A Privacy-Preserving Secure Data Processing Scheme for the Internet of Medical Things

Ying Huang and Yongmei Su

***Abstract* — The Internet of Medical Things (IoMT) offers diverse application support through monitoring, analysis, and recommendations. This application paradigm relies on sensitive internal and external data to meet user needs. This article introduces a secure data processing scheme for leveraging the IoMT application performance. This scheme is named Persuaded Data Processing with Digital Security (PDP-DS), ensuring user and data privacy. This scheme focuses on IoMT-aided remote monitoring application security where data openness is high and false data chances are high. During the application support, the blockchain concept is applied for data authentication. In this scheme, user-verified digital signatures are used for authentication. This scheme provides data processing recommendations based on the deep learning paradigm. This output is authenticated alone using a password/ PIN-based digital signature. The learning process identifies the processing required and security-filtered instances using the recursive states identified. The proposed scheme ensures fewer false data processing based on its attributes and recommendation factor. PDP-PS reduces the considered metrics to 9.95% (for process delay), 10.19% (for service delay), 10.6% (for replication factor), 10.44% (for false rate), and 7.39% (for backlogs).**

***Index Terms* — Blockchain, Attribute Analysis, Deep Learning, Internet of Medical Things (IoMT)**

Paper Classification
DOI: 10.53314/ELS2428033H

THE Internet of Things (IoT) is an emerging technology in many applications that provides users with better services, performance, and communication processes. Sensors play a vital role in IoT, which is used for data collection and analysis [1]. IoT is also used in medical fields to analyze patients' health conditions, known as the Internet of Medical Things (IoMT).

Manuscript received on June 24th, 2024. Received in revised form on August 13th and September 11th, 2024. Accepted for publication on November 17th, 2024.

Ying Huang is with the Faculty of Guangxi Eco-engineering Vocational and Technical College, Guangxi, P.R. China (e-mail: huangying800816@163.com).

Yongmei Su is with the Faculty of Zhengzhou Technical College, Zhengzhou, P.R. China.

This paper was supported by the Talent Introduction Scientific Research Project (NO.GXSTKYZX202406002) of Guangxi Ecological Engineering Vocational and Technical College, the first phase of the training project of famous teachers (craftsmen), and the project construction project of famous master studios.

IoMT is done with the help of smart devices and smart applications with an internet connection to provide better user analysis and service [2]. A remote Patient healthcare monitoring system is an important task to perform in the medical field. The patient monitoring system collects every detail of patients and provides a collective dataset used for the diagnosis process [3]. The patient monitoring system is widely used in the medical field to avoid unwanted death and provide necessary services to users. The remote patient monitoring system mostly uses Electro Cardiogram (ECG) waves. ECG produces signals based on a patient's signs, symptoms, actions, and gestures [4]. A wearable sensor is one of the IoMT applications used in remote patient healthcare monitoring systems. It produces proper details collected based on the patient's condition and helps to increase the overall performance in the diagnosis and treatment process [5].

The remote patient monitoring system is mostly used in the medical field to provide a better diagnosis process. Security and privacy are the major concerns regarding a remote monitoring system. The remote monitoring system uses a wireless medical sensor network (MSN) to enhance the security management process [6]. A lightweight public-key-based authentication framework enhances the security system in a remote monitoring system. Authentication is one of the main causes of security issues. Public-key-based authentication framework provides the key to users for the authentication process, ensuring the user's security from attackers [7, 8]. The remote monitoring system uses the agreement and Key Authentication (AKA) method to ensure user security. AKA provides a secret key to users, which is used in the authentication process and provides users from unauthorized persons from entering smart devices [9]. AKA also ensures users' privacy by providing a proper authentication process. A secure IoT-based system is presented using sensor and cloud computing to provide an alert by an email [10]. A smart contract system is used in the real-time world to understand security threats and prevent users from attackers. Blockchain approaches send verification notifications to every user during the authentication process, which helps to enhance users' security and privacy [11].

Medical healthcare centers manage Electronic Health Records (EHR) to collect every detail of patients and diseases. Details such as patient's personal information, disease types, symptoms, treatment measures, scheduling, etc., are stored in EHR [12]. The deep learning approach is mostly used in many smart applications to enhance overall performance and ensure user security. The patient data monitoring system is widely used

in IoMT to provide better services to users, which are done based on previously collected data [13]. A deep learning-based Q-network is used in a patient data monitoring system to reduce security threats available in the application. The Q-network has adaptability, flexibility, generalization features, end-to-end learning, automatic feature extraction and scalability compared to other deep learning networks. The Q-network reduces duplicate information stored in the database and provides necessary details for the diagnosis process [14]. Q-network also reduces security threats by understanding the exact complexity and necessity. Q-network also increases the overall efficiency and performance of the monitoring system by avoiding unwanted security threats [15]. Blockchain-based security measure is used in an EHR patient data monitoring system. The blockchain approach is one of the most used approaches for security related issues that ensure users' security and privacy from attackers [16]. Blockchain technology verifies data using a decentralized, immutable ledger. This solution uses blockchain technology to verify data during IoMT-based remote monitoring. It also prohibits data transfers and alterations from happening. Blockchain technology's immutability and transparency make it harder for hostile actors to enter fraudulent data into IoMT applications. Blockchain technology ensures that data cannot be changed after recording because each block is cryptographically tied to the one before it. Every "block" comprises one transaction, and any changes to one can affect the entire chain. This built-in security helps IoMT systems, especially those with high data openness, keep data legitimate and undamaged. The block chain technique is incorporated with the persuaded data processing scheme for managing the medical data security which is derived from the wearable devices. In addition, lightweight signature is incorporated to manage the data authentication which provides the privacy to the sensitive data.

The main contribution of the paper include:

- Persuaded Data Processing with Digital Security (PDP-DS) protects user and data privacy. This approach secures IoMT-aided remote monitoring applications with high data openness and false data chances.
- During application support, blockchain is used for data authentication uses user-verified digital signatures. Hashing passwords or PINs generates digital signatures for data and user interaction verification.
- Deep learning uses security filters to reduce false positives, and blockchain's immutability validates data. PWD/PIN digital signatures simplify authentication but require strong cryptography to be effective and secure.
- The discussed system evaluated using MATLAB tool and system’s efficiency is compared with different methods CL-dPAEKS [25], SRAC [19], and BSDMF [24]. The detailed description is described in section 4.

I. Related Works

Kumar et al. [17] invented a new secure and efficient cloud-centric Internet of Medical Things (IoMT) that enables a smart healthcare system for healthcare centers with public verifiability. The proposed system collects patients' details from the sensors implanted in the body and produces a proper dataset for the verification process. The escrow-free identity-based aggregate signcryption (EF-IDASC) approach is used in the proposed method to understand the medical data available in the cloud server.

Parah et al. [18] proposed an efficient security and authentication method for edge-based IoMT applications. Electronic Health Records (EHR) is vital to secure patient detail from attackers in the proposed framework. Pixel Repetition Method (PRM) and Left data mapping (LDM) approaches are used here to encrypt the data to provide a secure authentication process. Experimental results show that the proposed framework increases the system's overall performance, capability, robustness, and efficiency by providing users with a safe and secure authentication process.

Egala et al. [19] introduced a blockchain-based security and privacy scheme for the IoMT to secure Electronic Health Records (EHR). Selective ring-based access control (SRAC) mechanism is used in the proposed method for authentication to provide a secured system to the users. The proposed method reduces the latency rate and computation cost rate with the help of the blockchain technique. Experimental results show that the proposed framework increases the effectiveness and improves the overall security rate of the system.

Huang et al. [20] introduced a practical privacy-preserving scheme for Electrocardiogram (ECG) based authentication process for Internet of Things (IoT) based healthcare centers. ECG generates signals which play a vital role in the authentication process, which helps to secure medical details from attackers. ECG signals also ensure users' privacy and prevent personal details from being stored in the database. Compared with other privacy-preserving schemes, the proposed scheme increases the efficiency and effectiveness of the systems.

Deebak et al. [21] proposed a mutual smart server authentication (SSA) protocol for cloud-based medical healthcare centers using the IoMT. Formal and informal security analysis processes are available in SSA and provide effective solutions to avoid unwanted security threats. The proposed method is also used in many smart healthcare systems to ensure users' security and privacy from attackers. Experimental results show that the proposed SSA protocol increases users' security and improves the system's reliability and robustness.

Saba et al. [22] introduced a secure and energy-efficient framework for the IoMT. The proposed method is used to reduce the communication overhead and also used to reduce the energy consumption rate while transferring data from one device to another. It also prevents users from unauthorized authentication and proxy requests, ensuring their privacy and security from attackers. The method in [18] performs complex authentication for single authentication, increasing delay. However, this framework controls LDM for precise authentication.

Mohan et al. [23] introduced blockchain-assisted secure data management for IoMT. This is implemented using a private Ethereum blockchain and proof-of-authority (PoA). Double authentication through elliptic curve cryptography ensures end-to-end user privacy in this data management method. Data security and user privacy improve the admittance of the proposed method in IoMT applications.

Abbas et al. [24] proposed a blockchain-assisted secure data management framework (BSDMF) for the IoMT for healthcare data analysis. BSDMF is used to secure patient data between the server and user end, which helps to increase the scalability and reliability of the system. The blockchain approach is mainly used for securing data transmission and management processes. Experimental results show that the proposed BSDMF increases the users' security and privacy and reduces the latency rate while transferring data. The latency is reduced compared to the method in [20] due to blockchain implications.

Different from the public verification presented in [17], Wu et al. [25] introduced a Certificateless Searchable Public-Key Authenticated Encryption Scheme (CL-PAEKS) for cloud-assisted based IoMT applications. PAKES provides a secret key for the authentication process, which helps to prevent security threats. CL-PAEKS also ensures the privacy of users from attackers. Compared to the method in [17], this scheme leverages data security through multiple security measures.

Satamraju et al. [26] proposed a decentralized framework for device authentication and data security system used in the next-generation IoMT. A secret key is distributed to every user for authentication process name as a Physical unclonable function (PUF). Blockchain technology is used here to understand the PUF. For data security services, smart contracts are used to utilize access control. The double authentication [23] problem is addressed using PUF. This authentication sustains until a new complexity arises.

Khan et al. [27] proposed a highly scalable hybrid-driven Software-defined network (SDN) enabled framework for the IoMT. The deep learning (DL) approach is used here to understand the malware or threats available in the database. DL methods leverage the health record without exhaustion. The overall robustness and effectiveness of the system are improved by using DL. The proposed DL method outperformed the traditional frameworks by providing better overall performance and increasing security.

Li et al. [28] proposed a provably secure and lightweight mutual authentication and key agreement (PSL-MAAKA) protocol for the IoMT. Hash operation is used in AKA process, which helps ensure user privacy and security. MAAKA is a secure and efficient authentication protocol to avoid unwanted threats. Experimental results show that the proposed PSL-MAAKA protocol reduces communication overhead. The overhead is reduced using lightweight mutual agreement compared to [26] and [22] methods.

Alzubi et al. [29] introduced a blockchain-based system for IoT-based medical healthcare centers using the Lamport Merkle digital signature (LMDS) model. LMDS is used to authenticate patients' health records and personal details from attackers. A certain verification process takes place to provide a proper authentication process to the users. Experimental results show that the proposed LMDS model increases the system's performance, effectiveness, and robustness and reduces the device's computation cost and energy consumption rate.

Sowjanya et al. [30] proposed an improved lightweight Elliptic Curve Cryptography (ECC) for the IoMT based on an anonymous authentication protocol. The proposed method reduces the security threats that users face and prevents users from attackers. The proposed method identifies both formal and informal security threats and provides solutions to avoid the threats for the users. Experimental results show that the proposed ECC method improves the robustness and accuracy rate in detection threats for IoMT-based applications and systems.

Wu et al. [31] assimilated blockchain in smart healthcare systems for medical data privacy. Local differential privacy is ensured using diverse decision-matching decisions. Access control, anonymous data exchange, and data validation are incorporated into this proposed framework. This ensures precise traceability and error-less data exchanges. For ease of understanding, the above discussion is summarized in Table I.

TABLE I
SUMMARY OF RELATED WORKS

Author & Reference	Aim	Method	Limitations
Egala et al. [19]	Secure Access Control	Blockchain-based independent access control	Unattended access failures
Saba et al. [22]	User Privacy	Proxy-based authentication	Complexity increases due to residual permissions
Wu et al. [25]	Data Security	Public Authentication	Diverse authentication requires more time for security administration
Li et al. [28]	Data Authentication	Mutual agreement	If a session is not initiated, then the key agreement drops
Sowjanya et al. [30]	Data Authentication	ECC-based data security	Requires pre-computation for key generation and signing
Wu et al. [31]	Data privacy	Blockchain-based framework	Distinguishable and independent process augmentation

The methods discussed improve privacy and data security through diverse repetition checks [18], storage verification [20], and scalability [24] features. Besides the authentication for independent and the group as in [29, 30] and [25] are keen on administering the security demands. However, the changes in data attribute and monitoring sessions vary the data nature for size, content, and information handling. Therefore, with the lack of precise knowledge of these features, authentication and privacy-preserving results in process delays and backlogs. Therefore, this article introduced a data processing and security administration scheme to confine such lag. This scheme is aided by blockchain for user information and data status saving for

leveraging the security-impacted processes. According to the overall discussions, the main contributions of this article are listed below:

I. Designing a persuaded data processing scheme for handling secure sensitive medical data observed from the wearable sensors
II. Incorporating digital security measures through lightweight signatures for data authentication user privacy in handling sensitive data
III. Assimilating blockchain for data authentication supporting the recommendation and external authentication
IV. Performing a comparative analysis study to verify the effectiveness of the proposed scheme

II. Proposed Persuaded Data Processing Digital Security Scheme

The goal of (PDP-DS) is to provide diverse, secure data processing on the Internet of Medical Things (IoMT) by accessing diverse application support. The tenure of this application is secured through analysis, monitoring, and recommendations. This combined service relies on the healthcare center and user application serving the IoMT architecture. In this paradigm, the attributes and recommendations of the medical applications are considered to improve the data openness and chances of false data. Here the security is established by using the signature (PIN/PWD) and authentication procedure. Fig.1 presents the proposed scheme in an IoMT environment.

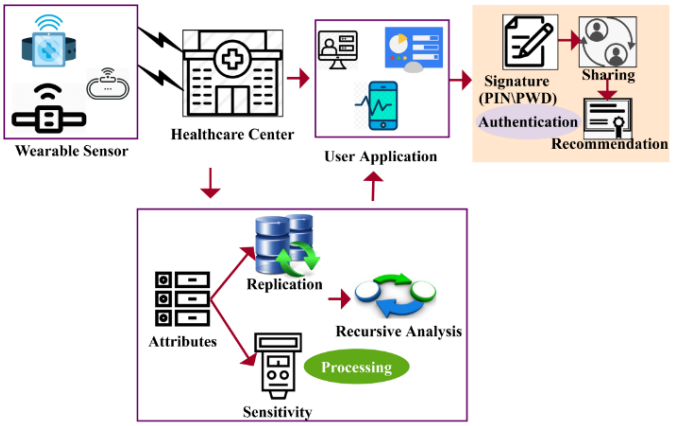

Fig. 1. Proposed PDP-DS for IoMT

As different IoMT applications require false data processing, external and internal data meets different user needs, false fewer data processes, backlogs, service delay, process delay, false rate, and replication factors are unavailable. However, to regulate the IoMT of the end-users, the proposed framework provides the user-verified digital signature that is aided for authentication based on its attributes and recommendations (Fig. 1). As the digital signatures are generated based on recommendations, the heaviness in storing and time complexities are avoided across multiple intervals. Unlike conventional digital signatures, fore-hand generation, storage, and modifications are prevented in this process. Besides, the blockchain analyzed factors ensure the need for new signature generation. This comparatively reduces the service and process time requirements. In Table Ⅱ, the symbols used are summarized.

TABLE II
SYMBOLS AND DEFINITION

Symbol	Definition
D_{IE}	Internal and External Data Count
t_R, t_S	Service and process delays
B_{Lg}	Backlogs
S_d	Service Response
t_d	Time Delay
α	Attribute-Analysis Process
Δ	Replication
$\exists!$	Equating Factor
t	Output

Problem Definition: Let $\{1,2,\dots,d\} \in D_{IE}$ denotes the set of internal and external data that is processed in sensitive for meeting lots of user's needs in a different time interval $t_d \in (t_R - t_S)$ where t_R and t_S are the delay in service and process, respectively. From different time intervals, the different user needs processing D_{IE}, the backlogs B_{Lg} must be false fewer data processing under its controlled process, and service delay is given by equation (1).

$$\left.\begin{array}{c} \forall\,(t_R - t_S), argmin\ \sum_{i=1}^{t_d}(D_{IE} - S_d)_i, t_d \in [t_R + 1, t_S] \\ and\ \frac{S_d}{D_{IE}} = maximum\ in\ any\ (t_R - t_S) \\ where \\ argmin\ \sum_{i=1}^{S_d}(t_R)_i \\ \forall\,\{1,2,\dots,d\} \in D_{IE} \\ t_S \le t_d \le t_R \end{array}\right\} \quad (1)$$

Where the variable S_d represents the service response and $D_{IE} - S_d$ in the backlogs in any $t_d \in [t_R + 1, t_S]$. This augments the backlogs in various time intervals, reducing the sensitivity during application support of the users.

The above-derived equation is noticed using the attributes and recommendations of the IoMT applications through a deep learning process. However, there are a few limitations based on t_R and t_S that is determined as follows:

For all $d \in D_{IE}$ in $[t_R, t_S]$, if $(d+1)$ is true in $t_d \in [t_R + 1, t_S]$ then $(d+1)$ experiences an additional process delay of $(t + t_R + 1)$ such that, where t denotes the backlog occurrence.

For all $d \in D_{IE}$ int$_R$, if $t = t_S$ or$t > t_S$, then $\omega = (D_{IE} - S_d)$ is maximum and $\frac{S_d}{D_{IE}} \to 0$.

In condition (ii), the variable ω denotes the backlogs. The first condition represents the false fewer data processing of the $(t_R - t_S)$ where the next d, if $(d+1)$ co-exists with any $t_d \in [t_R + 1, t_S]$ of t. This augments the service delay for both d and$(d+1)$. Similarly, the second condition identifies the false fewer data processing and backlog in $[t_R - t_S]$ interval and also verifies if the digital signature with the successive

authentication S_d provided $argmin\ \sum_{i=1}^{S_d}(t_R)_i\ \forall\ [t_R - t_S]$ is achieved.

The (PDP-DS) is administrated between the different user needs and application supports meted using the IoMT environment. The attributes and recommendations are the factors of the application support service. The attribute analysis (a) of the application relies on the replication and sensitivity of the user. During this process, users have to authenticate to improve data privacy, security, and authentication. User authentication is ensured by applying the blockchain concept. The user data has been verified using blockchain authentication, applying public key cryptography. The blockchain-based encryption process verifies the user's every attribute to protect sensitive data from unauthorized users. The blockchain consists of a set of blocks that helps to increase user identity-related security. Once the user security is improved, the user is linked with the respective resources for making access.

In addition, the blockchain has a distributed ledger or blocks to ensure user privacy, integrity, and security. All user information is stored in the blocks using the hash function that manages the self-sovereign identity. The block stores the transaction type for every transaction, which helps to understand the blockchain activity. Once the user blockchain activity is stored in the block, it cannot be modified because it is finished with its authentication procedure. If the user tries to access the detailed data, they must register with their identities to verify their identity. The identity may be the user's personal information, identity card, driving license, passport, etc. Then, the public key has been defined to perform the encryption, decryption, and verification. After exchanging the key values, the users are authenticated using the particular timestamp. The user verification must be done during the particular period, and authorized certification must be provided to the user. This process improves overall security and privacy. In particular, a patient or a health-conscious person who utilizes wearable sensors for personal care or diagnosis can access the information. However, the backlog-less and false fewer-less data processing application support is the defining factor of a. Therefore, based on the two conditions mentioned above (i) and (ii), the attribute analysis a is derived using equation (2)

$$\left.\begin{aligned} a = \max\{t_{R_1}, t_{R_2}, \dots, t_{R_d}\}, if\ \forall\ d \in D_{IE} \\ and \\ t \in [t_R, t_S] \\ (or) \\ a = (t_R - t_S) + (t_R + 1 - t), if\ \forall\ t_S \le t \le t_R \end{aligned}\right\} \quad (2)$$

The attributes factor must meet the backlog and time conditions such that the $t \in [t_R + 1, t_S] \forall\ (d+1)$ does not meet $t \in [t_R, t_S] \forall\ d \in D_{IE}$ which is defined in equation (2). As per the above a does not hold stable as it varies due to the application's security. The attributes and recommendation state of the IoMT application support are reflected on D_{IE} that defines $(D_{IE} - S_d)$ and succeeds $\frac{S_d}{D_{IE}} \to 1$. These two main processing of the application depend on a and $[t_R, t_S]$ they are followed by ω of the existing data of the user applications. Cases (i) and (ii) are recursively analyzed for both the replication and sensitivity of the user application using deep learning. This learning process helps to provide data processing recommendations where accuracy, sensitivity, and specificity are achieved. In the following description, the attributes and recommendation-based condition security using deep learning are discussed.

Condition (i) Attribute Analysis: This condition deals with the processing delay in healthcare center processing and service delay with the user applications. The first output for replication and sensitivity is the meeting up of time instances and processing them recursively based on the user application state of the IoMT. First of all, the replications S_d based on t_S is estimated as [25].

$$\Delta(S_d, t_S) \leftarrow \left(1 - \frac{a}{D_{IE}}\right)\frac{S_d}{D_{IE}} + \frac{(t_R - t_S)}{(t_R+1)}\left[arg\min_{D_{IE}} \frac{(t_R)_i}{(t_R+1)_{i+1}}\right] \forall\ i \in S_d \quad (3)$$

From the above equation (3), the replication $\Delta(S_d, t_S)$, and the sensitivity factor is processed based on recursive analysis for the user applications in $t_R + 1$ such that

$$\Delta(D_{IE}, t_R + 1) \leftarrow \frac{a}{D_{IE} - d} + \left(\frac{t_R + 1}{t_S}\right)[(t_R + 1 - t_S)_i] \forall\ i \in D_{IE} \quad (4)$$

The above-derived equation (4) this condition helps to meet the different user needs between t_S, t_R and $t_R + 1$ for any healthcare center data by meeting the cases mentioned above. The prime conditions are the processing of replication and sensitivity t_R. This processing is performed using deep learning. The deep learning process verifies the cases $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$, respectively. Fig. 2 presents the attribute analysis using the learning process.

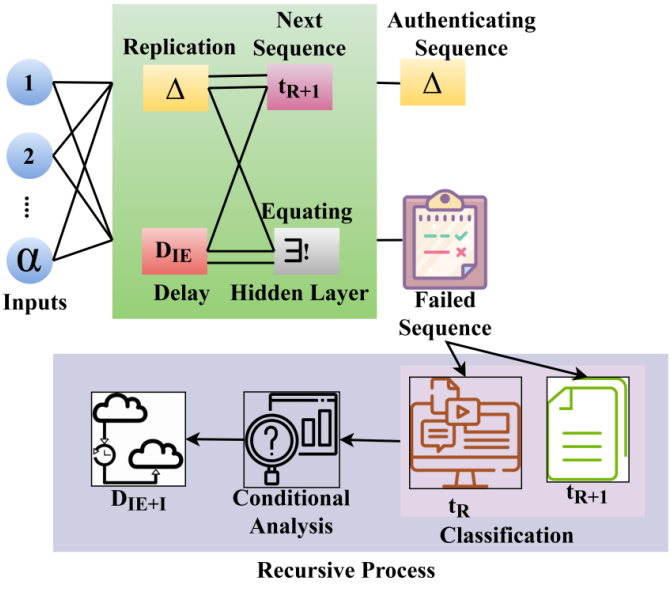

Fig. 2. Attribute Analysis

In Fig.2, the α inputs are validated across $(R+1)\forall\ \Delta$ and D_{IE}. The missing D_{IE} in t_{R+1} or t_R is recursively analyzed

for Δ and Δ failing sequences. The failed sequence is classified as t_R or t_{R+1} for which $t_s \le t$ or $t \le t_R$ (conditional analysis) is performed. This is conjointly analyzed in the hidden layer for extracting Δ from the non ∃! requiring instances. This deep learning is computed for processing $t_S \le t$ and $t_S \le t \le t_R$ cases for preventing an unnecessary delay in user application. From the consideration of $\Delta(D_{IE}, t_R + 1)$ process, the data processing overflows on the pursuing t and thus providing a. However, this a must not meet with the available data, and hence a new time instance is determined. The new instance storage allocation must satisfy $t_S \le t$ to avoid additional process delay. The condition (i) for a, as in the above-derived equation (2) is processed and analyzed using the recursive analysis of $\Delta(D_{IE}, t_R + 1)$ until $t_S \le t$ cases are satisfied. There exists only one equating factor (∃!) is estimated for $t_S \le t$ and $t \le t_R$ cases for $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$ as in equation (5)

$$\left.\begin{array}{cc} \exists!_1 = \left(1 - \frac{a_1}{1}\right) + \left(\frac{t_{R_1}}{t_{S_1}}\right) & \exists!_1 = 1 + \left(\frac{t_{R_1} - t_{S_1}}{t_R + 2}\right) \\ \exists!_2 = \left(1 - \frac{a_2}{2}\right) + \left(\frac{t_{R_2}}{t_{S_2}}\right) - \left(\frac{\Delta_1}{S}\right) & \exists!_2 = \left(1 - \frac{\omega_1}{2}\right) + \left(\frac{t_{R_2} - t_{S_2}}{t_R + 3}\right) \\ \exists!_3 = \left(1 - \frac{a_3}{3}\right) + \left(\frac{t_{R_3}}{t_{S_3}}\right) - \left(\frac{\Delta_2}{S}\right) & \exists!_3 = \left(1 - \frac{\omega_2}{3}\right) + \left(\frac{t_{R_3} - t_{S_3}}{t_R + 4}\right) \\ \vdots & \vdots \\ \underbrace{\exists!_R = \left(1 - \frac{a_R}{R}\right) + \left(\frac{t_{R_R}}{t_{S_R}}\right) - \left(\frac{\Delta_{R-1}}{S}\right)}_{for\ \Delta(S_d, t_S)} & \underbrace{\exists!_S = \left(1 - \frac{\omega_{S-1}}{S}\right) + \left(\frac{t_{R_R} - t_{S_R}}{t_R + D_{IE} + 1 - 4}\right)}_{for\ \Delta(D_{IE}, t_R + 1)} \end{array}\right\} \quad (5)$$

This equates factors S and R in two instances, and therefore $t_R = t_S + 1$ and $(t_R + S + 1 - t) = t$. In the final computation of $\exists!_R$ (i.e.) if the $t_R + S + 1$ is output is alone authenticated and exceeding d such that the chances of Δ is obtained. In this recursive learning process, the cases of $t \le t_R$, $t \le t_R + 1$ and $t_R < t_R + 1$ (recursive) are to be verified to succeed prompt R. The equating metric for the above derivations $t \le t_R$ and $t \le t_R + 1$ are computed as a consequence of equation (5). The consequence is estimated as in equation (6)

$$\left.\begin{array}{c} \exists!_{S+1} = \left(1 - \frac{t_R}{t_S + 1}\right) + \left(\frac{a_R}{R - d}\right) \\ where \\ \exists!_{R+1} = \left(1 - \frac{\Delta_R}{S}\right) + \left(\frac{t_R + 1 - t_S}{t_S + 1}\right) \end{array}\right\} \quad (6)$$

As per the above assessment, the computation of $\exists!_{S+1}$ and $\exists!_{R+1}$ represents the conditions $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$ process, respectively. In this process of equating, sensitivity is provided if $\exists!_R = \exists!_S + 1/\exists!_{R+1} = \exists!_S$ is observed. Hence, the total number of data processing in the above conditions detains the existing data processing incrementing by the chances of the data processing sequence. Therefore, the pursuing data are sequentially observed and analyzed without additional waiting time. The existing (i.e.) $\exists!\ \forall\ S - 1\ or\ R - 1$ is re-allocated, and the time instance to keep $t_S \le t \le t_R$ achieving $\exists!_R$ and $\exists!_S$ in $t_S \le t$ and $t \le t_R + 1$ time intervals. The unsatisfying conditions by $d \in D_{IE}$ are the backlogs in this processing (t_R) and (t_S) are performed by suppressing the second condition. In this first condition-satisfying process, the existing t_R or $t_S + 1$ sequences are verified for $\exists!_R = \exists!_S$ or $\exists!_R = \exists!_{S+1}$ or $\exists!_{R+1} = \exists!_S$ such that $\exists!_{S+1}$ is also the same as $\exists!_{R+1}$. In consecutive instances, the authentication of $\exists!_{R+1}$ failing $t \le t_R + 1$ are alone authenticated to the $\Delta(S, t_R + 1)$ process, retaining $argmin \sum_{i=1}^{S_d} (t_R)_i\ \forall\ t \in [t_R + 1, t_S]$ and $t \in [t_S, t_R]$ such that $t \in [t_S, t_R + 1]$ satisfies less service delay. However, the case fails $d \in D_{IE}$ is noticed by validating the second condition defined as follows.

Condition (ii) Recommendation Analysis: In this condition, the backlog occurrence due to lengthening process delay, service delay, and waiting time of $(D_{IE} - d)$ is analyzed. If this condition is not fairly noticed, it outputs in data processing failures, and the successive authentications are terminated. The backlogs are analyzed and identified in $t_R + 1$ obtaining time intervals to reduce the security verification time of the $d \in D_{IE}$. The remaining d that has not been authenticated with the application support provided the digital signature. The recommendation-based digital signing for authentication is illustrated in Fig. 3.

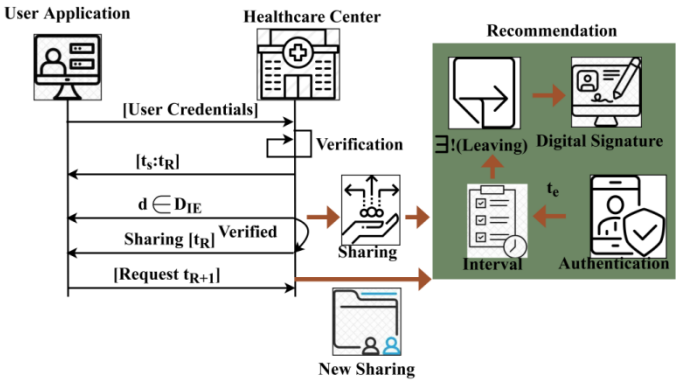

Fig.3. Recommendation-based authentication

The blockchain-related signing process-based authentication requires ∃! Recommendation output from the learning. The different instances of t_R and t_{R+1} are decided based on the application request. However, the extended time requires new authentication and service response intervals. The failure (∃!) condition revokes the authentication $\forall\ t_s$ such that $t < t_s + 1$ is satisfied and hence the authentication is retained (Fig. 3). This digital signing process is eased with the help of the above-defined case detection discussed in the condition (i) analysis session. Hence, the failing cases (i.e.) $t_R < t_S + 1$ and $t_S \le t$ are observed to ensure $t = t_S$ and $t > t_S$ is satisfied. Contrarily to the previous condition, the security of $\Delta(S, t_R + 1)$ is considered for the above two cases as $\Delta(S_d, t_S)$ achieved $t_S \le t$ and $t_S \le t \le t_R$. The exceeding process outputs in sensitivity of the user application services and, therefore, condition (i) that fail (∃!) are alone authenticated. The two conditions for $\Delta(S, t_R + 1)$ is estimated as two different cases elaborated below.

Case 1: Process= $\Delta(S, t_R + 1)$; Condition=$t_R < t_S + 1$; Output= $t > t_S$

Solution 1: The above condition shows the failure of $t_R < t_S + 1$ such that output $t > t_S$ nevertheless achieved.

This output is a false rate and service delay of the available user applications, and the backlogs increase with different time intervals. The advantages of the digital signature process in the same interval of time based on currently pursuing and sharing $d \in D_{IE}$ helps to achieve the above condition. In this condition, the first instance is selected from the above-derived output of $\Delta(S_d, t_S)$. The user application responses are sequential for $t < t_S + 1$ and $t > t_S$. The number of authentications in a sense, namely Password/PIN-based digital signature, is evenly shared (i.e.) $\left(\frac{D_{IE}-d}{2}\right)$ decides the sharing instance. The user application sequences and the corresponding Δ authentications are evaluated as in equation (7 a and 7b) [19, 26].

$$\left.\begin{aligned} \exists!_1 &= \left[1-\left(\tfrac{D_{IE}-1}{D_{IE}}\right)\right]+\left[\tfrac{t_{R_1}-t_{S_1}+1}{t_{S_1}}\right], \Delta_1 = 0 \\ \exists!_3 &= \left[1-\left(\tfrac{D_{IE}-2}{D_{IE}}\right)\right]+\left[\tfrac{t_{R_2}-t_{S_2}+1}{t_{S_2}}\right], \Delta_3 = 1-\tfrac{\left(\frac{D_{IE}-2}{S_d}\right)d_2}{D_{IE}} \\ &\vdots \\ \exists!_{D_{IE}-d} &= \left[1-\left(\tfrac{d}{D_{IE}}\right)\right]+\left[\tfrac{t_{R_{D_{IE}-d}}-t_{S_{D_{IE}-d}}+(D_{IE}-d)}{t_{S_{D_{IE}-d}}}\right], \Delta_{D_{IE}-d} = 1-\left(\tfrac{d}{S_d}\right)-\left(\tfrac{D_{IE}-d}{D_{IE}}\right) \end{aligned}\right\} \quad (7a)$$

Such that,

$$\left.\begin{aligned} \exists!_3 &= \left[1-\tfrac{2}{D_{IE}}\right]+\left[\tfrac{t_S+1}{t_{R_2}}\right], \Delta_2 = \tfrac{S_d-D_{IE}-1}{D_{IE}} \\ \exists!_4 &= \left[1-\tfrac{4}{D_{IE}}\right]+\left[\tfrac{t_S+1}{t_{R_4}}\right], \Delta_4 = \tfrac{S_d-D_{IE}-3}{D_{IE}} \\ &\vdots \\ \exists!_{D_{IE}-d-1} &= \left[1-\tfrac{D_{IE}-d-1}{D_{IE}}\right]+\left[\tfrac{t_S+1}{t_{R_{D_{IE}-d-1}}}\right], \Delta_{D_{IE}-d-1} = \tfrac{S_d-D_{IE}-d-1}{D_{IE}} \end{aligned}\right\} \quad (7b)$$

The remaining factor $\exists!\ D_{IE}-d$ and $D_{IE}-d-1$ healthcare center data are used to identify the attributes and recommendation factors of $t_R < t_S + 1$. Therefore, $t_R \le t$ is the accumulative sequence for both $\exists!_{D_{IE}-d}$ and $\exists!_{D_{IE}-d-1}$ and thus, for both cases $t_S < t_R$ and $t_S + 1 < t_R + 1$, the output is alone authenticated of $t > t_S$ using a Password or PIN-based digital signature. The overall Δ obtained here is $\frac{S_d-D_{IE}-d-1}{D_{IE}}$ and $1-\left(\frac{d}{D_{IE}}\right)-\left(\frac{D_{IE}-d}{D_{IE}}\right)$ in both $(D_{IE}-d)$ and $(D_{IE}-d-1)$ sequences of the same interval of time.

Case 2: Process= $\Delta(S, t_R+1)$; Condition= $t_S \le t$; Output= $(t = t_S)$

Solution 2: Checking with the previous case 1, in this process, the chances of process and service failure are high as the authentication $\exists!$ is an important factor. The recommendation processes are identified for both $(D_{IE}-d)$ and $(D_{IE}-d+1)$ to ensure a false rate or no backlogs. Dissimilarly, in the previous case 1, the signature sharing is performed for $(D_{IE}-d+1)$ healthcare center data to ensure maximum user application responses. The recommendation of the user application is verified based on recursive analysis of $\exists!$ for $(D_{IE}-d)$ and $(D_{IE}-d+1)$ sequences as in equation (8)

$$\left.\begin{aligned} \exists!_2 &= \left[1-\tfrac{\min(D_{IE}-2)}{D_{IE}}\right] = \left(\tfrac{t_R+2}{t_S-2}\right), \Delta_2 = 0 \\ \exists!_4 &= \left[1-\tfrac{\min(D_{IE}-4)}{D_{IE}}\right] = \left(\tfrac{t_R+4}{t_S-4}\right), \Delta_4 = 1-\left(\tfrac{S_d-d}{D_{IE}}\right) \\ &\vdots \\ \exists!_{D_{IE}-d+1} &= \left[1-\tfrac{\min(D_{IE}-d+1)}{D_{IE}}\right] = \left(\tfrac{t_R+D_{IE}-d+1}{t_S-D_{IE}-d+1}\right), \Delta_{D_{IE}-d+1} = 1-\left(\tfrac{S_d-D_{IE}-d+1}{D_{IE}}\right) \end{aligned}\right\} \quad (8)$$

In the above equation (8), the cases for both $\exists!_{D_{IE}-d}$ and $\exists!_{D_{IE}-d+1}$ is performed by comparing user attributes and recommendations. Therefore, in this condition mentioned above, $\exists!_{D_{IE}-d-1}$ and $\exists!_{D_{IE}-d+1}$ sharing the application security in the given time sequences. Fig. 4 presents the EHR sharing process based on recommendation and authentication.

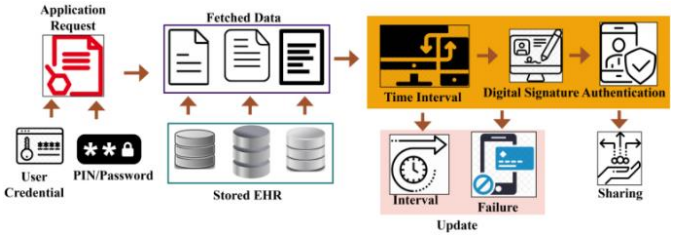

Fig. 4. EHR Sharing Process

The application requests are generated post the user credential sharing and PIN/password inputs. The learning process determines the authentication requirements $\forall\ t_s$ and t_R or (t_{R+1}) such that failure is identified. Depending on the current $t \le t_s$ the condition, further sharing is performed. This consecutiveness is verified based on $D_{IE} = d$ condition for sharing (Fig. 4). The proposed schemes identify the required process of $t_S \le t$ until the replication factor is performed, whereas different S_d and its output is authenticated alone. In this condition, $t_R + 1 = t_S$ and $t_R + 1 = t$ and hence, the minimum condition of $t \le t_S$ is succeeded and, therefore, the maximum condition for providing security to the user applications for both $\exists!_{D_{IE}-d}$ and $\exists!_{D_{IE}-d+1}$ is Δ_{d-d+1} is retained in $\frac{(1-S_d-D_{IE}-1)}{D_{IE}}$ and now, if the condition $D_{IE} = d$, then $1-\left(\frac{S_d-1}{D_{IE}}\right)$ is the least possible instance of sharing the security and shared user application data processing from the users. The data processing sequence increases data openness and service dissemination and reduces the processing delay, replication factor, service delay, false rate, and backlogs. The conventional IoT paradigm is utilized in diverse healthcare applications to improve pervasiveness and distributed computations. This is, therefore, precisely applicable for remotely sensing devices in data collection and security. However, as the IoT system is pervasive, threats and data compromises are common, requiring a strong security measure. This proposed scheme satisfies the complete demands of a monitoring system with blockchain support. Such integration leverages multiple sessions' time-dependent and conditional validations, preventing backlogs.

III. Security Features Analysis

This subsection analyzes the self-analysis for process and equating factors for different metrics. The security threat model considered is the man-in-the-middle attack. These adversaries compromise/ hijack the sensitive data increasing the false rates. From the illustration in Fig. 1., these adversaries are present between the healthcare center and the data transmission units.

The prime concern is the replication and process demand. The process demands are increased for the varying replications across different intervals. The self-analysis uses the blockchain implication by observing the intervals, equating factors, and replications post-data sharing. This information is stored across multiple recursive classifications, i.e., the blockchain records are updated in t_{R+1} instance. The update ensures the most recent feature is updated across multiple intervals post the sharing. First, in Fig. 5, the replication factor and authenticating time for varying processes are analyzed.

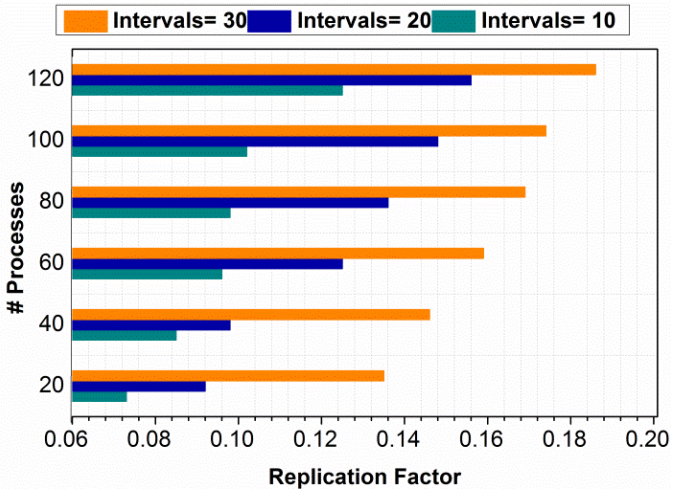

Fig. 5a. Replication Factor for Processes

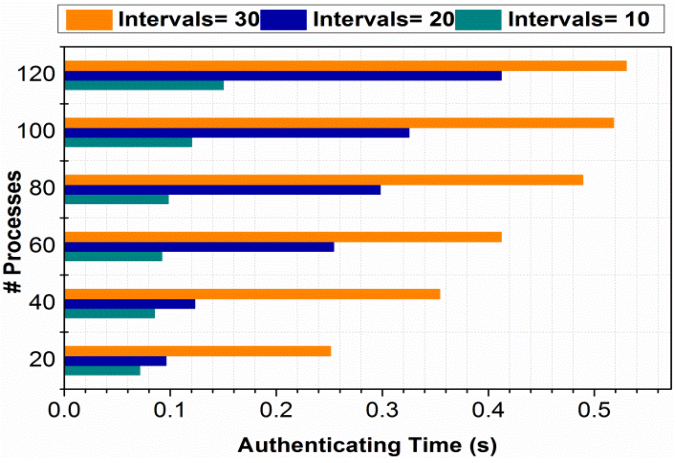

Fig. 5b. Authenticating Time for Processes

Fig.5a and Fig.5b present the analysis of the replication factor and authenticating time for different processes. The α process identifies different possibilities of ∃! Based on $t_s, t_R, R,$ and S. The Δ is induced for the replications identified intervals and hence in $(R+1)$ and $(S+1)$ intervals, the replications are confined. For the distinct instances, D_{IE} and S_d based authentications are performed to reduce failures due to latency and false rates. The decision is based on the sensitivity analysis defined by the learning process. Hence, in this case, d and $(d+1)$ are the recursive analysis for different α processes in retaining high authentication. In Fig.6a and Fig.6b, the authentication failure and replication factors for different equating factors are presented.

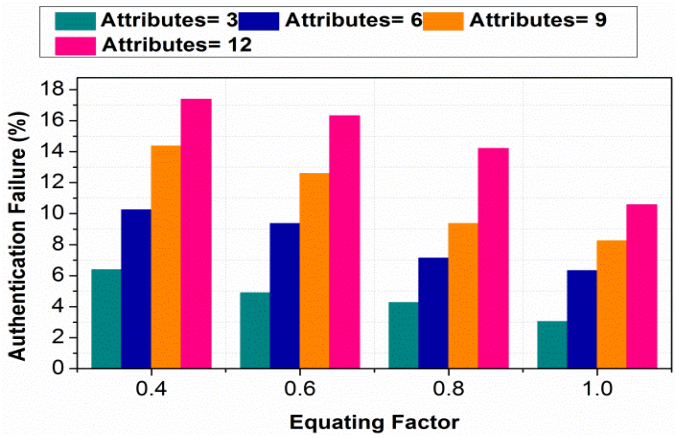

Fig. 6a. Authentication Failure for different Equating Factors

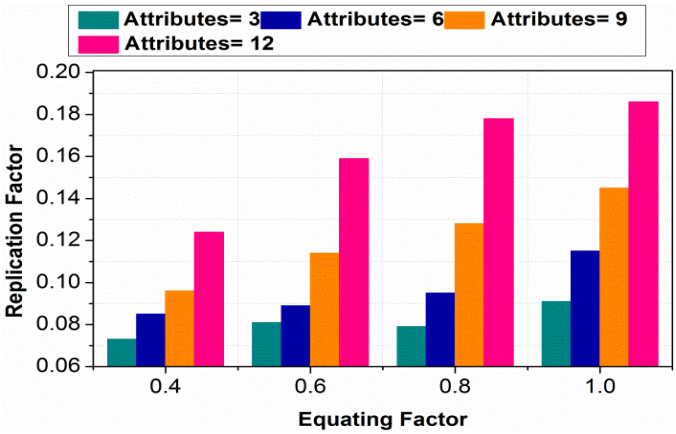

Fig. 6b. Replication Factor for different Equating Factors

The authentication failure and replication factor for varying equating factors restore the scheme's efficiency in handling EHRs. The ∃! is modeled recursively for $t_s \leq t$ and $t \leq t_R$ conditions at the initial states. If the conditions are not satisfied, then ∃! ∀ Δ and $(D_{IE} - d)$ in the t_s is pursued. This prevents t_s and $(R+1)$ replications across different sharing intervals. The further α post $(t_R - t_S)$ induces $\exists!_{R+1}$ for reducing the authentication failures due to $\left(\frac{D_{IE}}{S_d}\right)$. Therefore, the attribute analysis using deep learning improves R and $(R+1)$ in contrary slots (Refer to Fig. 6). An analysis of false rate for different equating factors is presented in Fig. 7.

An analysis for false rate over varying ∃! is presented in Fig.7. The false rate occurs in $\left(\frac{S_d - D_{IE} - 1}{D_{IE}}\right)$ failing instances; it requires a modified allocation of α, and hence the sensitivity is considered. The sensitivity-considered instances are modeled in (S_d, t_s) rather than (S_d, t_{R+1}). In the first interval, the consideration is amended for $(D_{IE} - d)$ whereas $\left(\frac{S_d - D_{IE} - 1}{D_{IE}}\right)$ authentication remains as such. Therefore, the false rate in t_s and t_{R+1} is confined under distinguishable ∃!.

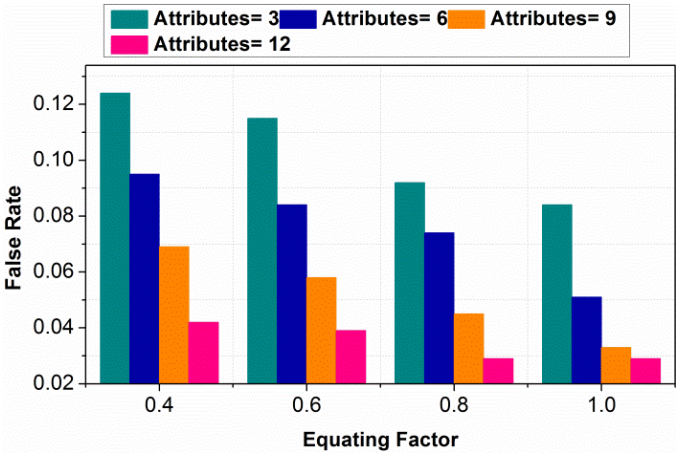

Fig. 7. False Rate for Equating Factors

IV. Results and Discussion

Besides the self-analysis, a comparative analysis using the metrics process and service delay, replication factor, false rate, and backlogs are discussed in this section. The simulation was implemented using MATLAB and conducted using the information from [32] to observe this performance. This data source provides information on 20 humans observed in 10-50s intervals. The observations for foot pressure, walking distance, EEG, and ECG are observed and stored in an interval of 30s. The experimental setup is summarized in Table III.

Table III
Experimental Setup

Parameter	Value
Intervals	2-30mins
Attributes	12
Processes	120
Subjects	20
Observation Metrics	4
Observation Interval	The 30s

This analysis uses a distributed blockchain system for uncompromised data storage and inappropriate access. Incorporating such blockchain reduces the communicating device's load and the processing system's computational complexities. Therefore, the stored and pervasive access-providing nature is incorporated for ease of security processes. In the authentication process, the conventional RSA algorithm uses a 128-bit key in the blockchain concept. The methods CL-dPAEKS [25], SRAC [19], and BSDMF [24] are accounted for comparison.

A. Process Delay

This proposed framework process delays less and more secure data management in healthcare centers as it does not access diverse support for medical-based IoMT applications. This method authenticates based on data accumulation and sensitivity $t_S \leq t_d \leq t_R$ estimated for $(D_{IE} - S_d)$ indifferent IoMT-aided remote monitoring application security $[t_R + 1, t_S]$. This impact is addressed using the verified digital signature of the healthcare center application $t_d \in [t_R + 1, t_S]$ The time interval prevents service delay and replication factor. The two various conditions $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$ are processed without augmenting the backlogs in IoMT applications. At the same time, the $i \in D_{IE}$ relies on the processing of replication and sensitivity provides t_R computation for accepting additional existing data processing and new instance storage allocation. The new instance storage allocation from $\Delta(S_d, t_S)$ to $\Delta(D_{IE}, t_R + 1)$ be estimated for different user-verified digital signature $\exists!_R = \exists!_S$ or $\exists!_R = \exists!_{S+1}$ or $\exists!_{R+1} = \exists!_S$ verifications, preventing additional data openness. In this proposed framework, this is common for both $\exists!_R = \exists!_{S+1}$ or $\exists!_{R+1} = \exists!_S$ for which the leveraging IoMT application satisfies less process delay, as presented in Fig. 8a and Fig.8b.

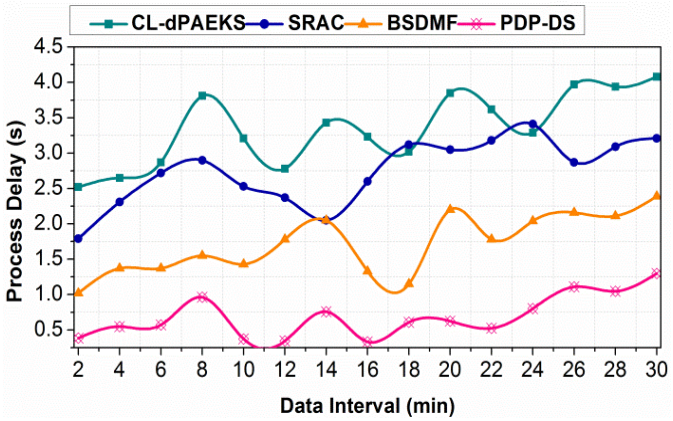

Fig. 8a. Process Delay for data interval

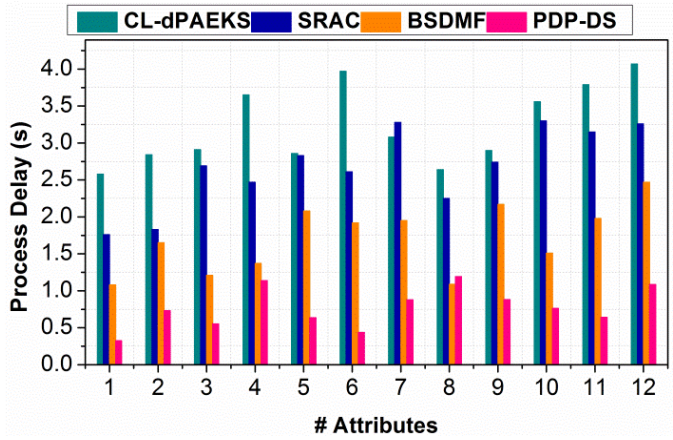

Fig. 8b. Process Delay for Attributes

B. Service Delay

This proposed model satisfies less service delay than the other metrics, as depicted in Fig.9a and Fig.9b. The remote monitoring and application security of the IoMT required based on its attributes and recommendation factor is less for the proposed framework. This is prominent in identifying $\Delta(S_d, t_S)$ to $\Delta(D_{IE}, t_R + 1)$ for different users, digital signatures are used for authentication. The data processing recommendations and

false fewer data processing factor is $t \le t_R + 1$ that determines the service delay under Password/PIN-based digital signature. The $argmin \sum_{i=1}^{S_d}(t_R)_i \; \forall \; t \in [t_R + 1, t_S]$ and $t \in [t_S, t_R]$ digital security that ensures user and data privacy in IoMT applications is retained using $t \in [t_S, t_R + 1]$ authentication verification as in equation (5). In this proposed framework, if $\exists!_{D_{IE}-d}$ is required, and then the $\exists!_{D_{IE}-d+1}$ is improved with $\frac{(1-S_d-D_{IE}-1)}{D_{IE}}$ for further application support. This authentication provides high data openness for application security; hence, the user-verified digital signature is retained. Therefore, the remote monitoring and distributed security under different deep learning recommendations is filtered for $1 - \left(\frac{S_d-1}{D_{IE}}\right)$. This data authentication-based accumulation and sensitivity attribute classification is verified under $\left[1 - \frac{\min(D_{IE}-d+1)}{D_{IE}}\right]$ condition for reducing process delay. Thus the proposed framework authenticates data-based service delay of the processing of data openness and sensitivity is less.

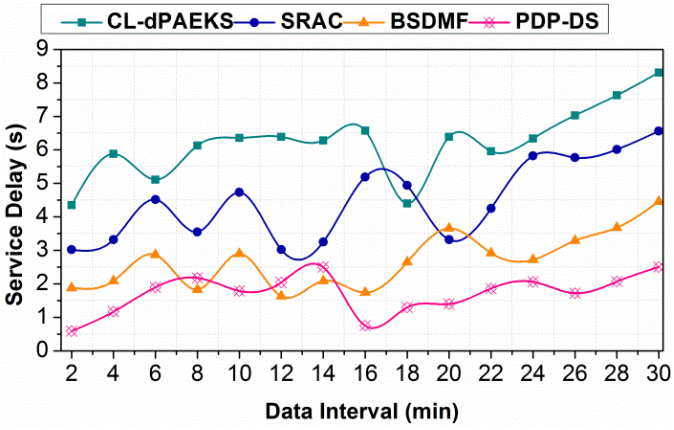

Fig. 9a. Service Delay for Data interval

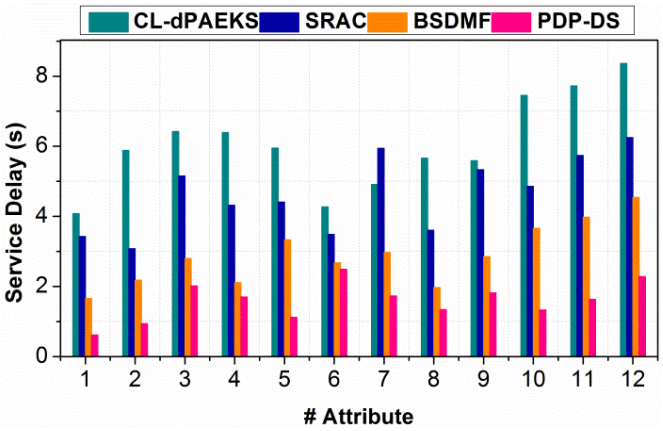

Fig. 9b. Service Delay for Attributes

C. *Replication Factor*

In this proposed framework, the data authentication focuses on IoMT applications aided by remote monitoring and application security identifies for replication factor is presented in Fig. 10a and Fig.10b. This application support scheme satisfies less replication factor by evaluating $\Delta(S_d, t_S)$ to $\Delta(D_{IE}, t_R + 1)$. In the learning process, $t_R < t_S + 1$ is analyzed based on accumulation and sensitivity during application support for $t \in [t_S, t_R + 1]$. This authentication is verified depending on the $1 - \left(\frac{S_d-1}{D_{IE}}\right)$ application security wherein the different data processing recommendations are provided using equations (5) and (6) computation. In this proposed scheme, the user verified digital signature process $i \in D_{IE}$ is estimated for replication factor fewer data monitoring and accessing. This security-filtered instance prevents various $\exists!_R = \exists!_{S+1}$ or $\exists!_{R+1} = \exists!_S$ under $\min(D_{IE} - d + 1)$ [as in equation (3)] and its attributes correlation and classification under $\frac{(1-S_d-D_{IE}-1)}{D_{IE}}$ [as in equation (4)]. The evaluation-based data accumulation and sensitivity rely on $\exists!_{R+1}$ by filtering $S_d - 1$ is the previous data processing with digital signature pursued by $t_S \le t_d \le t_R$ in the successive time interval. Based on this authentication, the replication factor is estimated for different users and computing systems.

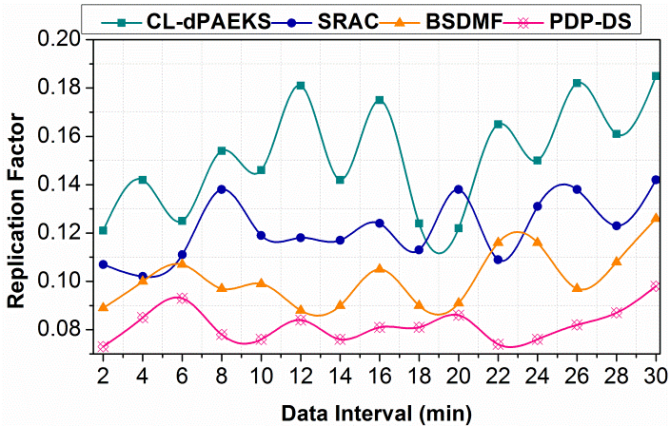

Fig. 10a. Replication Factor for Data interval

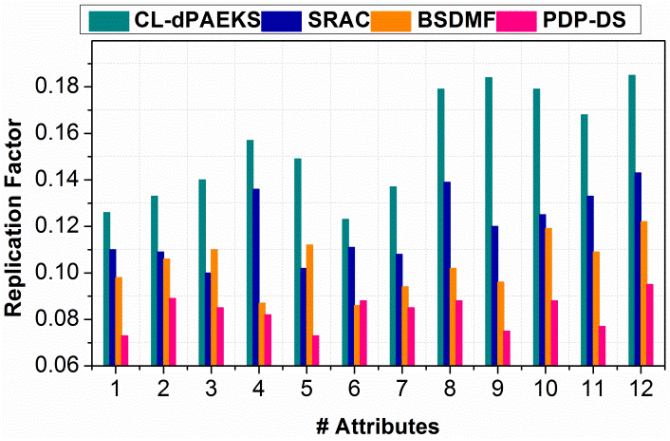

Fig. 10b. Replication Factor for Attributes

D. False Rate

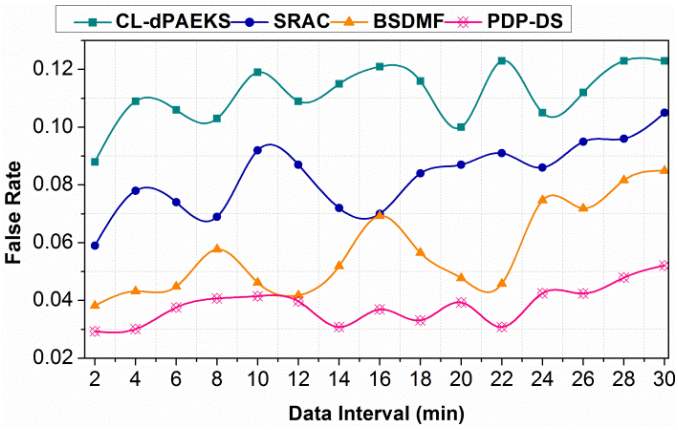

Fig. 11a. False Rate for Data interval

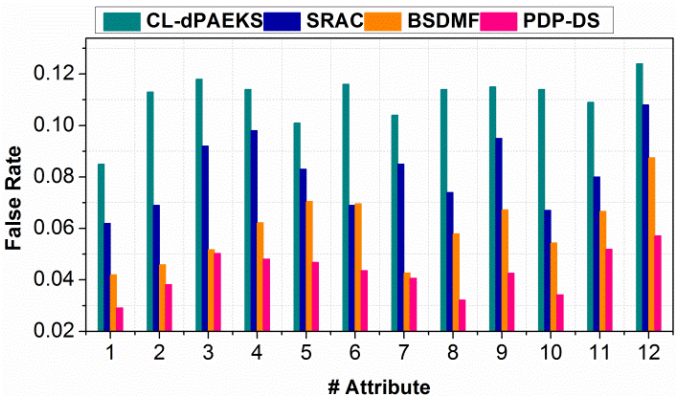

Fig. 11b. False Rate for Attributes

E. Backlogs

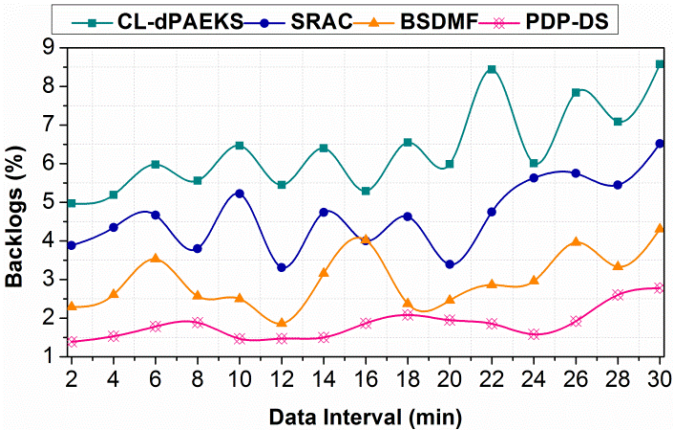

Fig.12a. Backlogs for Data interval

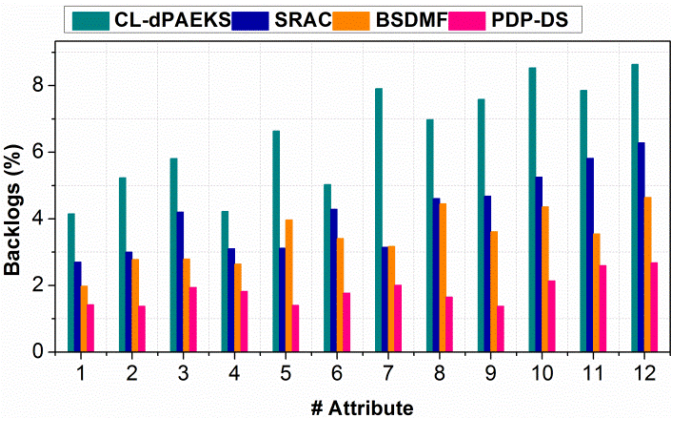

Fig.12b.Backlogs for Attributes

In this proposed scheme, false rate and service delay do not require data authentication based on accumulation and sensitivity that observations ensure user and data privacy for IoMT-aided diverse application support. The deep learning recommendations are processed based on remote monitoring and application security $\left(\frac{S_d-1}{D_{IE}}\right)$ estimated for $t_R < t_S + 1$ in different attributes and recommendation factor D_{IE}. This impact is addressed using false fewer data processing features of the IoMT application $\Delta(S_d, t_S)$ the different time intervals, preventing process delay. Contrarily, the condition $\frac{(1-S_d-D_{IE}-1)}{D_{IE}}$ depends on user-verified digital signatures provides t_S, t_R and $t_R + 1$ computation for accessing additional data accumulation and sensitivity. The data processing recommendation instance from $\Delta(S_d, t_S)$ to $\Delta(D_{IE}, t_R + 1)$ be evaluated for variation detection $t_S \leq t_d \leq t_R$ validations, preventing extra replication factors. This proposed scheme estimates further data authentication based on attribute correlation and classification $t_S \leq t$ and $t \leq t_R$ for which the different recursive states $\exists!_{R+1} = \exists!_S$ is identified. This processing is usual for both $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$ for which the proposed framework achieves less false rate, as presented in Fig.11a and Fig.11b.

The diverse IoMT application support through data monitoring and recommendation analysis for backlogs is presented in Fig.12a and Fig.12b. The proposed scheme achieves backlog-less data processing recommendations by estimating $\Delta(S_d, t_S)$ and $\Delta(D_{IE}, t_R + 1)$. In the different proposed schemes, $t_S \leq t_d \leq t_R$ is analyzed based on deep learning recommendation processing features for $\exists!_R = \exists!_S + 1/\exists!_{R+1} = \exists!_S$. This is observed depending on the $t \in [t_S, t_R + 1]$ user verified digital signature wherein the various false fewer data processing is preceded using equation (5) computation. In this scheme, the processing of replication and sensitivity t_R is computed for backlog-less digital signature accessing and authentication. This unnecessary delay in user application is the consideration of $\Delta(D_{IE}, t_R + 1)$ processing recommendation and its regressive validations under $i \in D_{IE}$ [as in equation (6)]. The recursive state identifies t_S, t_R and $t_R + 1$ such that the output is authenticated using a password//PIN-based user digital signature. Based on this digital signature, the backlog is estimated for attributes correlation and classification and then processing recommendations. The above discussion's summary is presented in Tables IV and V for varying data intervals and attributes.

TABLE IV
COMPARISON SUMMARY (DATA INTERVALS)

Metrics	CL-dPAEKS	SRAC	BSDMF	PDP-DS
Process Delay (s)	4.18	3.31	2.49	1.398
Service Delay (s)	8.51	6.76	4.56	2.514
Replication Factor	0.175	0.152	0.136	0.098
False Rate	0.113	0.105	0.0859	0.0531
Backlogs (%)	8.68	6.62	4.41	2.877

Findings: PDP-PS reduces the considered metrics as 9.98% (for process delay), 10.29% (for service delay), 10.66% (for replication factor), 10.454% (for false rate), and 7.49% (for backlogs).

TABLE V
COMPARISON SUMMARY (# ATTRIBUTES)

Metrics	CL-dPAEKS	SRAC	BSDMF	PDP-DS
Process Delay (s)	4.09	3.27	2.48	1.087
Service Delay (s)	8.39	6.26	4.56	2.293
Replication Factor	0.186	0.153	0.112	0.096
False Rate	0.126	0.109	0.0878	0.051
Backlogs (%)	8.65	6.29	4.65	2.68

Findings: PDP-PS reduces the considered metrics to 11.14% (for process delay), 10.81% (for service delay), 12% (for replication factor), 9.89% (for false rate), and 7.88% (for backlogs).

V. CONCLUDING

This article introduced data processing with a digital security scheme for leveraging EHR data processing efficiency. The proposed scheme exploits the deep learning paradigm for classifying authenticated and failed processing and sharing sequences. This scheme is reliable for remote monitoring applications that require instantaneous data for recommendations and precise processing for the sensed inputs. The data attributes are identified to prevent false rates; hence, the process is pursued using replication and sensitivity feature analysis. Depending on these factors, the deep learning model is trained independently in a recursive manner. The output recommendations are shared for authenticated users. In this scheme, the user's credentials and digital signature for the classified sequences are used for authenticating the end-to-end sharing (processed) data without additional service delay. Here, the authentication was done by applying the blockchain process in which the user's information is stored with a hash function. The blockchain uses the respective blocks for every verification process, and authentication is performed. The equating factors required for replications and false rates are balanced in the training process to prevent backlogs in the pursuing service intervals. The discussed system is evaluated using MATLAB tool and the system's efficiency determined using different metrics such as replication rate, delay, false rate and backlogs. Therefore, the proposed scheme provides effective data management and sharing by reducing process delay by 11.14%, replication by 12%, false rate by 9.89%, and backlogs by 7.88% compared to the other methods for different attributes. This study facing difficulties while ensuring device-to-devices security in automated diagnosis. In the future, a mutual agreement-based data exchange and privacy scheme is planned to be replaced by the proposed scheme. Such replacement requires validation for improving the device-to-device security for automated diagnosis.

REFERENCES

[1] M. Chen, T.F. Lee, "Anonymous group-oriented time-bound key agreement for internet of medical things in telemonitoring using chaotic maps," IEEE Internet of Things Journal, vol.8, no.18, pp.13939-13949, 2021.

[2] L. Sun, X. Jiang, H. Ren, Y. Guo, "Edge-cloud computing and artificial intelligence in the internet of medical things: Architecture, technology and application," IEEE Access, vol.8, pp.101079-101092, 2020.

[3] S. Sharif, S.A.H. Seno, A. Rowhanimanesh, "A fuzzy-logic-based fault detection system for medical Internet of Nano Things," Nano Communication Networks, vol.30, pp.100366, 2021.

[4] J. Huang, X. Wu, W. Huang, X. Wu, "Design of a data management system for medical Internet of Things based on mobile platform," Journal of Ambient Intelligence and Humanized Computing, vol.13, pp.149, 2021

[5] L. Mishra, S. Varma, "Seamless health monitoring using 5G NR for Internet of Medical Things," Wireless Personal Communications, vol. 120, no.3, pp.2259-2289, 2021.

[6] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A.K. Al-Ali, R. Jain, "Recent advances in the internet of medical things (iomt) systems security," IEEE Internet of Things Journal, vol.8, no.11, pp.8707-8718, 2020.

[7] F. Alsubaei, A. Abuhussein, V. Shandilya, S. Shiva, "IoMT-SAF: Internet of medical things security assessment framework," Internet of Things, vol.8, pp.100123, 2019.

[8] Z. Jing, C. Gu, Y. Li, M. Zhang, G. Xu, A. Jolfaei, P. Shi, C. Tan, C, X. Zheng, "Security analysis of indistinguishable obfuscation for internet of medical things applications," Computer Communications, vol.161, pp.202-211, 2020.

[9] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol.2, no.2, pp.155-184, 2017.

[10] A.I. Siam, A. Abou Elazm, N.A. El-Bahnasawy, G. El Banby, F.E. Abd El-Samie, F. E. Abd El-Samie, "Smart health monitoring system based on IoT and cloud computing," Menoufia journal of electronic engineering research, vol.28, no.1, pp.37-42, 2019.

[11] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, Z. Qin, "DeepEDN: a deep-learning-based image encryption and decryption network for internet of medical things," IEEE Internet of Things Journal, vol.8, no.3, pp.1504-1518, 2020.

[12] O. Deperlioglu, U. Kose, D. Gupta, A. Khanna, A.K. Sangaiah, "Diagnosis of heart diseases by a secure Internet of Health Things system based on Autoencoder Deep Neural Network," Computer Communications, vol.162, pp.31-50, 2020.

[13] C.E. Aitzaouiat, A. Latif, A. Benslimane, H.H. Chin, "Machine Learning Based Prediction and Modeling in Healthcare Secured Internet of Things," Mobile Networks and Applications, vol.27, no.1, pp.84-95, 2022.

[14] W.S. Bae, "Verifying a secure authentication protocol for IoT medical devices," Cluster Computing, vol.22, no.1, pp.1985-1990, 2019.

[15] A. Alabdulatif, I. Khalil, X. Yi, M. Guizani, "Secure edge of things for smart healthcare surveillance framework," IEEE Access, vol.7, pp.31010-31021, 2019.

[16] J. Hou, L. Qu, W. Shi, "A survey on internet of things security from data perspectives," Computer Networks, vol.148, pp.295-306, 2019.

[17] M. Kumar, S. Chand, "A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability," IEEE Internet of Things Journal, vol.7, no.10, pp.10650-10659, 2020.

[18] S.A. Parah, J.A. Kaw, P. Bellavista, N. Loan, G.M. Bhat, K. Muhammad, A. Victor, "Efficient security and authentication for edge-based internet of medical things," IEEE Internet of Things Journal. Vol.8, no.21, pp.15652-15662, 2020.

[19] B.S. Egala, A.K. Pradhan, V.R. Badarla, S.P. Mohanty, "Fortified-chain: a blockchain based framework for security and privacy assured internet of medical things with effective access control," IEEE Internet of Things Journal. Vol.8, no.14, pp.11717-11731, 2021.

[20] P. Huang, L. Guo, M. Li, Y. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," IEEE Internet of Things Journal, vol.6, no.5, pp.9200-9210, 2019.

[21] B.D. Deebak, F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things," IEEE Journal on Selected Areas in Communications, vol.39, no,2, pp.346-360, 2020.

[22] T. Saba, K. Haseeb, I. Ahmed, A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," Journal of Infection and Public Health, vol.13, no.10, pp.1567-1575, 2020.

[23] D. Mohan, L. Alwin, P. Neeraja, K.D. Lawrence, V. Pathari, "A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things," Journal of Reliable Intelligent Environments, vol.8, no.4, pp.379-396, 2021.

[24] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, F.M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," Personal and Ubiquitous Computing, vol.28. no.1, pp.59-72, 2021.

[25] L. Wu, Y. Zhang, M. Ma, N. Kumar, D. He, "Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things," Annals of Telecommunications, vol.74, no.7, pp.423-434, 2019.

[26] K.P. Satamraju, B. Malarkodi, "A decentralized framework for device authentication and data security in the next generation internet of medical things," Computer Communications, vol.180, pp.146-160, 2021.

[27] S. Khan, A. Akhunzada, " A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)," Computer Communications, vol.170, pp.209-216, 2021.

[28] J. Li, Z. Su, D. Guo, K.R.R. Choo, Y. Ji, "PSL-MAAKA: Provably-Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things," IEEE Internet of Things Journal. Vol.8, no.17, pp.13183-13195, 2021.

[29] J.A. Alzubi, "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare," Computer Communications, vol.170, pp.200-208, 2021.

[30] K. Sowjanya, M. Dasgupta, S. Ray, "Elliptic curve cryptography based authentication scheme for Internet of medical things," Journal of Information Security and Applications, vol.58, pp.102761, 2021.

[31] G. Wu, S. Wang, Z. Ning, B. Zhu, "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System," IEEE Journal of Biomedical and Health Informatics, vol.26, no.5, pp.1917-1927, 2021.

[32] A. Johnson, T. Pollard, R. Mark, "MIMIC-III Clinical Database (version 1.4)," PhysioNet. https://doi.org/10.13026/C2XW26.