Homomorphic Encryption for Privacy-Preserving Data Sharing with IOTA and IPFS in IoT-based Medical Cyber-Physical Systems

Sivaranjani Reddi, Patruni Muralidhara Rao, Pedada Saraswathi, Basudeb Bera, Ashok Kumar Das, Biplab Sikdar

***Abstract*—The recent rise in cyber-attacks has jeopardized the protection and secrecy of data in Medical Cyber-Physical Systems (MCPS). Existing encryption methods prioritize system architecture over end-user concerns, necessitating innovative data management approaches. In this article, we develop a decentralized patient health data-sharing system using IOTA tangle and Inter Planetary File System (IPFS) technologies. Our method employs Brakerski/Fan-Vercauteren (BFV) homomorphic encryption and fragmentation and dispersion techniques to store and share data securely. This ensures data privacy even if the transmission media and cryptographic keys are compromised. Emphasizing a patient-centric approach, our design places data protection on the end user's trusted device, like a smartphone, granting users control over data access and sharing, thus bolstering overall MCPS security.**

***Index Terms*—Medical Cyber-Physical Systems (MCPS), Internet of Things (IoT), Healthcare, Homomorphic encryption, Security and Privacy.**

I. Introduction

Healthcare applications store sensitive user information on medical servers and execute computational tasks to aid various patient diagnoses. The increasing frequency of cyber-attacks targeting hospital systems leads to the extortion of user data [1]. Additionally, mathematical computations performed on cloud-stored data are vulnerable to exploitation by external entities lacking trustworthiness, who exploit the sale of confidential data for monetary profit. The mobile electronic health (e-health) system, supported by cloud technology, facilitates the sharing of electronic health data between healthcare providers and patients. However, this raises concerns about security and privacy related to the e-health data. Despite these concerns, sharing Electronic Health Records (EHRs) is crucial for efficient healthcare delivery within Medical Cyber-Physical Systems (MCPS). The increasing interconnectivity of healthcare systems enhances the patient outcomes through the real-time monitoring as well as advanced analytics. However, at the same time, it also raises concerns about the security, privacy, and integrity of sensitive medical data across various decentralized networks. Homomorphic encryption on the other hand offers a promising solution by allowing computations on encrypted data without revealing the underlying information, and thus, it ensures the privacy throughout the data's lifecycle. Integrating homomorphic encryption with decentralized technologies like IOTA's Tangle architecture and IPFS helps in achieving secure, scalable, and efficient data sharing. Moreover, this approach ensures data integrity and compliance with healthcare regulations in a decentralized healthcare ecosystem. This article proposes a robust framework integrating IOTA, Inter Planetary File System (IPFS), and Brakerski/Fan-Vercauteren (BFV) homomorphic encryption to facilitate secure EHR sharing in MCPS.

MCPS integrates smart medical devices, software, and networking, revolutionizing healthcare capabilities. Despite these advancements, EHR sharing faces data privacy, integrity, and interoperability obstacles. Various approaches have been proposed, such as Attribute-Based Encryption (ABE) [2], adversarial ML-based cloud architecture [3], differential privacy techniques [1], and so on. Most cannot achieve the desired security for sharing medical cyber-physical system data. Addressing these challenges necessitates innovative solutions. Therefore, Fully Homomorphic Encryption (FHE) can serve as a counterpart, enabling individuals to manage data access through end-to-end encryption while utilizing FHE for data analysis. Moreover, the cost of data transfer limits the free flow of information. Advanced data management systems offer various solutions, including Distributed Ledger Technologies (DLT) like blockchain [4] and Directed Acyclic Graph (DAG). IOTA, a DAG-based protocol, addresses blockchain limitations in its early stages. The Inter Planetary File System (IPFS) supplements DLT protocols for effectively managing large-scale data, leveraging content-addressing and peer-to-peer networking.

This study focuses on enhancing privacy protection while improving data access for healthcare institutions. The proposed architecture allows individuals to manage their Personal Health

Sivaranjani Reddi is with the Department of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, 531 162, India (e-mail: sivaranjani.reddi@raghuenggcollege.in).

Patruni Muralidhara Rao is with the School of Technology, Woxsen University, Hyderabad 502 345, India, and also with the Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam 530 048, India (e-mail: muralidhar.patruni@woxsen.edu.in).

Saraswathi Pedada is with the Department of Computer Science and Engineering, GITAM School of Technology, GITAM Visakhapatnam, 530 045, India (e-mail: spedada@gitam.edu).

Basudeb Bera and Biplab Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: b.bera26@nus.edu.sg, bsikdar@nus.edu.sg).

Ashok Kumar Das is with the Center for Security, Theory and Algorithms Research, International Institute of Information Technology, Hyderabad 500 032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in). *(Corresponding author: Ashok Kumar Das).*

Records (PHRs) through a Decentralized System (DS), where encrypted PHR data is stored using individual encryption keys. The study presents a comprehensive framework for secure Electronic Health Record (EHR) sharing within Medical Cyber-Physical Systems (MCPS), utilizing IOTA, IPFS, and BFV homomorphic encryption. By harnessing these technologies, the framework fosters patient-centered healthcare delivery while ensuring the confidentiality and integrity of medical records.

The paper is organized as follows. Section II provides a review of the existing literature on EHR sharing, while Section III explains the preliminaries. Section IV details the proposed methodology. Section V focuses on the security analysis, followed by Section VI, which presents the experimentation results and performance evaluation. Finally, Section VII offers the conclusions.

II. Background and Related Work

Numerous auditing solutions, effective for Public Key Infrastructure (PKI), rely on certificate-based systems, incurring additional certificate administration expenses. Consequently, such schemes fail to support cloud-based MCPS as they necessitate bilinear-pairing schemes for auditing by Third Party Auditors (TPAs). Shabisha et al. [5] proposed a pairing-based encryption technique for storing data in the cloud. However, real-time applications do not employ this method. Conversely, cloud-assisted data warehouses can accommodate vast medical records, emphasizing data integrity. Zhang et al. [6] proposed an identity-based mechanism called Distributed Public Integrity Verification (DOPIV) for cloud storage. In this case, the DOPIV permits the original owner to create and outsource signatures to the cloud while enabling the legitimate proxy. They also guaranteed that their approach maintains identity-based systems while avoiding complicated certificate management procedures. However, assessing remote physical access and processes is challenging for most cyber-physical systems [7]. A deep Q-network is used by Leong et al. [8] to propose a Markov Decision Process (MDP) that securely determines how to convey numerous states of remote and changing processes. They also ensured that their model could function online.

Nguyen et al. [9] proposed BEdgeHealth, a decentralized health architecture that combines Mobile Edge Computing (MEC) and blockchain technology to facilitate data offloading and sharing within distributed hospital networks. This approach includes a data offloading scheme that enables mobile devices to transfer health data to nearby MEC servers for efficient computation while maintaining privacy. Salim et al. [10] introduced a privacy-preserving scheme utilizing homomorphic encryption to protect medical plaintext data from potential attackers. By secret sharing, computations are distributed across multiple virtual nodes at the edge, concealing all arithmetic operations. This configuration prevents untrusted cloud servers from obtaining insights into the tasks performed on the encrypted patient data. Leveraging cloud computing resources, virtual edge nodes adeptly manage computationally intensive mathematical functions, thus reducing latency in data transmission between devices and edge nodes. In the scheme by Akbulut et al. [11], integration of IOTA Tangle, DLT, IPFS protocols, Application Programming Interfaces (APIs), Proxy Re-encryption, and access control mechanisms secure patient medical records and IoT medical devices. Their system empowers patients with full control over their health records. Liu et al.'s scheme [12] relies on a consortium blockchain, emphasizing both security and privacy. Encrypted EHRs are stored on the IPFS, with the resulting hash addresses logged on the blockchain. Through the proxy re-encryption algorithm, users can grant decryption authorization to specific individuals, guaranteeing that only intended persons can access EHR files. Table I shows the comparative analysis of the existing techniques.

A. Motivation

MPCS provides wide-ranging opportunities for researchers and diverse sectors to tackle security and privacy concerns. However, discussions on numerous issues, including security, privacy, and trust in various cyber-physical systems, are prevalent within MPCS. IOTA is favored over Hyperledger for IoT-based MCPS due to its lightweight, scalable, and energy-efficient Tangle consensus mechanism, which eliminates traditional miners and reduces computational overhead. Unlike Hyperledger's complex peer-based infrastructure, IOTA's cryptographic security and feeless transactions make it ideal for decentralized, resource-constrained IoT networks.

To ensure secure data sharing, Homomorphic Encryption (HE) enables computations on encrypted medical data without decryption. The BFV scheme is chosen for its precise arithmetic, making it suitable for medical applications like ECG analysis and glucose monitoring. BFV balances security and efficiency, allowing real-time encrypted processing on IoT devices with limited computational power.

Integrating BFV with IOTA and IPFS enhances data security and integrity. IPFS provides decentralized storage, while IOTA's tamper-proof ledger ensures authenticity. Compared to other Fully Homomorphic Encryption (FHE) schemes, BFV optimizes encryption and decryption, supporting essential arithmetic operations. This combination enables privacy-preserving analytics, regulatory compliance, and decentralized trust in MCPS.

Generally, several challenges associated with MCPS include aspects such as modifiability, performance, and dependability. Furthermore, some attacks within MCPS are as follows:

1) *Data Breach Perpetrators:* These attackers, relying on malware, aim to infiltrate healthcare industries to extract highly sensitive medical information. Subsequently, they may sell this information for personal gain.
2) *Social Engineering Exploiters:* These adversaries target the security systems of healthcare networks by focusing on hospital staff. They achieve this by sending deceptive emails and enticing staff to click on links that facilitate the exposure of passwords and other sensitive data.
3) *Insider Threat Actors:* These attackers, comprising disgruntled and criminally motivated employees, harbor intentions of turning against their organization due to past grievances.

TABLE I
COMPARISON OF RELATED WORKS

Scheme	Purpose	Security Goals	Platform used	Limitations
[9]	Patient health data sharing	Data privacy	Blockchain and smart contracts	Cost-effectiveness and protection of patient data from leaking
[10]	Secure medical data sharing	Data confidentiality	Homomorphic encryption	Greater computational and communication costs
[11]	Secure personal health records management	Data privacy	IOTA tangle, DLT and IPFS protocol	Distributed storage in IPFS and IOTA lacks full decentralization due to coordinator nodes
[12]	Electronic Medical Record (EHR) data sharing	Data privacy	Elliptic curve cryptography and IPFS	No formal security analysis proof

III. PRELIMINARIES

This section describes the basic background knowledge of the terms used in the proposed technique.

1) Inter Planetary File System (IPFS):: It is a decentralized protocol that enables direct network storage and sharing of digital content on the web. IPFS leverages a distributed network of nodes to store and retrieve files efficiently while ensuring fault tolerance.

2) Brakerski–Fan–Vercauteren (BFV) Encryption Scheme:: BFV, is a somewhat homomorphic encryption (SHE), consisting of three algorithms [13]:

- *Key Generation Algorithm (KEYGENBFV):* This algorithm utilizes security parameter k as input, produces public key PU_k along with a secret key PR_k.
- *Encryption Algorithm (ENCBFV):* This algorithm requires a given message m, a public key PU_k, and a random polynomial as inputs. It outputs a ciphertext c.
- *Decryption Algorithm (DECBFV):* The decryption algorithm takes c and a secret key PR_k to compute the original plaintext message m.

The details of these algorithms can be found in [13].

3) IOTA Tangle:: It is a distributed ledger similar to blockchain, based on the mathematical concept of a DAG. It consists of various layers and components, including transactions, client nodes, APIs, and network types. The Comnet serves as primary network intended for testing and development purposes. Transactions on the Tangle are organized into bundles, each containing essential components such as the transaction hash, value, confirmation status, tag, address, bundle, nonce, signature message fragment, and the address of the parent transaction. Moreover, the developers can apply the Tangle's API to test transactions and develop applications.

IV. PROPOSED METHODOLOGY

The proposed MCPS's architecture, shown in Fig. 1, consists of the following: 1) Data Publisher, 2) IPFS Data Storage, 3) IOTA Tangle, and 4) Data Subscriber.

A. Data Publisher

Patients in the architecture are considered Data Publishers and are nothing but data owners; in general, Body Area Networks (BAN) sensors provide the data or the patient's past medical history and can also become EHR. In the proposed architecture, Data Providers perform the following responsibilities:

1) *Data collection onto mobile:* In this phase, sensors periodically collect the patient's health condition and then send it to the mobile device.
2) *Data processing:* After receiving sensor data, it separates the collected sensor data into public and private data. Afterward, BFV homomorphic encryption encrypts both public and private sensor data.
3) *Sending of public features onto IPFS:* Later, the mobile device sends the cipher public health data onto IPFS and stores the hash received from the IPFS nodes.
4) *IOTA Tangle channel creation:* A channel is first established using a secret channel key, Then the publisher can encrypt data with the data subscriber's public key, and then use a channel key and publish it into IOTA Tangle.
5) *Sharing of private HER features to data subscriber:* In this phase, upon receiving of EMR request from the data subscriber, Mobile apk places encrypts the data using the Subscriber's private key and then places cipher EMR onto the Tangle. A protected IOTA Tangle is used in the experimentation, where a user knows the secret key to access the data.

B. IPFS Data Storage

The main characteristics of IPFS includes:

1) Assign a unique address derived from the hash of the file's content, referred to as a Content Identifier (CID).
2) Combine the file's hash with a unique identifier for the hash algorithm into a single string. IPFS currently employs the Secure Hash Algorithm (SHA-256), which generates a 256-bit (32-byte) output, encoded using Base58.

C. IOTA Tangle Data Sharing Platform

IOTA Tangle, using the "masked authenticated messaging (MAM) communication protocol", is responsible for sharing private features securely with the doctor.

D. Data Subscriber

In the proposed technique the doctor treating the patient is termed a data subscriber and is responsible for the following operations.

1) Receive private data from the IOTA Tangle.
2) Collect a secret key from a data subscriber, which is used to decrypt the private data received from the IOTATangle.

3) Decrypt the patient private data using his/her private key.
4) Collect encrypted public data from IPFS using the CIDs received from the IOTA Tangle.
5) Decrypt the received public data using the data provider's public key.

Biological or medical data in the MCPS setting is generated by smart medical devices and stored as EHR files, as illustrated in of Fig. 1. This EHR is being accessible for treatment/analysis by data subscribers. At first, a direct and offline connection is established between the medical devices and smartphones to enable data transmission. During this process, smartphones receive the health data, from the sensors attached to patient body, as input. Selective Feature Engineering (SFE) method on smartphone fragment the features and selectively encrypt the data. Depending on the sensitivity of the feature, the features will be identified, and only the less critical data pieces (referred to as public features in Fig. 1) will be transmitted to IPFS. Meanwhile, the more critical data pieces (private fragments in Fig. 1) will be stored locally on the smartphones in encrypted form. This approach ensures efficient utilization of resources while maintaining security levels appropriate to the sensitivity of the data.

In EHR data sharing, data publisher can initially take a decision whether to share their private fragment data with Data Subscriber by directly controlling the data sharing settings on their smartphones. Once the institutions are authenticated to access a patient's EHR, the public fragment can be retrieved from cloud server. On the other hand, private fragment can be shared anonymously after removing sensitive information, such as identity. This cloud server deployment serves as an efficient data storage and sharing middleware, ensuring comprehensive functionality and helping to prevent data leaks.

Traditional encryption algorithms, like "Advanced Encryption Standard (AES)" handles key management to secure EHRs stored on cloud servers. It emphasizes the risk of data leakage if the encryption key is exposed., especially when users reuse keys across multiple platforms. Fragmentation is proposed to prevent complete data exposure, even if the key is compromised. Lossless transformations like the discrete wavelet transform (DWT) are suggested to fragment digital files into segments with varying importance levels. However, this approach is deemed unsuitable for EHR protection due to the nature of EHRs being comprised of multiple files rather than large data chunks.

The proposed method involves breaking down digital data to establish connections among different segments. A small fraction of the data is used to safeguard the remaining segments efficiently, which are then protected using encryption techniques and a key. A dispersion strategy is used for storage: the encrypted portion is kept on the user's device, while the rest is stored on IPFS for cost efficiency. This setup ensures that even if the encryption key is compromised, the data on IPFS remains inaccessible since the key cannot decrypt those segments. As a result, this approach prevents data leakage resulting from password reuse, even if the encryption key is exposed.

We now introduce an algorithm to selectively encrypt sensitive features and store them using a dispersion method. Parameters from Table 1 are utilized to accommodate various file formats of Electronic Health Record (EHR) data. Initially, the EHR data input (D_{input}), which could be in the form of an image or a database file, undergoes pre-processing to create a file header (D_{head}) containing all necessary markers for the format. The content (C) of D_{input} is then split into D_{head} and C. The size of D_{head} is typically negligible compared to C and is stored locally in plaintext. Subsequently, C is processed by the Selective Encryption Algorithm (SAE) using keys (PU_k and PR_k) and a counter set to 0. BFV key generation creates public and private keys for patients and doctors. The algorithm outputs encrypted private fragment (PRF_c) and encrypted public fragment (PUF_c). Further details are provided in Algorithm 1.

Algorithm 1 Selective Features Encryption

Input: Data D_{input}, PR_k and PU_k
Output: Public and private fragments: $EPUF_c$ and $EPRF_c$

1: $D_{input} \longleftarrow D_{head} + C$
2: $C = (C_1, C_2, \cdots, C_N)$
3: $PRF_c = \{\emptyset\}$; $PUF_c = \{\emptyset\}$ {Initialize the public and private fragments to null set}
4: $feature \longleftarrow$ private features
5: **for** $i \leftarrow 1$ to N **do**
6: **if** C_i in $feature$ **then**
7: $PRF_c \longleftarrow$ Add(PRF_c, C_i) {C_i is collected onto PRF_c }
8: **else**
9: $PUF_c \longleftarrow$ Add(PUF_c, C_i) {C_i is collected onto PUF_c }
10: **end if**
11: **end for**
12: $EPRF_c \longleftarrow$ ENCBFV(PRF_c, PU_k) {PRF_c is protected by patient's public key}
13: $EPUF_c \longleftarrow$ ENCBFV(PUF_c, PR_k) {PUF_c is protected by patient's private key }
14: **return** ($EPRF_c$, $EPUF_c$)

In lines 1-2, we initialize the algorithm to configure parameters and read the input EHR data content C as N features with each feature onto $(C_1, C_2, \cdots, C_N)$. Then, the patient finalizes the features that are considered private onto $feature$ in line 4. Each data unit C_i is processed in line 5. In lines 7-12, we identify which features will be designated as the private fragments and which will become the public fragments. In this algorithm, the sequence of C is processed using a for loop. However, it can be parallelized to enhance performance, which allows simultaneous processing of the sequence of C.

The algorithm employs BFV homomorphic encryption (HE) to encrypt both public and private fragments. Thus, PR_k is used to encrypt PUF_c, and PU_k is used to encrypt PRF_c as detailed in lines 13-14. This process generates $EPRF_c$ and $EPUF_c$. Next, $EPUF_c$ is uploaded to the IPFS network. A CID is created and returned to the mobile device after successful storage. To access the patient's public features, the doctor needs to retrieve the CID and view it on the IPFS network (https://ipfs.io/ipfs/) using the CID. Private information, however, remains encrypted. After receiving the CID, the handling unit creates a transaction that includes the CID and metadata describing the shared data, such as the "data owner, data type, a brief description, and decryption keys" for the IPFS content. Transactions can be published in various

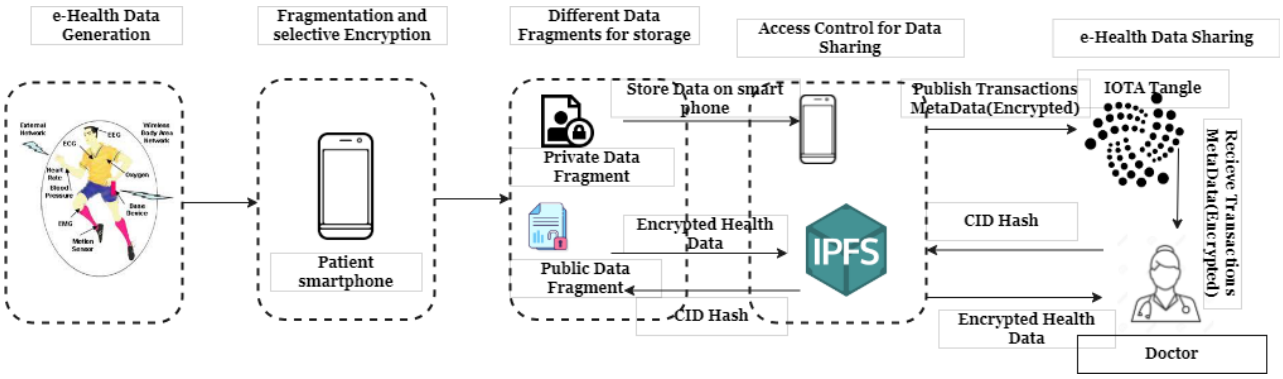

Fig. 1. Architecture of peer-to-peer MCPS based on IOTA Tangle and IPFS.

privacy modes. In our method, the transaction is published in a restricted mode, requiring an additional key to access the content, and thus, it allows the data publisher to manage access flexibly. The decryption algorithm requires PU_k to decrypt $EPUF_k$, and PR_k must be known to decrypt $EPRF_c$.

V. Security Analysis

This section describes the following attacks that are resisted by the proposed system.

1) Stolen Verifier Table Attack: The proposed scheme embraces IOTA's distributed ledger architecture, eliminating any entity needing to maintain the verifier table. This protects against the risk of the verification table being stolen, thereby making the proposed protocol resilient to stolen verifier table attacks.

Fig. 2. IPFS Configuration

2) Black Box Attacks: A black box attack on Homomorphic Encryption (HE) occurs when an adversary gains access to encrypted data but lacks the secret key necessary for decryption. In this scenario, the adversary aims to extract information about plaintext data by analyzing the output of homomorphic operations performed on the encrypted data. IOTA's capabilities for private transactions ensure that transaction details, including sender, receiver, and transaction amount, are obscured from external observers. Encrypting transaction data and limiting access to authorized parties enhances the privacy of transactions within the Tangle, making it more difficult for attackers to analyze and exploit vulnerabilities.

3) Data Breach Perpetrators: BFV enables end-to-end data encryption, ensuring that sensitive information remains encrypted at rest and in transit. Even if attackers gain unauthorized access to the encrypted data, they cannot decipher it without the corresponding private key. So, the proposed technique is secure against Data Breach Perpetrators.

4) Social Engineering Exploiters: BFV allows for secure data sharing and collaboration while maintaining confidentiality. Encrypted data can be shared among authorized parties without the risk of exposure to unauthorized individuals, reducing the likelihood of social engineering exploiters gaining access to sensitive information through deceptive means.

5) Indistinguishability under CPA: In a chosen-plaintext attack (CPA), an adversary $\mathcal{A}$ selects two messages m_0 and m_1, and then receives an encryption of one of them. The adversary's goal is to determine which message was encrypted. Here, $c_b = Enc(m_b) = (a, as + e + \Delta m_b) \mod q$, where $b \in \{0, 1\}$. Given that adversary $\mathcal{A}$ must guess b with probability significantly greater than $\frac{1}{2}$. Since a is chosen randomly from $\mathbb{Z}_q$ and e follows a discrete Gaussian distribution, the value of b (which determines m_b) is statistically hidden in the noise term. The encryption outputs (a, b) resemble random values from $\mathbb{Z}_q^2$ under the Learning With Errors (LWE) assumption, where it makes difficult for $\mathcal{A}$ to distinguish between encryptions of different plaintexts. Assume λ is the security parameter. Then, for any polynomial-time adversary $\mathcal{A}$, the distinguishing advantage is also negligible, where $\Pr[\mathcal{A}(Enc(m_0)) = 1] - \Pr[\mathcal{A}(Enc(m_1)) = 1] \leq \varepsilon(\lambda)$, which is a negligible function.

VI. Performance Evaluation

We perform an experimental analysis on a well-established heart disease dataset available in JSON format from the HL7 FHIR repository. Based on the "HL7 FHIR (Fast Healthcare Interoperability Resources) standard", this dataset ensures structured and interoperable medical data exchange. The "Observation" resource specifically tracks body temperature measurements, featuring a unique observation ID, a meta-profile linking to the FHIR vital signs structure, and a

Fig. 3. IPFS Execution

category classifying it under “Vital Signs.” Additionally, the “code” field incorporates a standardized “LOINC (Logical Observation Identifiers Names and Codes) identifier (8310-5)” for “Body temperature,” promoting semantic interoperability in medical data sharing. To enable decentralized and tamper-proof data storage, HL7 FHIR data was uploaded to the IPFS using its API [14], [15]. Upon successful upload, Fig. 2 shows a content identifier as follows: “CID: QmWne2o16JgWsSCgJJurBYDeJjsq6LcYhjWU6f5qJjZsUM” was generated and provided to the patient. An IPFS node was also established to facilitate secure and authenticated communication.

In Fig. 3, we show the peer ID which uniquely identifies the node within the distributed IPFS network “PID: 12D3KoowC3VSwQsxo7JHLRNDe48AVvZuMN3eYG35 Ldcq-7enNLo”, while the public key is as “CAESIEUJ652eRASfH8c3dKE0NsQ27Fs4Km1TPqwHuOGi” that enhances cryptographic security for data exchange and verification. IPFS’s cryptographic hash-based addressing system ensures data integrity, as any modifications generate a new hash. When a doctor required access, the patient shared the CID, enabling retrieval of the stored data via IPFS, ensuring efficient, decentralized access to public health information.

For secure storage and transmission of sensitive health data, we implemented BFV homomorphic encryption using the “Pyfhel library in Python 3.10.12”. The encryption and decryption processes were executed on an “Intel(R) Xeon(R) CPU @ 2.20GHz in a Google Colab” environment. Upon a doctor’s request for access to a patient’s sensitive health record, the patient encrypted the data with the doctor’s public key before transmitting it over the IOTA Tangle network via the PYOTA package available at https://pyota.readthedocs.io/en/latest/. The doctor then used their private key to decrypt and securely access the health information.

Table II shows the proposed technique’s computation time of encryption and decryption time. The key generation is done by considering polynomial modulus (n) was varied among 1024, 2048, and 4096, with corresponding coefficient modulus (q) values of 27, 52, and 86. The results, shown in Table II, reveal that encryption consumes roughly 48% of the processing time, decryption consumes 52%, and the addition calculation step takes up less than 1% of the total time. These data transactions on IOTA Tangle could be published in different privacy modes, such as public and private or restricted modes, where an extra key is required for access, allowing the data publisher to control the data. Restricted access mode is preferred to do data transactions. Once the transaction is published on the IOTA Tangle, the doctor treating the patient only knows about the channel key used to receive transactions from the IOTA Tangle. Later, the doctor uses his/her private key with a BFV homomorphic algorithm to decrypt patient-sensitive information.

The data transaction on IOTA Tangle focused on three primary tasks in publishing and fetching transactions: create, attach, and fetch. For the create task, the time taken to generate transactions before publishing them to IOTA nodes was measured, termed as “create time,” utilizing the IOTA API to create transaction objects from data payloads. Next, the attached task involved publishing the transaction objects to the IOTA network, including conducting a Proof-of-Work (PoW) consensus algorithm and storing transactions by nodes. The time taken for this step was labeled as “attach time.” Finally, the fetch task encompassed retrieving transactions from the IOTA network, achieved by querying the private Tangle, and the corresponding execution time was measured and termed as “fetch time.”

In evaluating the performance of a scheme, communication

TABLE II
BFV ALGORITHM PERFORMANCE

n	q	$Enc(ms)$	$Add(ms)$	$Dec(ms)$
1024	27	2.37	0.012	2.58
2048	52	2.36	0.012	2.47
4096	86	2.44	0.012	2.66
σ		0.044	0	0.095

Note: Enc: Encryption time; Add: Addition time; Dec: Decryption time; σ: Standard deviation

TABLE III
COMPUTATION AND COMMUNICATION COSTS

Metrics	[9]	[10]	[11]	[12]	Proposed
Data storage time (sec)	22-90	15-50	15-50	0.5	0.5
Data access time (sec)	9-40	7-35	2-15	0.173	0.25
Data storage length (bits)	10240	2560-11264	1792	2880	2464
Data access length (bits)	11980	2880-10264	1536	3296	4864

TABLE IV
COMPARATIVE ANALYSIS WITH EXISTING TECHNIQUES

Feature	[9]	[10]	[11]	[12]	Proposed
Data Confidentiality	✓	✓	✓	✓	✓
Data Integrity	✓	✓	✓	✓	✓
Stolen Verifier Table Attack	✓	×	✓	×	✓
Black box attacks	×	✓	×	✓	✓
Data Breach Perpetrators	×	✓	×	✓	✓
Social Engineering Attacks	×	×	×	✓	✓
Decentralization	✓	×	✓	×	✓
Decentralized Storage	✓	×	✓	×	✓
Traceability	✓	×	✓	×	✓

overhead is also another important factor. In Table III, we will compare the communication overhead of the proposed scheme with other existing schemes. Firstly, in the data storage phase, the patient needs to send encrypted public medical record information to IPFS for storage, including encryption of patient personal details like name, age, blood group, and address with a size of 400 + 24 + 32 = 456 bits. Then IPFS returns the hash value to the patient and uploads it to IPFS for storage, including hash value, name, age, and blood group, with a size of 256 bits. The message length in the data storage phase is 256 + 456 = 712 bits. A total of 19 bytes of patient-sensitive data (like cp, trestbps, chol, fbs, restecg, thali, exacting, old peak, slope, ca and thal) is stored in cipher form, encrypted using BFV is stored in the patient system. The storage size required for the storage is of 760 bits. Next, in the data access phase, the doctor needs to send a request to the patient, including a request message and other messages, with a total size of 256 bits. The patient sends hash value and other information, totaling 256 + 160 = 416 bits. Then, the doctor accesses IPFS to retrieve the EMR information using the hash address and decrypts it into 256 bits using the private key. The message length in the data access phase is 256 + 416 + 760 = 1422 bits.

The performance of the proposed technique in terms of security services is shown in Table IV. All the existing methods ensure data confidentiality using HE and ECDSA algorithms, with data integrity verified at the recipient's end. Social engineering attacks exploit human behavior rather than technical vulnerabilities, meaning technologies like blockchain, IOTA, and HE alone are insufficient. Integrating technological solutions with human-centered security practices is crucial to preventing such attacks. The methods discussed in [10]–[12] may not fully address these social engineering threats. Preventing Stolen Verifier Table Attacks requires secure credential storage, strong hashing, and multi-factor authentication. However, if data is stored on the cloud instead of in a decentralized system, decentralized storage, and traceability cannot be achieved, making the countermeasures in [11] and [12] potentially inadequate for this attack. Table IV shows that the proposed technique provides more security features and can protect patient health data from various attacks in MCPS.

VII. CONCLUSION

This article introduces a patient-centric EHR data-sharing system for MCPS, utilizing advanced technologies, such as BFV HE, IOTA Tangle, and IPFS. The aim is to address data safety threats from end users' behaviors, such as key reuse and leakage. An SFE algorithm with fragmentation and dispersion techniques was proposed for data storage to protect against leaks of both the encryption key and public EHR data fragments. BFV HE secures sensitive patient data, while a DAG-structured IOTA Tangle ensures high scalability, low cost, and tamper-resistance in data sharing. IPFS also handles the challenge of large-volume data storage. Test results confirm the algorithm's ability to prevent data recovery even with compromised keys and public fragments. One future work is to deploy the system in practical healthcare environments, potentially integrating with patient health prediction using machine learning and deep learning approaches.

ACKNOWLEDGMENTS

The authors would like to thank the associate editor and the anonymous reviewers for their valuable feedback on the paper.

REFERENCES

[1] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2020.

[2] Y. Miao, F. Li, X. Li, J. Ning, H. Li, K.-K. R. Choo, and R. H. Deng, "Verifiable Outsourced Attribute-Based Encryption Scheme for Cloud-Assisted Mobile E-health System," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–18, 2023.

[3] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar, and S. K. R, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023.

[4] X. Zhu, J. Zheng, B. Ren, X. Dong, and Y. Shen, "Microthingschain: blockchain-based controlled data sharing platform in multi-domain iot," *Journal of Networking and Network Applications*, vol. 1, no. 1, pp. 19–27, 2021.

[5] P. Shabisha, A. Braeken, A. Touhafi, and K. Steenhaut, "Elliptic curve qu-vanstone based signcryption schemes with proxy re-encryption for secure cloud data storage," in *Cloud Computing and Big Data: Technologies, Applications and Security*. Rabat, Morocco: Springer International Publishing, 2019, pp. 1–18.

[6] X. Zhang, J. Zhao, C. Xu, H. Wang, and Y. Zhang, "DOPIV: Post-Quantum Secure Identity-Based Data Outsourcing with Public Integrity Verification in Cloud Storage," *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 334–345, 2022.

[7] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to Cyber-Physical System Security: A Cross-Layer Perspective," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 3, no. 3, pp. 215–227, 2017.
[8] A. S. Leong, A. Ramaswamy, D. E. Quevedo, H. Karl, and L. Shi, "Deep reinforcement learning for wireless sensor scheduling in cyber-physical systems," *Automatica*, vol. 113, p. 108759, 2020.
[9] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdge-Health: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 743–11 757, 2021.
[10] M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic encryption based privacy-preservation for iomt," *Applied Sciences*, vol. 11, no. 18, p. 8757, 2021.
[11] S. Akbulut, F. H. Semantha, S. Azam, I. C. A. Pilares, M. Jonkman, K. C. Yeo, and B. Shanmugam, "Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology," *Sensors*, vol. 23, no. 11, p. 5174, 2023.
[12] G. Liu, H. Xie, W. Wang, and H. Huang, "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," *Journal of Cloud Computing*, vol. 13, no. 1, p. 44, 2024.
[13] S. Halevi, Y. Polyakov, and V. Shoup, "An Improved RNS Variant of the BFV Homomorphic Encryption Scheme," in *Topics in Cryptology – CT-RSA 2019*. Cham: Springer International Publishing, 2019, pp. 83–105.
[14] M. Olivya, D. Nur, F. A. Lasawedi, I. Syamsuddin, and I. Irmawati, "Distributed storage systems: Leveraging blockchain and ipfs protocols," in *AIP Conference Proceedings*, vol. 3140, no. 1. AIP Publishing, 2024.
[15] [Online]. Available: https://pypi.org/project/ipfs-api/

Sivaranjani Reddi received Ph.D. and M.Tech from Andhra University, India, and B.Tech. from National Institute of Technology, Warangal, India. She is currently a full professor Dean(CSE), Raghu Engineering College,India.Her research interests include network security and blockchain.

Patruni Muralidhara Rao received his Ph.D. degree from Vellore Institute of Technology, Vellore, India. He received M.Tech degree in 2014 from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. He is currently working as a senior assistant professor at Gayatri Vidya Parishad, Vishakhapatnam, India. He is an active member of IEEE and IAENG professional bodies. His research interests include Network Security and Blockchain. He has authored over 30 papers in international journals and conferences in the above areas.

Saraswathi Pedada "obtained M.Tech. (Computer Science and Engineering) degree from JNTU, Kakinada, India, in 2016. She is currently a Ph.D. student at National Institute of Technology, Warangal and working as an assistant professor at GITAM University, Visakhapatnam, India. Her research interests include wireless sensor networks and network security. She has published several articles in international journals and conferences."

Basudeb Bera is a post-doctoral researcher at the Department of Electrical and Computer Engineering, National University of Singapore (NUS). His research interests include cryptography and network security, AI/ML security and post-quantum cryptography. He received his Ph.D. degree in computer science and engineering from International Institute of Information Technology, Hyderabad, India. He has published more than 30 papers in international journals and conferences.

Ashok Kumar Das [SM] received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a full professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is an adjunct professor with the Korea University, Seoul, South Korea. He was also a visiting research professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His current research interests include cryptography, system and network security, blockchain, AI/ML security, and post-quantum cryptography. He has authored over 475 papers in international journals and conferences in the above areas, including over 405 reputed journal papers. He is/was on the editorial board of IEEE Transactions on Information Forensics and Security, IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), IET Communications, and International Journal of Communication Systems (Wiley).

Biplab Sikdar [F'25] is a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Head of Department of the Department of Electrical and Computer Engineering. He received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from IIT Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017.