]. Thus, data breach outcomes are wide-ranging and extremely impactful. In this way, fortified data storage, reliable communication, edge security, and privacy appear as crucial challenges in shared cloud environments that must be handled properly. Proactive, healthcare data breach estimation emerges as a prominent way out of this problem. Several approaches [17], [18], [19], [20], [21] have been defined in this regard but these approaches detect data breaches after their occurrence. However, in a real environment, proactive computation of possible data breaches is the key to safeguarding healthcare confidential data security and privacy.

In this context, a novel **I**ntelligent **Q**uantum Cyber-Security Framework for **H**ealthcare **D**ata **M**anagement (**IQ-HDM**) framework is proposed to accomplish the comprehensive healthcare data management by equipping secure storage and communication to estimate the crucial healthcare data access intention for being 'malicious' or 'non-malicious' and identification of malicious entity, in case of data breach. To the best of author's knowledge, this is the first framework that concurrently addresses the aforementioned multiple data security issues by furnishing a *Quantum one-time padding encryption* (QOTPE) unit for secure data storage and *Quantum feed-forward neural network* (QFNN) based *quantum-protected healthcare data communication* (QPHDC) request analysis unit for proactive estimation of a mal-intentional entity. Thus, the proposed IQ-HDM framework establishes a comprehensive quantum-oriented security-embedded automated healthcare data management.

A. Related Work

The considerable works presented for preserving healthcare data security via privacy-preserving, encryption, and prediction approaches, a few acting in reactive and others in a proactive manner. Lim et al. [22] presented a more practical, scaleable, and easy-of-deploy solution to address the problem of privacy-preserving dataset integration using the concept of a prototype called PrivateLink without requiring key sharing among participants. Gupta and Kush [23] proposed a forecasting-based data leakage prevention (DLP) model to restrict data access permission to users by using a simple piece-wise linear function for model learning. This approach forecast possible guilty users based on past data access records of users. Rosa et al. [4] presented a small-form and battery-less implantable device with acquisition channels for bio-potential, arterial pulse oximetry, and temperature recordings with in-situ encryption of data. Though implantable devices are the future of the remote medical field but they suffer from data theft and spoofing. Data disclosure poses serious threats to data security. This concept lags in strict data security norms. Gupta et al. [18] proposed a novel model to support multiple participants to securely share their data for distinct purposes. The model defines the access policy and communication protocol among the involved multiple untrusted parties by utilizing encryption, machine learning, and probabilistic approaches. Xu et al. [19] presented a model to process the complex healthcare security event in real-time by analyzing the security performance, using an improved convolutional neural network (CNN) having a four-branch inception block to increase the width of the CNN while reducing the parameters.

Gupta et al. [24] proposed a novel quantum machine learning based malicious user prediction (QM-MUP) and privacy-preserving model. The proposed model preserves data privacy via the Laplace mechanism-based noise addition and uses Quantum Pauli gate-based Neural Network predictor to exploit the computational and behavioral properties of qubits. Sun et al. [25] proposed privacy-preserving bilateral fine-grained access control (PBAC-FG) which employs fine-grained access control and matchmaking encryption technologies to ensure participants can specify their respective fine-grained access control over the encrypted healthcare data. Thus allowing only authorized counterparts to access the healthcare data. Song et al. [26] proposed a cryptographic approach, controllable out-sourced attribute-based proxy re-encryption (COAB-PRE) enabling bilateral and distributed access control whereby data producers and data consumers can both specify policies the other party must satisfy without a centralized access control server along with supporting verifiability to find out a wrong result produced by the edge nodes and locate the misbehaved one. Chang et al. [27] proposed a universal quantum circuit (UQC) based scheme named DQFHE to deal with the volatility problem of the servers using a quantum environment. Gupta et al. [10] proposed a novel malicious user detection model by using the gradient boosting. Also, Gupta et al. [2] proposed a data security model to predict the malicious user in advance. It utilized the federated machine learning which incorporated data safety by making the learning at local user site without actually sharing data. Table I showcases the studied literature in a consolidated form.

The approaches discussed above assure data security, either using encryption to provide secure data access, prediction of malicious entities, or detection of guilty agents. Thus, existing work has presented data safety solutions for addressing a particular data security issue. Moreover, all these issues like secure data storage, data communication, and malicious entity prediction should be handled together, as these are diverse constituents of comprehensive data security. However, none of the existing work is sufficient to tackle the above-mentioned issues, concurrently considering these issues are different components of security. Unlike existing work, a comprehensive framework with a more potent, computational, and enhanced performance is proposed which addresses the limitation of

TABLE I
ENCAPSULATED VIEW OF RELATED STUDIES AND PROPOSED WORK

Contributor	Features			Strategy	Target
	$\mathbb{E}$	$\mathbb{P}$	$\mathbb{D}$		
Lim et al. [22]	✓	×	×	PP	Secure data sharing
Gupta et al. [23]	×	✓	×	Forecasting	Malicious party detection
Gupta et al. [18]	✓	×	✓	Probabilistic	Guilty user detection
Xu et al. [19]	×	✓	×	I-CNN	Healthcare security
Gupta et al. [24]	×	$✓^q$	×	QNN	Malicious user prediction
Sun et al. [25]	✓	×	×	PP	Unauthorized access control
Song et al. [26]	✓	×	×	ABE	Data access control
Chang et al. [27]	$✓^q$	×	×	HE, UQC	Server management issue
Gupta et al. [10]	×	×	✓	XG-Boost	Malicious user detection
Gupta et al. [2]	×	✓	×	Federated Learning	Malicious user prediction
IQ-HDM	$✓^q$	$✓^q$	$✓^q$	QOTPE, QFNN	Healthcare data management

$✓^q$: Quantum mechanics, $\mathbb{E}$: Encryption, $\mathbb{P}$: Prediction, $\mathbb{D}$: Detection, PP: Privacy preserving, ABE: Attribute based encryption, HE: Homomorphic encryption, UQC: Universal quantum circuits, QNN: Quantum neural network, I-CNN: Improvised convolutional neural network, QE: Quantum encryption, QFNN: Quantum feed-forward neural network.

the existing work to deliver data security. The proposed framework mitigates the malicious data request proactively to shield data from further breaches by utilizing the capability of QOTPE unit and QPHDC unit. Quantum-oriented data security approach is considered more robust, secure, and efficient because quantum deals with an infinite number of potential states along with zero and one state whereas classical considers either zero or one as the possible outcome states. Various quantum gate permits a rotational outcome in a 360° view that analyzes the input data deeply with numerous possible qubit states to generate possible outcomes from it and thus predicts the data breach more adequately.

B. Key Contributions

In light of the aforementioned approaches, the fivefold key contributions of this paper are discussed below.

1) A novel quantum driven IQ-HDM framework using the computational efficiency of *quantum encryption* and *quantum feed-forward neural network* approaches is designed to furnish end-to-end management of healthcare data ensuring secure data storage, efficient data communication, and prediction of malicious entities.
2) The *QOTPE* unit is designed that is responsible for encryption of data in the form of quantum states resulting in maximally mixed states, providing a perfect and unconditional security to the transmitted data.
3) A *QPHDC* unit incorporating pauliX, Hadamard quantum gates, and qubits is developed that eventually add more potency to data communication by allowing the secure sharing of data among various stakeholders.
4) The proposed framework strengthens data communication by proactively mitigating the hazardous data request intentions and recognizing the malicious entity to prevent further breaches.
5) A series of experiments are conducted utilizing the widely adopted four benchmark datasets that demonstrate the efficacy of the proposed end-to-end quantum-oriented approach for improving the security of electronic healthcare data management. The accomplished results are compared with the state-of-the-art works through diverse performance metrics.

TABLE II
NOMENCLATURE

$\mathbb{H}^a$	Healthcare agency	$\mathbb{DU}$	Data users
$\mathbb{T}^p$	Third party	$\mathbb{CSS}$	Cloud Service Supplier
m	Number of users	D^h	Healthcare data objects
$\mathbb{DSS}$	Data Storage Server	$\|\psi\rangle$	Quantum states
$\mathbb{R}_d$	Quantum superposition of bit strings	$\mathcal{DB}^{grand}$	Total number of data access
$\mathbb{R}_i$	Data access request	$\mathbb{DU}_i^\star$	Live details
$\mathbb{DU}_i^{\star\star}$	Historical details	ρ	Breach susceptibility
ξ	Eligibility parameters	$\mathcal{AU}$	Users' authenticity
$\mathcal{AD}$	Authorized data	$\mathcal{RF}$	Risk factor
t_{a*}, t_{b*}	Time-interval	ϕ	Past leakage status
$\mathcal{DB}^{mal}$	Malicious data breach	Π	Breach factor
α, β	Padding keys	$\Re$	Accuracy

C. Paper Outline

This article is structured as follows. Section I discusses introduction and related work with key contributions of the presented research work. Section II furnishes a detailed elaboration of the proposed IQ-HDM framework involving two units QOTPE and OPHDC, to ensure comprehensive data management as explained in Section II-B and Section II-C, respectively. The design and complexity of IQ-HDM are conferred in Section III. The performance evaluation followed by discussion remarks about the proposed work is presented in Section IV. The conclusive remarks and the future scope of the proposed work are outlined in Section V. Table II shows the list of symbols with explanatory terms used throughout this article.

II. IQ-HDM

This section describes the framework entities and their designated roles, and summarizes the workflow of IQ-HDM. The comprehensive architecture of the proposed framework is depicted in Fig. 1.

A. System Model

The system model comprises of four entities *healthcare agencies* ($\mathbb{H}^a$), *cloud service supplier* ($\mathbb{CSS}$), *data users* ($\mathbb{DU}$), and *third parties* ($\mathbb{T}^p$) which are defined as follows.

1) *Healthcare Agencies* ($\mathbb{H}^a$): An entity generating healthcare data using various Sensors and IoT devices. $\mathbb{H}^a$ treats $\mathbb{CSS}$ as trusted but is curious-to-know therefore it encrypts the data before transferring it for storage and sharing purposes. Moreover, $\mathbb{H}_i^a$ itself might not leak its data, but may leak the other $\mathbb{H}_j^a$'s data, therefore is considered an untrusted entity.
2) *Cloud Service Supplier* ($\mathbb{CSS}$): An entity that collects all the encrypted data from $\mathbb{H}_i^a$ to offer storage, computation for further sharing among $\mathbb{DU}$. $\mathbb{CSS}$ supports secure data communication and malicious entity estimation by deploying a QFNN based quantum-protected healthcare data communication unit (QPHDC).
3) *Data User* ($\mathbb{DU}$): An entity raising a request to $\mathbb{CSS}$ for grant of *healthcare data objects* (D^h) access required for different utility purposes and obtains quantum encrypted D^h along with the key. $\mathbb{DU}_i$ is considered a highly untrusted entity.
4) *Third Party* ($\mathbb{T}^p$): An unauthorized and untrusted entity that belongs indirectly to the system. $\mathbb{T}^p$ can access

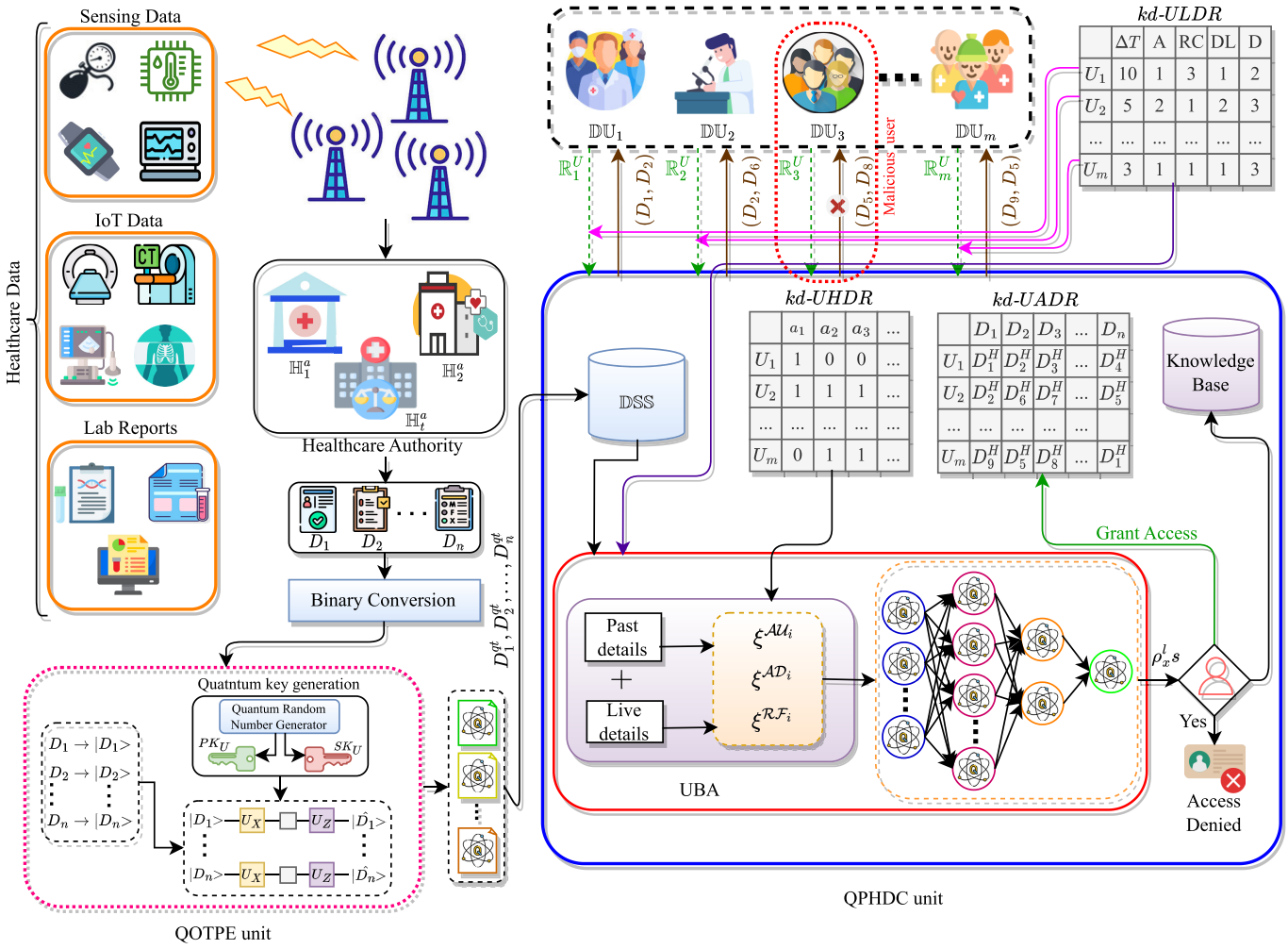

Fig. 1. Architecture of the proposed intelligent quantum oriented healthcare data management framework.

the relevant information from an malicious entity or by accessing D^h illegally from some authorized entity.

Considerable *healthcare agencies* $\mathbb{H}^a$ are accumulating crucial medical data from different sources such as sensor devices, IoT devices, and diagnosis reports, etc. as displayed in Fig. 1. $\mathbb{H}^a$, share *healthcare data objects* D_i^H with multiple *data users* $\mathbb{DU}_i$ utilizing data to deliver better medical services. Data sharing encounters the threat of safety, privacy, and breaches. The proposed framework considers entities $\mathbb{H}^a$, $\mathbb{DU}$, and $\mathbb{T}^p$ are untrusted and $\mathbb{CSS}$ is semi-trusted but curious-to-know entity. Specific challenges are described as follows.

- Lack of secure data storage at cloud premises due to the possibility of being misused by curious-to-know $\mathbb{CSS}$.
- Assessment of intention for data request before D_i^h is granted because $\mathbb{DU}_i$ might be mal-intentional.
- Proactive estimation of malicious user might responsible for unauthorized transmission of sensitive D_i^h to particular $\mathbb{T}^p$.

To ensure data security during transmission and to keep data hidden from curious-to-know cloud service supplier ($\mathbb{CSS}$), data owner $\mathbb{H}^a$ encrypts their respective data into some directly unreadable format by utilizing the QOTPE approach. Also, QFNN oriented QPHDC unit is employed for proactive estimation of potential breach and malicious entity by performing extensive analysis of each user for each data access request. The purpose of IQ-HDM is to anticipate an advanced, suitable quantum-driven solution for the overall management of crucial healthcare data which delivers secure storage, mitigates communication issues, and predicts malicious entity in case of data leakage by utilizing extremely powerful quantum approaches imparting high privacy, robust security and, mitigating the threats, to intensify the overall performance of the system.

B. Quantum Encryption for Outsourced Data

To make data secure before allowing its transmission to a shared cloud platform data is encrypted into some unreadable content by deploying the quantum one-time padding encryption (QOTPE) approach. The encrypted data is then stored at a cloud data storage server ($\mathbb{DSS}$) thus enabling highly secure data storage. It comprises following consecutive steps:

1) Encoding: In order to perform any quantum computations, the classical data needs to be converted to the quantum states, which is achieved through basis encoding in the proposed model. The classical

data is converted to the equivalent binary strings as$(D_1^H)_2 =, (D_2^H)_2 = b_0b_1b_{x-1}b_x, \cdots, (D_n^H)_2 = n_0n_1n_{x-1}n_x$, where $a, b, \cdots, n$ subscripts denote the individual binary digits for each data instance. Thereafter, each classical bit of data instance D_i^H is encoded as quantum state $|\psi_0^a\rangle|\psi_1^a\rangle \cdots |\psi_{x-1}^a\rangle|\psi_x^a\rangle, |\psi_0^b\rangle|\psi_1^b\rangle \cdots |\psi_{x-1}^b\rangle|\psi_x^b\rangle, \cdots, |\psi_0^n\rangle$ $|\psi_1^n\rangle \cdots |\psi_{x-1}^n\rangle|\psi_x^n\rangle$ by initializing corresponding quantum registers QR_i, $\forall i = 1, 2, \cdots, n$, defined in Eq. (1), along with application of Controlled-Not gate on required qubits, given in Eq. (2).

$$QR = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\} \tag{1}$$

$$\begin{aligned} U(|\psi_i\rangle) = {} & \text{CNOT}(|1\rangle, |\psi_i\rangle) \cdot |1\rangle\langle 1| \\ & + \text{Id}(|0\rangle, |\psi_i\rangle) \cdot |0\rangle\langle 0| \cdot |\psi_i\rangle \end{aligned} \tag{2}$$

where, $U(|\psi_i\rangle)$ denotes the application of unitary gate to the ith input data state $|\psi_i\rangle$. CNOT$(|1\rangle, |\psi_i\rangle)$ representing the application of CNOT gate to the target qubit $|\psi_i\rangle$ along with the control qubit $|1\rangle$. Id$(|0\rangle, |\psi\rangle)$ is the identity gate applied to the target qubit $|\psi_i\rangle$ and the control qubit $|0\rangle$. Furthermore, the projectors being applied over the states $|1\rangle$ and $|0\rangle$ are $|1\rangle\langle 1|$ and $|0\rangle\langle 0|$, respectively. The resultant quantum states $(|\psi_i\rangle)$ are capable of performing multiple computations simultaneously due to underlying quantum mechanical properties such as entanglement and superposition. A state vector with m number of qubits used for the precision and d number of samples, is represented as $m + [log(d)]$ and $x = (x_1, ..., x_d) \in \mathbb{R}_d$ denoted as quantum superposition of bit strings, in which each instance is a binary string formed using N bits for the basis encoding. Furthermore, for $x_i = (b_1, ..., b_j, ..., b_N)$ for $j = 1, ..., N$ with $b_j \in \{0, 1\}$, basis encoding is stated in Eq. (3).

$$|x\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |x_i\rangle \tag{3}$$

Following the encoding of classical data, in order to achieve a secure communication, the equivalent quantum states need to be encrypted before being transmitted to the cloud, which is accomplished by utilizing quantum one time padding as described in forthcoming subsection.

2) Encryption: The quantum-mechanical principles underlying in the quantum states establish the information-theoretical security of the quantum information. The quantum analogy of classical one time pad is quantum one time pad that is one of the most examined quantum encryption algorithms. The security of quantum information is established on the principles of quantum mechanics, which is information-theoretically-secure. QOTPE is amongst the most investigated techniques in quantum encryption [28]. For each quantum state $|\psi\rangle$, two randomly generated keys $\alpha, \beta \in \{0, 1\}^n$ are used for padding of original information. For secret-key quantum encryption, it is assumed that secret keys are known to both receiver and sender. This bit-wise quantum one time pad protocol can be represented as $X^\alpha = \otimes_{i=1}^n \sigma_x^{\alpha(i)}$ and $Z^\beta = \otimes_{i=1}^n \sigma_z^{\beta(i)}$, where σ is the operation performed over the given qubit. Corresponding to X^α, σ_x is applied to the bits at positions in the n-bit string α and analogously for Z^β, which leads to a maximally mixed state

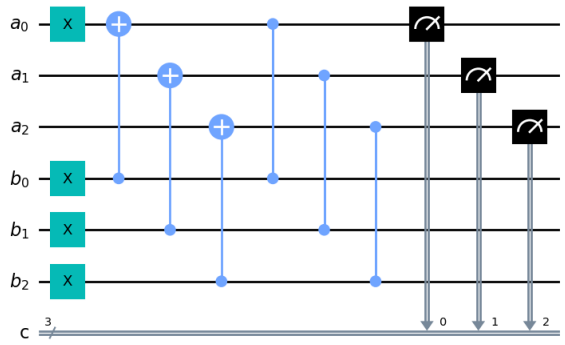

Fig. 2. Circuit for Quantum one time padding with 3 qubits.

that is completely unidentifiable for the attacker. The resultant encrypted state in generalized form can be rewritten as stated in Eq. (4).

$$\begin{aligned} Enc_\psi &= \otimes_{i=1}^n X^{\alpha_i} Z^{\beta_i} |\phi_i\rangle \\ &= X^{\alpha_1} Z^{\beta_1} \otimes X^{\alpha_2} Z^{\beta_2} \otimes \ldots \otimes X^{\alpha_n} Z^{\beta_n} \\ &\quad |\phi_1\rangle|\phi_2\rangle \ldots |\phi_n\rangle \end{aligned} \tag{4}$$

The circuit generated for quantum one time padding is provided in Fig. 2 which is tested using six qubits. It depicts the QOTPE circuit equivalent to Eq. (4) but the encryption keys are not presented in the circuit as the circuit is generated on the quantum computer; where encryption keys are being used in back-end. The maximally mixed states are retrieved after encryption and subsequently delivered to the cloud securely. Eq. (5) demonstrates the perfect security achieved by QOTPE, which is as follows:

$$\begin{aligned} \tilde{\rho} &= \sum_{k=1}^{M} p_k U_k \rho U_k^\dagger \\ &= \frac{1}{2^{2n}} \sum_{\alpha,\beta \in \{0,1\}^n} X^\alpha Z^\beta \rho (X^\alpha Z^\beta)^\dagger = \frac{I_{2^n}}{2^n} \end{aligned} \tag{5}$$

where ρ denoting the data quantum state and the maximally mixed state for n qubits is represented by $\frac{I_{2^n}}{2^n}$.

Security Proof: The most general scheme to form an encryption framework for any n-qubit system is to have a set of M operations $\{U_k\}, k = 1, 2, \ldots, M$, where each element U_k is a $2^n \times 2^n$ unitary matrix. Any random number being used as key k with probability p_k and each quantum state is encrypted through the corresponding unitary operation U_k. Subsequently, decryption is achieved through application of $U_k^\dagger$ to obtain the actual state. Considering ρ as the input state and $\tilde{\rho}$ is the equivalent encrypted state. In order to have the protocol to be informationally secure, every output state $\tilde{\rho}$ must be a maximally mixed state, corresponding to each input state ρ. Therefore, to prove the perfect security of the quantum one time pad protocol, we consider $p_k = 1/2^{2n}$ and $U_k = X^\alpha Z^\beta$, where $\alpha, \beta \in \{0, 1\}^n$. The inner product of two matrices M_1 and M_2 is defined as $Tr(M_1, M_2^\dagger)$. Furthermore, considering a set of $2^n \times 2^n$ matrices as an inner product space, it is trivially verifiable that the set of 2^{2n} unitary matrices $\{X^\alpha Z^\beta\}$ results in an orthonormal basis. If any input message

ρ is expanded in the $X^{\alpha}Z^{\beta}$ basis, is retrieved as in Eq. (6).

$$\rho = \sum_{\alpha,\beta} A_{\alpha,\beta} X^{\alpha} Z^{\beta}, \tag{6}$$

where, $A_{\alpha,\beta}$ is equivalent to $Tr(\rho Z^{\beta} X^{\alpha})/2^n$. Thereby, the perfect security for underlying protocol is given by satisfying maximally mixed state through Eq. (7).

$$\begin{aligned}\sum_{k=1}^{M} p_k U_k \rho U_k^{\dagger} &= \frac{1}{2^{2n}} \sum_{\zeta,\eta} X^{\zeta} Z^{\eta} \rho Z^{\eta} X^{\zeta} \\ &= \frac{1}{2^{2n}} \sum_{\alpha,\beta} A_{\alpha,\beta} \sum_{\zeta,\eta} X^{\zeta} Z^{\eta} X^{\alpha} Z^{\beta} Z^{\eta} X^{\zeta} \\ &= \frac{1}{2^{2n}} \sum_{\alpha,\beta} A_{\alpha,\beta} \sum_{\zeta,\eta} (-1)^{\alpha\eta \oplus \zeta\beta} X^{\alpha} Z^{\beta} \\ &= \sum_{\alpha,\beta} A_{\alpha,\beta} \eta_{\alpha,0} \eta_{\beta,0} X^{\alpha} Z^{\beta} \\ &= A_{0,0} I = \frac{Tr(\rho)}{2^n} = \frac{1}{2^n} I \end{aligned} \tag{7}$$

C. Quantum Prediction for Malicious Entities

Let us assume *m data users*: $\{\mathbb{DU}_1, \mathbb{DU}_2, \ldots, \mathbb{DU}_m\} \in \mathbb{DU}$ raises the request $\{\mathbb{R}_1, \mathbb{R}_2, \ldots, \mathbb{R}_m\}$ to achieve access for sensitive data D_i^h. Each $[\mathbb{R}_i : \langle D_i^h, \mathbb{DU}_i^{\star} \rangle]$ comprising details for required D_i^h and requesting user's current details such as type of data, amount of data, request channel etc. are provided to $\mathbb{CSS}$ for further analysis to determine the intention of user behind the data access request $\mathbb{R}_i$. $\mathbb{CSS}$ employs quantum feed forward neural-network (QFNN) based module to proactively determine possible malicious user by extensive analysis of live details $\mathbb{DU}_i^{\star}$ supplied with request from (*knowledge database-users' live details repository* (kd-ULDR) and historical details $\mathbb{DU}_i^{\star\star}$ such as leakage record, leakage channel etc. accessible from *knowledge database-users' historical details repository* (kd-UHDR). $\mathbb{DU}_i^h$ are considered to be {*known*, *unknown*, *mal-intentional*}.

1) User Behaviour Analysis: The user intention for being malicious or non-malicious, is evaluated prior to data access grant. Eqs. (8 and 9) assesses the breach susceptibility (ρ) of the $\mathbb{DU}_i$, established on basis of N^* user eligibility parameters ξ such as *users' authenticity* ($\mathcal{AU}$); *authorized data* ($\mathcal{AD}$); *risk factor* as computed in Eqs. (10-17).

$$\xi = \xi^{\mathcal{AU}_i} + \xi^{\mathcal{AD}_i} + \xi^{\mathcal{RF}_i} + \xi^{N^*} \tag{8}$$

$$\rho^{\mathbb{DU}_i} = \begin{cases} Non\text{-}malicious\ (1), & \text{If}(\xi < 1) \\ Malicious\ (0), & Otherwise \end{cases} \tag{9}$$

Users' authenticity ($\mathcal{AU}$): User is validated using Eq. (10) through login credential ($\mathbb{LC}$). Eq. (11) determine whether the user $\mathbb{DU}_i$ is 'existing' or 'new'.

$$\mathcal{AU}_i = \begin{cases} Authentic, & \text{If}(\mathbb{LC} \cup \mathbb{RA} = match) \\ Un\text{-}authentic, & Otherwise \end{cases} \tag{10}$$

$$\xi_i^{\mathcal{AU}} = \begin{cases} Existing\ (0), & \text{If}(|\Im_i| > 0) \\ New\ (1), & Otherwise \end{cases} \tag{11}$$

Authorised data ($\mathcal{AD}$): Every user is allowed to raise request $\Re_i$ as computed in Eq. (12) and Eq. (13), for predefined set of data ($\mathcal{AD}_i$) only, for example a patient can only access personal data, not the entire healthcare data. Here, $z_1, z_2, \ldots, z_{m^*}$ specifies the number of datasets from different medical categories: $w_1, w_2, \ldots, w_{m^*}$, respectively.

$$\begin{aligned}\mathcal{AD}_i = (w_1 \times \sum_{k=1}^{z_1} D_k) \cup (w_2 \times \sum_{k=1}^{z_2} D_k) \cup \\ \cdots \cup (w_{m^*} \times \sum_{k=1}^{z_{m^*}} D_k)\end{aligned} \tag{12}$$

$$\xi^{\mathcal{AD}_i} = \begin{cases} Legal\ (1), & \text{If}(\Re_i \times (w_i \times D_i) \subseteq \mathcal{AD}_i) \\ Illegal\ (0), & Otherwise \end{cases} \tag{13}$$

Risk factor ($\mathcal{RF}$): Suppose the associated user $\mathbb{DU}_i$ has demanded data $\{D_1^h, D_2^h, \ldots, D_n^h\}$ during time-interval $\{t_{a^*}, t_{b^*}\}$ and the status (ϕ) for any past leakage is stated in Eq. (14). The total number of $\mathcal{DB}^{mal}$ during this period is estimated using Eq. (15). The breach factor (Π) by u_i is computed using Eq. (16), where $\mathcal{DB}^{grand}$ is total number of data access over period $\{t_{a^*}, t_{b^*}\}$. The data breaches frequency is computed in Eq. (17) where $\sum_{k=1}^{H} Dz_k \notin \mathcal{AD}_i$ and t_{ijk} represents number of times u_i has endeavored to access unauthorized data (Dz_k) over j^{th} time-period. The term H and M stands for total number of unauthorized data requested by u_i during time duration M where, $M \in \{t_{a^*}, t_{b^*}\}$.

$$\phi_i = \begin{cases} True\ (1), & \text{If}(Breach = yes) \\ False\ (0), & Otherwise \end{cases} \tag{14}$$

$$\mathcal{DB}_i^{mal} = \sum_{i=1}^{z} (D_i \times \phi_i \times t) \quad \forall_t \in \{t_{a^*}, t_{b^*}\} \tag{15}$$

$$\int_{t_{a^*}}^{t_{b^*}} \Pi_i dt = \int_{t_{a^*}}^{t_{b^*}} \frac{\mathcal{DB}_i^{mal}}{\mathcal{DB}_i^{grand}} dt \tag{16}$$

$$\mathcal{FDB}_i^{mal} = |\sum_{k=1}^{H} \sum_{j=1}^{M} Dz_k \times t_{ijk} \times u_i| \tag{17}$$

Eq. (18) computes the risk factor ($\mathcal{RF}$) associated with a $\Re_i$ and Eq. (19) determines whether the data demand should allow utilizing cloud services for data access or not.

$$\mathcal{RF}_i = \Pi_i \times \mathcal{FDB}_i^{mal} \tag{18}$$

$$\xi^{\mathcal{RF}_i} = \begin{cases} insensitve\ (0), & \text{If}(Thr^{risk} > \mathcal{RF}_i) \\ sensitve\ (1), & Otherwise \end{cases} \tag{19}$$

2) Malicious Entity Prediction: Before the requested data is granted to $\mathbb{DU}_i$, a proactive analysis of the intention behind the request is performed to safeguard the communication. Only after being recognized as a legitimate user, requested data is granted to the authorized user and *users' allocated data repository* (kd-UADR) is updated, accordingly. As shown in Fig. 3 a *quantum feed-forward neural network* machine learning-based algorithm is employed to accomplish proactive estimation of the malicious user. The key idea of the QFNN-based QPHDC unit is to optimize the user's request parameters according to the cost function as illustrated in Eq. (21).

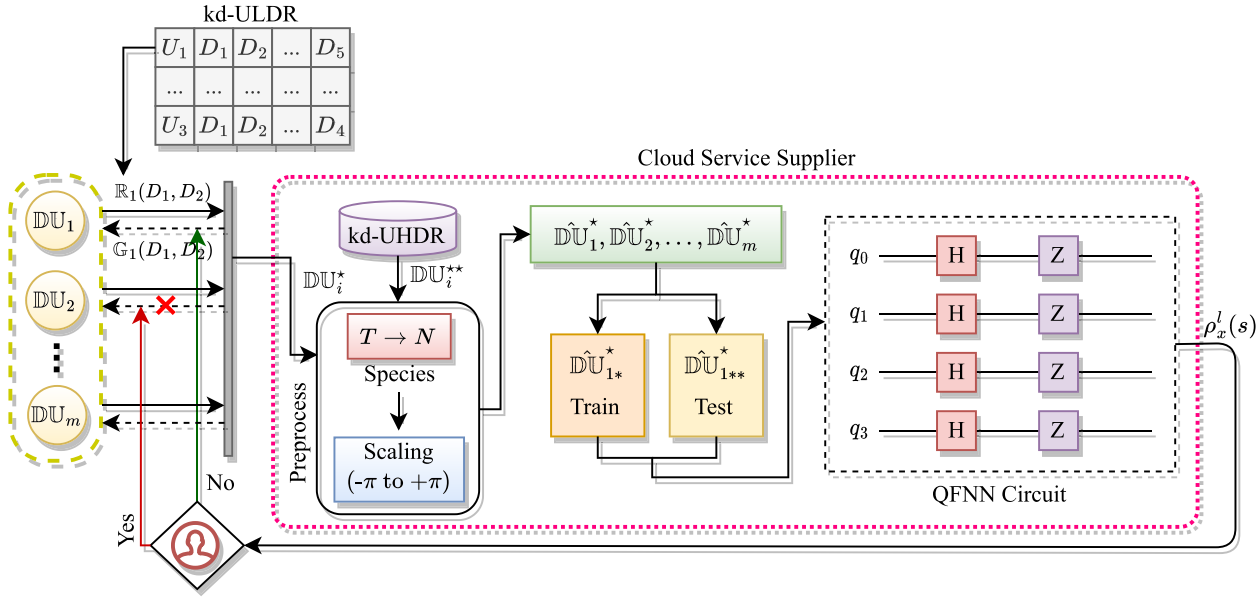

Fig. 3. QFNN based QPHDC to predict malicious entity for secure data communication.

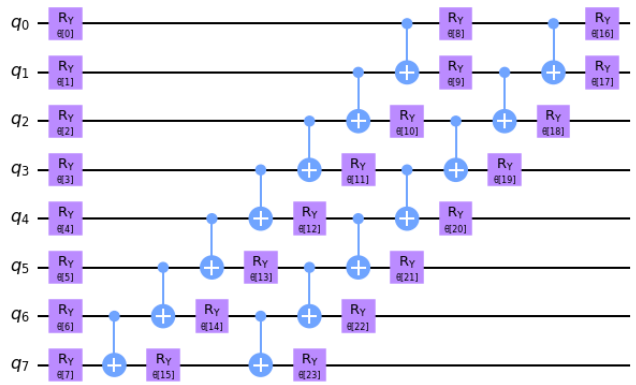

Fig. 4. Quantum circuit for qubit embedding.

Moreover, cost function assumes to be given training data and output states to compute the cost function as stated in Eqs. (20 and 21), respectively.

$$\begin{aligned} trainingData[x][1] &= |\phi_x^{out}\rangle \\ outputStates[x] &= |\rho_x^{out}(s)\rangle \end{aligned} \tag{20}$$

$$C(s) = \frac{1}{N}\sum_{x=1}^{N} |\phi_x^{out}\rangle \rho_x^{out}(s) \phi_x^{out} \tag{21}$$

QFNN architecture creates adjoint layer channel that can be described as a 4-tuple trainable quantum neural network like (QFNN architecture, unitaries, training Data, network unitary) as represented in Eq. (22). Fig. 4 is displaying the quantum circuit for qubit embedding in QFNN prediction unit.

$$\begin{aligned} \mathcal{F}_s^l(X^l) = tr_l\Big(&\big(\mathbb{1}_{l-1} \otimes 0\ldots 0_l 0\ldots 0\big) \\ &U^l(s)^\dagger \big(\mathbb{1}_{l-1} \otimes X^l\big) U^l(s) \Big) \\ = tr_l\Big(&\big(\mathbb{1}_{l-1} \otimes 0\ldots 0_l 0\ldots 0\big)\ U_1^l(s)^\dagger \ldots U_{m_l}^l(s)^\dagger \\ &\big(\mathbb{1}_{l-1} \otimes X^l\big) U_{m_l}^l(s) \ldots U_1^l(s) \Big) \end{aligned} \tag{22}$$

for input state $= X^l$.

Feed-forward neural network assumed to be given QFNN architecture, unitaries, and training data as usual, to carry out the malicious user estimation task as described in efficient learning for deep quantum neural networks in the following steps:

- For each element $\left[\phi_x^{in}, \phi_x^{out}\right]$ in training data do:
- Calculate the network input $\rho_x^{in} = \phi_x^{in}\phi_x^{in}$
- For every layer l in QFNN architecture do:
- Apply the layer channel $\mathcal{E}_s^l$ to the output of the previous layer $l-1$
- Store the result $\rho_x^l(s)$

The probability of cost Function returns the average as computed in Eq. (23).

$$\Pr(\tilde{m}(\Phi) \neq y | m(\Phi) = y) \approx \sigma\left(\sqrt{R}\frac{\frac{1-yb}{2} - \hat{p}_y}{\sqrt{2(1-\hat{p}_y)\hat{p}_y}}\right) \tag{23}$$

III. Operational Design and Complexity

Algorithm 1 imparts the operational summary of IQ-HDM, by utilizing the computational efficiency of quantum computing to provide shielded data storage and determines data breaches proactively for secure healthcare communications in the distributed cloud environment.

Time complexity: Steps (1)-(2) performs basic operations such as input the required datasets and initializes a data request, user details, and related attributes, consuming $\mathcal{O}(1)$ complexity, while steps (3)-(6) involves the encoding, encryption of crucial data before storage on shared data cloud platform, contributing complexity $\mathcal{O}(QE)$. The periodical training of QFNN predictor where the complexity depends

Algorithm 1 IQ-HDM: Operational Summary

Input: Knowledge databases including *User Historical Data Repository (kd-UHDR)* and *User Allocated Data Repository (kd-UADR)*;
Initialize: Data request, user details and related attributes ;
Perform Quantum Encryption, to shield the data in storage ;
for *each data object* $\{D^{\mathbb{H}_1^a}, D^{\mathbb{H}_2^a}, \ldots, D^{\mathbb{H}_p^a}\}$ **do**
    QE using *QOTPE* as computed in Eq. (4) ;
Periodical, training of *QPHDC* for secure communication ;
for *every data user* $\{\mathbb{DU}_1, \mathbb{DU}_2, \ldots, \mathbb{DU}_m\}$ **do**
    for *each data request* $(\{\mathbb{R}_1, \mathbb{R}_2, \ldots, \mathbb{R}_m\}$ *{1, 2, . . . , m} from respective data user* $(\mathbb{DU})$ **do**
        Examine the probable purpose of data request by *QFNN*- qubit measurement as computed in Eq. (21);
        if *malicious* **then**
            Request $\mathbb{R}_i$ leads to 'Data Breach';
        else
            Grant data access;

on the quantum gates and circuits rendering $\mathcal{O}(\tilde{Q})$. Steps (8)-(14) iterate for m users, wherein steps (9)-(15) replicate for m data request. Step 10 examines the probable purpose of data request by deploying QFNN-based QPHDC, to find the users' intentions for being malicious or non-malicious show complexity $\mathcal{O}(N^*)$. Steps (11)-(15) grant or deny healthcare data access depending upon the anticipated intention of the data request inducing $\mathcal{O}(1)$ complexity. Hence, the absolute complexity comes out to be $\mathcal{O}(n \times QE \times \tilde{Q} \times N^*) \Rightarrow \mathcal{O}(nQE\tilde{Q}N^*)$.

IV. Performance Evaluation

A. Experimental Setup and Implementation

The experimental work is carried out on a server machine encompassing two Intel® Xeon® Silver 4114 CPU with a 40 core processor and having 2.20 GHz clock speed. The simulation machine run on Ubuntu 16.04, an 64-bit LTS operating system comprising 128 GB of main memory RAM. Enactment of proposed work is carried out using Python 3.9. Moreover, IQ-HDM is simulated using the IBM Qiskit platform (version 0.43.0). The simulation is conducted on IBM QASM simulator and IBM quantum systems including IBM Nairobi (No. of qubits used-7), IBM Perth (No. of qubits used-5), selected on the basis of availability of the system along with most suitable parameters such as number of qubits supported by the system, quantum volume and number of jobs being queued. Also, QFNN to carry out prediction work employs Adam optimizer on two qubits and four qubits by utilizing Hadamard and CNOT quantum gates. However, due to execution constraints of available quantum computer instances and classical simulator, small chunks of dataset are used to run the experiments. Performance of framework under consideration, is examined through a dataset comprising of 10k agents live details alongwith ancient details. Major live details parameters are type of profession, number of requests from agent, type of requests from agent, and data limit for which data was accessed whereas the major ancient details parameters are ancient data of agents, leaked or never leaked data, how many times leaked the data, how frequently asking for data, and data retention. These agents all together are classified into three strictly different brackets which are non-malevolent, malevolent, and unknown. Moreover, framework assumes all the entities as non trusted to carry out execution task. The important primitives related to execution over quantum computer are listed in Table III.

TABLE III
Experimental Setup Parameters for the Quantum Computers Used and Their Values

Quantum Computer Used	IBM Perth	IBM Nairobi
Version	1.2.8	1.3.3
Number of Qubits	7	5,7
Quantum Register Size	7	7
Classical Register Size	2	3
Number of Shots	300	300
Execution Time on Quantum Computer	1.987 (s)	6.41 (s)
Total Execution Time	1h:14m:24s	0h:49m:42s

B. Datasets and Simulation Parameters

IQ-HDM is evaluated using different benchmark datasets available in public real workload datasets. For quantum encryption purposes, the following datasets are employed: 1) Covid-19 surveillance [29], 2) TCGA [30], and 3) Diabetes [31]. COVID-19 surveillance data categorizes the health details into three categories based on seven different health parameters. TCGA data is comprised of 839 instances with twenty-three features related to Gliomas, the most common primary tumors of the brain. This dataset considers, the most frequently mutated 20 genes and 3 clinical features from TCGA-LGG and TCGA-GBM brain glioma projects to determine whether a patient is LGG or GBM. Diabetes provides information gathered by monitoring sixteen health parameters such as Age, Gender, Polyuria, Polydipsia, Sudden weight loss, Weakness, Polyphagia, Genital thrush, Visual blurring, Itching, Irritability, Delayed healing, Partial paresis, Muscle stiffness, Alopecia, Obesity, for a set of 520 patients, to identify whether the patient diabetes is positive or negative. In this context, for malicious entity prediction by QFNN, an extended version of CMU CERT synthetic insider threat dataset r4.2 [32] is employed.

C. Computational Analysis

1) QOTPE Result: Statistical measurements of probabilities is an important metric to analyze the performance of a quantum-based algorithm, which forms a basis to access the randomness achieved in security keys along with encryption measurements. Fig. 5 represents the probability of each security key that depends on number of times the QRNG is executed on quantum computer and classical computer, that turns out to be almost equivalent for each key. This equivalent

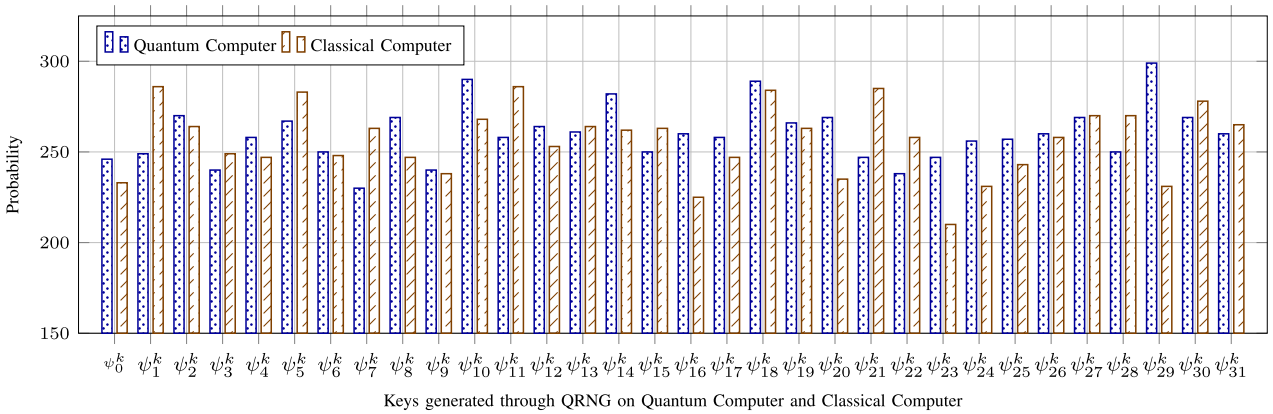

Fig. 5. Probability statistics for Key generation randomness on classical computer and classical computer.

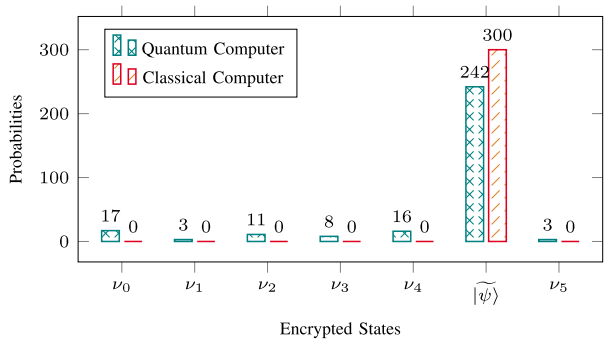

Fig. 6. Probability statistics of measurements for encrypted states on quantum computer and classical computer.

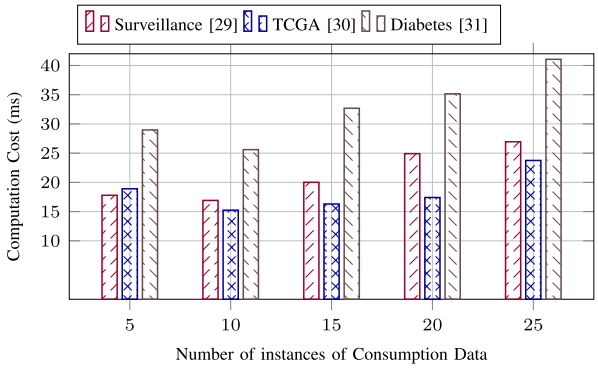

Fig. 7. Encryption cost with number of instances of DATA for diverse datasets.

comparability in their probability establishes the immunity of the encrypted data to outside attacks, while highly random keys will be more difficult to be estimated. The security keys are generated through the IBM qasm simulator and the IBM Perth quantum computer along with IBM nairobi, according to number of qubits supported.

Furthermore, Fig. 6 demonstrates the measurement performances for encryption over classical and quantum computer as well, where classical computer exhibits the precise measurements for the expected encrypted state. The quantum computer measures the expected encrypted state as maximum probable state accompanying few erroneous states (ν_0-ν_5) also. These error states exhibited by quantum computer is due to their fragility to external noise, decoherence and other factors impacting the qubit states.

Fig. 7 provides an analytical insight to quantum encryption cost with varying number of data instances, tested on three different datasets Covid-19 surveillance [29], TCGA [30], and Diabetes [31]. All three datasets incur a non-uniform computation cost while the Covid-19 surveillance dataset comes up with least encryption overhead and Diabetes dataset with the maximum encryption overhead.

2) Prediction Result: A coherent insight to quantum neural network driven prediction frameworks' loss parameter; over different number of epochs, in two different scenarios with two and four qubits, for dataset size 2k and 10k, respectively is depicted in Fig. 8. It is visible from figure that, framework is performing better with increase number of data instance as it can learn, significantly from a more informed data. Moreover, prediction unit performance is appearing better by reducing the loss value, with increased number of qubits due to deep computation with increase number of qubits.

D. Comparison

IQ-HDM is compared with existing state-of-the-art works like *Machine Learning and Probabilistic Analysis Based Model* (MLPAM) [18], *Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using an Improved CNN* (IoT-HSM) [19], *Quantum Machine Learning driven Malicious User Prediction Model* (QM-MUP) [24], *Malicious Agent Identification-based Data Security Model for cloud environments* (MAIDS) [10], and *Federated learning driven Malicious User Prediction Model for secure data distribution in cloud environments* (FedMUP) [2]. Brief details regarding these state-of-the-art works are already discussed in Section I-A.

Fig. 9 depict the comparison of the proposed framework's performance parameters; accuracy and data breach coverage with other state-of-the-art works by considering different data access request scenarios for {0.5k, 1.0k, 1.5k, Overall} requests, respectively. The accuracy of the proposed approach is having an edge over all the compared approaches for different request scenarios. High values of $\Cap$ show the improved performance in range between 3.13% to 16.13%. Hence, this is evident that the IQ-HDM is outperforming considered existing approaches and its performance is remarkably elevated due to

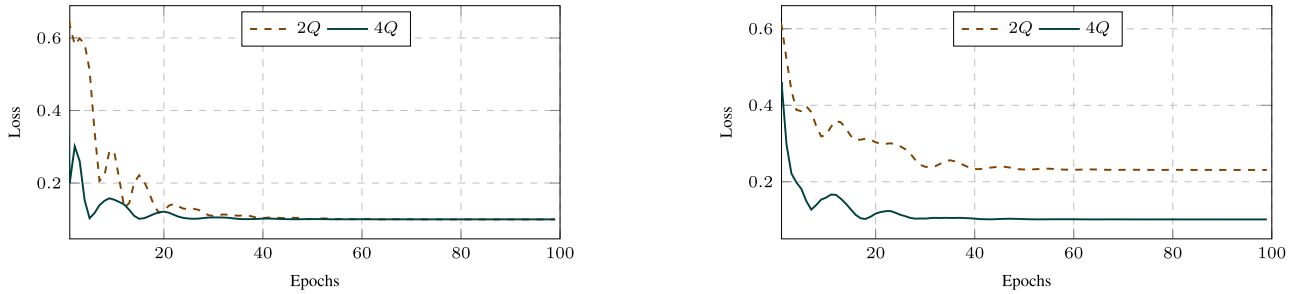

Fig. 8. Prediction loss values with Epochs = 100. (a) 2k (b) 10k.

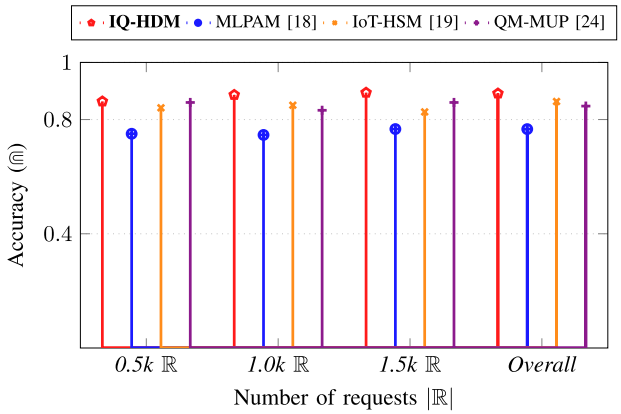

Fig. 9. Comparative analysis of accuracy with state-of-the-art approaches.

TABLE IV
FEATURE ANALYSIS: PROPOSED VS EXISTING MODELS

Models	$\mathbb{O}$	$\mathbb{SC}$	$\mathbb{SDS}$	$\mathbb{SDD}$	⋒	**Complexity**
MLPAM [18]	$\star$	×	√	√	76.65	$\mathcal{O}(\lvert\sum_{j=1}^{m} d_j\rvert)$
IoT-HSM [19]	$\star\star$	√	√	×	86.32	$\mathcal{O}(\lvert\sum_{j=1}^{m} d_j\rvert)$
QM-MUP [24]	×	√	√	√	84.71	$\mathcal{O}(tL\tilde{N}N^*)$
MAIDS [10]	×	√	×	√	86.75	$O(tmxyN)$
FedMUP [2]	×	√	×	√	87.24	$O(ntL\xi N^*)$
IQ-HDM	$\star\star$	√	√	√	89.02	$\mathcal{O}(nQE\tilde{Q}N^*)$

$\star$: Single; $\star\star$: Multiple, $\mathbb{O}$: IoT Devices, $\mathbb{SC}$: Secure Communication, $\mathbb{SDS}$: Secure Data Storage, $\mathbb{SDD}$: Secure Data Distribution, ⋒: Accuracy.

secure storage, communication, and prediction strategies in the proposed framework.

Table IV entails an absolute deviation among proposed IQ-HDM and existing models MLPAM, IoT-HSM, QM-MUP, MAIDS, and FedMUP by correlating different security features. It exhibits that IQ-HDM is the only framework to assume all entities not fully trusted. This means any of the entity can have mal-intentions and responsible for the data breaches. Also, it facilitates potent security and privacy features such as data storage, data communication and malicious prediction altogether delivers comprehensively secure communication and visionary breach prediction. The proposed quantum driven healthcare data management framework outperforms the state-of-the-art data security methods, and it is suitable to enhance the performance of breach prediction in a distributed environment. The reason for this enhanced performance of predicted values is the learning of useful information by using quantum values from input data samples.

After comprehensive evaluation of proposed work the enhancements in terms of quantum network security observed are that the proposed framework provisions an unconditional security through QOTPE and OPHDC by utilizing the quantum mechanical principles making it highly immune to classical and quantum computer attacks as well, unlike classical security mechanisms relying on computational hardness problems. Moreover, the sensitive data after being encrypted through QOTPE turns out to be maximally mixed states, that are completely unidentifiable by any adversary. Any measurements or alterations made by adversary can be detected trivially. Consequently, IQ-HDM stands ahead in all respects for supporting secure healthcare data access and cloud communication for overall data management.

E. Discussion

The results of this study showcase the effectiveness of the proposed approach. Extant literature reflects that none of the existing approaches alone is sufficient to impart healthcare data management. Accordingly, the study proposed a comprehensive framework to ensure all-round data management by utilizing the one of finest tools, quantum computing. The rationality to be motivated for the deployment of a quantum-oriented data security approach lies in the fact that quantum approaches are far superior to classical computing as quantum gate permits an infinite number of qubit states and rotational outcome in a 360° view for deep analysis to predict the data breach, efficiently. The quantum one-time padding encrypts the data before storage on the cloud and then the quantum malicious entity prediction unit analyses the user intention before allocating data. Hence, the study first fortified the crucial data and then checked for user intention. The significant impact of the study is in the successful implementation to deliver comprehensive healthcare data management.

V. CONCLUSION AND FUTURE WORK

Quantum oriented comprehensive data management framework is proposed to provide secure data storage, implementing data privacy and security policy with expanded digitalization of healthcare data. The IQ-HDM framework utilizes the QOTPE unit to enhance the quality of data-sharing needs and the QPHDC unit to strengthen data communication for proactive estimation of the malicious entity. In this way, the framework furnishes a more nuanced and contextually relevant approach in the context of healthcare data security.

Also, extensive experimental work has been conducted to demonstrate the effectiveness of the proposed methodology in real-world scenarios, contributing insights into the application of these criteria in the healthcare domain. This ensures that the proposed work goes beyond mere theoretical alignment with established practices, offering a substantively practical contribution to the field.

In the future, the IQ-HDM framework can be extended to develop an advanced, robust, and effective mechanism to enhance its capability of detecting the malicious entity, in case crucial data got disclosed intentionally or non-intentionally. Additionally, quantum-based transfer learning can be utilized to improve the proposed framework by making it capable of countering unknown types of cyber attacks.

REFERENCES

[1] B. Shen, W. Xie, and Z. J. Kong, "Clustered discriminant regression for high-dimensional data feature extraction and its applications in healthcare and additive manufacturing," *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 4, pp. 1998–2010, Oct. 2021.

[2] K. Gupta, D. Saxena, R. Gupta, J. Kumar, and A. K. Singh, "FedMUP: Federated learning driven malicious user prediction model for secure data distribution in cloud environments," *Appl. Soft Comput.*, vol. 157, May 2024, Art. no. 111519. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S156849462400293X

[3] K. Gupta and A. Kush, "A learning oriented DLP system based on classification model," *INFOCOMP J. Comput. Sci.*, vol. 19, no. 2, pp. 98–108, 2020. [Online]. Available: https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/1008

[4] B. M. G. Rosa, S. Anastasova, and G. Z. Yang, "NFC-powered implantable device for on-body parameters monitoring with secure data exchange link to a medical blockchain type of network," *IEEE Trans. Cybern.*, vol. 53, no. 1, pp. 31–43, Jan. 2023.

[5] D. Saxena, R. Gupta, A. K. Singh, and A. V. Vasilakos, "Emerging VM threat prediction and dynamic workload estimation for secure resource management in industrial clouds," *IEEE Trans. Autom. Sci. Eng.*, early access, Oct. 4, 2023, doi: 10.1109/TASE.2023.3319373.

[6] S. Pan, Y. Zhang, and S. Wang, "A secure aggregate authentication scheme with efficient revocation for IoT-based primary healthcare service," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6480–6491, Dec. 2023.

[7] Q. Fan, D. He, J. Chen, C. Peng, and L. Wang, "Isoga: An isogeny-based quantum-resist searchable encryption scheme against keyword guessing attacks," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2101–2112, Jul. 2022.

[8] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, and Y. Xiang, "Data-driven cyber security in perspective—Intelligent traffic analysis," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3081–3093, Jul. 2020.

[9] V. Mishra, K. Gupta, D. Saxena, and A. K. Singh, "A global medical data security and privacy preserving standards identification framework for electronic healthcare consumers," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4379–4387, Feb. 2024.

[10] K. Gupta, D. Saxena, R. Gupta, and A. K. Singh, "MAIDS: Malicious agent identification-based data security model for cloud environments," *Cluster Comput.*, vol. 27, no. 5, pp. 6167–6184, Aug. 2024, doi: 10.1007/s10586-023-04263-9.

[11] C. Hou, C. Zhou, C.-G. Wu, R. Cong, and K. Li, "Optimization of cloud-based multi-agent system for trade-off between trustworthiness of data and cost of data usage," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 1, pp. 106–122, Nov. 2004.

[12] (2023). *2022 Healthcare Cybersecurity Year in Review, and a 2023 Look Ahead*. [Online]. Available: https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

[13] G. Kurtz. (2023). *2023 Global Threat Report*. [Online]. Available: https://www.crowdstrike.com/global-threat-report/

[14] V. Mishra and M. Mishra, "Privacy and security concerns with electronic health records- shreds of evidence from India," *IMI Konnect*, vol. 11, no. 3, pp. 41–54, Sep. 2022.

[15] S. Sarkar, S. Chatterjee, S. Misra, and R. Kudupudi, "Privacy-aware blind cloud framework for advanced healthcare," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2492–2495, Nov. 2017.

[16] Z. Zhao, Y. Huang, Z. Zhen, and Y. Li, "Data-driven false data-injection attack design and detection in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 51, no. 12, pp. 6179–6187, Dec. 2021.

[17] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 1, pp. 51–63, Jan. 2011.

[18] I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, "MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4248–4259, Sep. 2021.

[19] L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent security performance prediction for IoT-enabled healthcare networks using an improved CNN," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2063–2074, Mar. 2022.

[20] H. Wu, B. Zhou, and C. Zhang, "Secure distributed estimation against data integrity attacks in Internet-of-Things systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 19, no. 3, pp. 2552–2565, Jul. 2022.

[21] M. Zhang, J. Zhou, P. Cong, G. Zhang, C. Zhuo, and S. Hu, "LIAS: A lightweight incentive authentication scheme for forensic services in IoV," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 2, pp. 805–820, Apr. 2023.

[22] H. W. Lim, G. S. Poh, J. Xu, and V. Chittawar, "PrivateLink: Privacy-preserving integration and sharing of datasets," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 564–577, 2020.

[23] K. Gupta and A. Kush, "A forecasting-based DLP approach for data security," in *Data Analytics and Management*, A. Khanna, D. Gupta, Z. Pólkowski, S. Bhattacharyya, and O. Castillo, Eds., Singapore: Springer, Jan. 2021, pp. 1–8.

[24] R. Gupta, D. Saxena, I. Gupta, A. Makkar, and A. K. Singh, "Quantum machine learning driven malicious user prediction for cloud network communications," *IEEE Netw. Lett.*, vol. 4, no. 4, pp. 174–178, Dec. 2022.

[25] J. Sun, Y. Yuan, M. Tang, X. Cheng, X. Nie, and M. U. Aftab, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6483–6493, Sep. 2022.

[26] Z. Song, H. Ma, R. Zhang, W. Xu, and J. Li, "Everything under control: Secure data sharing mechanism for cloud-edge computing," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2234–2249, 2023.

[27] W. Chang, Z.-Z. Li, F.-C. You, and X.-B. Pan, "Dynamic quantum fully homomorphic encryption scheme based on universal quantum circuit," *J. Inf. Secur. Appl.*, vol. 75, Jun. 2023, Art. no. 103510. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212623000947

[28] C. Cheng, Y. Qin, R. Lu, T. Jiang, and T. Takagi, "Batten down the hatches: Securing neighborhood area networks of smart grid in the quantum era," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6386–6395, Nov. 2019.

[29] *COVID-19 Surveillance*, UCI Machine Learning Repository, Irvine, CA, USA, 2020, doi: 10.24432/C5TC85.

[30] C. K. K. A. V. Tasci, Erdal, and Y. Zhuge, *Glioma Grading Clinical and Mutation Features*. Irvine, CA, USA: UCI Machine Learning Repository, 2022, doi: 10.24432/C5R62J.

[31] *Early Stage Diabetes Risk Prediction Dataset*, UCI Machine Learning Repository, Irvine, CA, USA, 2020, doi: 10.24432/C5VG8H.

[32] (Jan. 27, 2021). *Software Engineering Institute, Carnegie Mellon University. [n. d.]. Insider Threat Test Dataset*. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099

Kishu Gupta (Member, IEEE) received Ph.D. degree form India in 2023. She is currently a Post-Doctoral Research Fellow with the Cloud Computing Research Center, Department of Computer Science and Engineering, National Sun Yat-sen University (NSYSU), Kaohsiung, Taiwan. Her research interests include data security and privacy, cloud computing, traffic management, federated learning, machine learning, neural networks, and quantum machine learning. She has research findings published with top-notch venues, such as IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, *Applied Soft Computing*, and *Cluster Computing*. She was a recipient of the Gold Medal for securing first rank in overall university during the M.Sc. degree (computer science). She received the prestigious INSPIRE Fellowship sponsored by the Department of Science and Technology (DST) under the Ministry of Science and Technology, Government of India, for her Ph.D. degree.

Deepika Saxena (Member, IEEE) received the Ph.D. degree in computer science from the National Institute of Technology, Kurukshetra, India. She was a Post-Doctoral Research Fellow with the Department of Computer Science, Goethe University, Frankfurt, Germany. She is currently an Associate Professor with the Division of Information Systems, The University of Aizu, Japan. Also, she is an Online Lecturer with the University of Economics and Human Sciences, Warsaw, Poland, Europe. Her research interests include neural networks, evolutionary algorithms, resource management and security in cloud computing, internet traffic management, quantum machine learning, data lakes, and dynamic caching management. She was a recipient of the prestigious IEEE TCSC 2023 Outstanding Ph.D. Dissertation Award and the EUROSIM 2023 Best Ph.D. Thesis Award. She received the 2022 Best Paper Award for her research article published in IEEE TRANSACTIONS ON CLOUD COMPUTING JOURNAL. Also, she is the recipient of the prestigious Japan Society for the Promotion of Science (JSPS) KAKENHI Early Career Young Scientist Research Grant FY2024.

Pooja Rani received the M.Sc. degree from the Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India. She is currently pursuing the Ph.D. degree with the Department of Computer Applications, National Institute of Technology, Kurukshetra. Her research interests include data security and demand-response management in smart grids, predictive analytics, quantum computing, and cloud computing.

Jitendra Kumar (Senior Member, IEEE) received the Ph.D. degree in machine learning and cloud computing from the National Institute of Technology Kurukshetra, India, in 2019. He is currently an Assistant Professor with the Department of Mathematics, Bioinformatics, and Computer Applications, Maulana Azad National Institute of Technology Bhopal, India. His research interests include cloud computing, computational intelligence, time series forecasting, and optimization.

Aaisha Makkar (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Technology, Patiala, India. She was a Post-Doctoral (Research) Professor with the Department of Computer Science, Seoul National University of Science and Technology, South Korea. She is currently a Lecturer of computer science with the College of Science and Engineering, University of Derby, U.K. Her current research interests include cloud computing, machine learning, data analytics, and parallel processing.

Ashutosh Kumar Singh (Senior Member, IEEE) received the Ph.D. degree in electronics engineering from Indian Institute of Technology (BHU) Varanasi, India. He was a Post-Doctoral Researcher with the Department of Computer Science, University of Bristol, U.K. He is currently a Professor and the Director of Indian Institute of Information Technology Bhopal, India. Also, he is an Adjunct Professor with the University of Economics and Human Sciences, Warsaw, Poland. He has research and teaching experience in various universities in India, the U.K., and Malaysia. He has published more than 400 research papers in different journals and conferences of high repute. Some of his research findings are published in top cited journals, such as IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE COMMUNICATIONS LETTERS, IEEE NETWORKING LETTERS, IEEE DESIGN AND TEST, IEEE SYSTEMS JOURNAL, IEEE WIRELESS COMMUNICATION LETTERS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, *IET Electronics Letters*, FGCS, *Neurocomputing*, *Information Sciences*, and *Information Processing Letters*. His research interests include the design and testing of digital circuits, data science, cloud computing, machine learning, and security. His research paper, published in IEEE TRANSACTIONS ON CLOUD COMPUTING JOURNAL was honored with the 2022 Best Paper Award by the IEEE Computer Society Publications Board.

Chung-Nan Lee (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 1980 and 1982, respectively, and the Ph.D. degree in electrical engineering from the University of Washington, Seattle, WA, USA, in 1992. Since 1992, he has been with National Sun Yat-sen University, Kaohsiung, Taiwan, where he was the Chairperson of the Department of Computer Science and Engineering from 1999 to 2001. Currently, he is a Distinguished Professor and the Director of the Cloud Computing Research Center. His research interests include multimedia over wireless networks, cloud computing, and the IoT. He was the President of the Taiwan Association of Cloud Computing from 2015 to 2017 and the VP for TA of Asia–Pacific Signal and Information Processing Association from 2019 to 2020. In 2016, he received the Outstanding Engineering Professor Award from Chinese Institute of Engineers, Taiwan.