processes

MDPI

Article

A Deep-Learning Neural Network Approach for Secure Wireless Communication in the Surveillance of Electronic Health Records

Zhifeng Diao [1] and Fanglei Sun [2,*]

[1] College of Design and Innovation, Tongji University, Shanghai 200092, China
[2] School of Creativity and Art, ShanghaiTech University, Shanghai 201210, China
* Correspondence: sunfl@shanghaitech.edu.cn

Abstract: The electronic health record (EHR) surveillance process relies on wireless security administered in application technology, such as the Internet of Things (IoT). Automated supervision with cutting-edge data analysis methods may be a viable strategy to enhance treatment in light of the increasing accessibility of medical narratives in the electronic health record. EHR analysis structured data structure code was used to obtain data on initial fatality risk, infection rate, and hazard ratio of death from EHRs for prediction of unexpected deaths. Patients utilizing EHRs in general must keep in mind the significance of security. With the rise of the IoT and sensor-based Healthcare 4.0, cyber-resilience has emerged as a need for the safekeeping of patient information across all connected devices. Security for access, amendment, and storage is cumulatively managed using the common paradigm. For improving the security of surveillance in the aforementioned services, this article introduces an endorsed joint security scheme (EJSS). This scheme recognizes the EHR utilization based on the aforementioned processes. For each process, different security measures are administered for sustainable security. Access control and storage modification require relative security administered using mutual key sharing between the accessing user and the EHR database. In this process, the learning identifies the variations in different processes for reducing adversarial interruption. The federated learning paradigm employed in this scheme identifies concurrent adversaries in the different processes initiated at the same time. Differentiating the adversaries under each process strengthens mutual authentication using individual attributes. Therefore, individual surveillance efficiency through log inspection and adversary detection is improved for heterogeneous and large-scale EHR databases.

Keywords: security; electronic health record; federated learning; IoT

Citation: Diao, Z.; Sun, F. A Deep-Learning Neural Network Approach for Secure Wireless Communication in the Surveillance of Electronic Health Records. *Processes* **2023**, *11*, 1329. https://doi.org/10.3390/pr11051329

Academic Editor: He Fang

Received: 3 March 2023
Revised: 18 April 2023
Accepted: 20 April 2023
Published: 25 April 2023

1. Introduction

Every health-care center maintains an electronic health record (EHR) system. EHR contains various details that are relevant to a patient's medical health conditions. The Internet of Things (IoT) network is mostly used in EHR, enhancing patient performance and communication services [1]. Ensuring the safety and security of users' data are complicated tasks to perform in IoT-based EHR systems. Various methods and techniques are used as security measures in IoT-based EHR. A lightweight encryption algorithm is used in the authentication process [2]. The encryption algorithm identifies the exact patterns and features of data that the users produce. A lightweight encryption algorithm-based security framework is mostly used for EHR security management systems [3]. A wireless sensor network (WSN) is also used in EHR, which ensures patient data from third-party members. Wireless sensors are used in every WSN system that gathers relevant information for further processes. WSN checks the exact content related to users, reducing the error ratio in the authentication process. WSN improves the safety and security of user data, enhancing the systems' feasibility and efficiency [4].

EHR contains sensitive data, which leads to various security problems and threats. Access control provides necessary services and schemes to secure patients' data from attackers. Access control in EHR aims to prevent health records from illegal actions [5]. A blockchain-based access control policy is mostly used in IoT-based EHR systems [6]. Blockchain identifies both fiducial and non-fiducial features that are present in a database. The blockchain approach reduces computation's overall latency and energy consumption ratio, improving access control policies' performance [7]. A non-cryptographic approach is also used in the EHR data access control process. An anonymization algorithm is used in a cryptographic approach that protects information from third-party members [8]. A ciphertext-policy attribute-based encryption (CP-ABE) method is used for EHR data sharing in IoT systems. CE-ABE uses an encrypted method to secure data while sharing one user with another user. CE-ABE minimizes the error range in data sharing, which maximizes the efficiency of the systems [9].

Machine learning (ML) methods and algorithms are used in various fields and applications. ML is mainly used for detection processes. An ML algorithm is also used for EHR security management systems [10]. A convolutional neural network (CNN) algorithm in EHR detects the exact threats from the system. CNN identifies the actual cause of the problems that produce an optimal solution to solve those problems. CNN uses a feature extraction method that extracts the important features and patterns from the database [11,12]. A support vector machine (SVM) algorithm-based approach is also used for the security detection process. SVM detects the threats and problems that occur in EHR management systems. SVM reduces the computation process's latency and energy consumption range [13]. SVM classifies security threats based on certain classification and optimization processes. SVM improves the overall security and safety of EHR from third-party members [14]. Deep reinforcement learning (DRL)-based authentication is also used in EHR and protects user data from the attackers. DRL provides an optimal authentication scheme to users that secures EHR data. DRL reduces the error ratio in the authentication process [12,15].

The suggested system is geared on protecting private medical information during storage and retrieval. Relative security, in which the user and the EHR database share keys, is necessary for access control and storage change. The learning procedure identifies the differences between several procedures for mitigating hostile interference. There is a strict order to the suggested method's storage and retrieval procedures based on federated learning judgments. The circumstances analyzed by the learning paradigm make the choices necessary to recognize security variances across subsequent sequences. Two primary goals stand out: efficient two-way communication, and careful tracking of patients' health and medication use.

The article is organized as follows. Section 2 overviews the relevant literature. Section 3 explains the endorsed joint security system, and Section 4 offers a comparative and experimental study. Section 5 of the report summarizes the findings and concludes.

2. Related Works

Sun et al. [16] introduced a new approach for cloud-based secure electronic health records (EHR). The actual aim of the proposed approach is to secure EHR data from third-party members. EHR is mainly used to store electrocardiograph (ECG) data, providing optimal information for further diagnosis processes. The performance evaluation method is used here that evaluate the actual content and features of the patient's data. The introduced approach improves the performance range of real-time health-care applications.

Madine et al. [17] designed a multiparty consent management for data sharing of patient health records (PHR). The multiparty authorization (MPA) method is implemented in management that secures health-care data during data sharing. The secret key is implemented in every data-sharing process, which reduces the overall risks and threats in sharing. Experimental results show that the proposed MPA maximizes accuracy and secu-

rity in PHR data sharing. The proposed method increases the performance and robustness level of PHR systems.

Wang et al. [18] proposed a consortium blockchain-based privacy-preserving patient health record (PHR) management and sharing scheme for health-care centers. PHR is maintained in hospitals that provide the necessary medical data of patients. PHR data sharing provides accurate datasets, which increase accuracy in decision-making and diagnosis processes. Consortium blockchain provides proper authentication and authorization process to the users, which protect data from the attackers. The proposed method enhances the efficiency and reliability of PHR systems.

Wei et al. [19] developed a revocable storage and hierarchical attribute-based access control (RS-HABE) scheme for data sharing in electronic health record (EHR) systems. The proposed RS-HABE scheme provides a proper solution to ensure the safety of medical data. The RS-HABE scheme secures the data which are transmitted during data sharing. The proposed scheme increases the accuracy of data sharing, improving the systems' performance and feasibility.

Zhu et al. [20] introduced an improved Merkle tree-based blockchain electronic medical record (EMR) secure storage scheme. The convolutional layer structure is implemented in EMR systems that provide various services to the users. The introduced scheme reduces the complexity and latency in data sharing and further processes. Merkle tree calculates the exact content of EMR data. When compared with other schemes, the introduced scheme maximizes the security range of EMR data in health-care centers.

Zaghloul et al. [21] proposed a distributed multilevel electronic medical record (d-EMR) management scheme. Blockchain technology is used here to identify the security threats that occur during data sharing. The main aim of the proposed scheme is to handle EMR data while sharing. Blockchain technique reduces the latency and energy consumption ratio in threat identification, improving the systems' energy-efficiency level. The proposed d-EMR scheme enhances the safety, security and privacy of EMR data against third-party members.

Olakanmi et al. [22] designed a new fog-enhanced expressible access control scheme (FEACS) for security management in electronic health systems. The main aim of the proposed scheme is to improve the health-care delivery range in health-care systems. The proposed method provides effective information for diagnosis and decision-making processes in health-care centers. The proposed FEACS increases the performance and efficiency levels of electronic health systems.

Shuaib et al. [23] developed a blockchain-based health-care data-sharing system. Blockchain technology is mainly used here to address the problems that occur during data sharing and storage processes. Blockchain increases privacy and security policies in health-care centers. The proposed scheme increases the accuracy range in data sharing, which reduces latency in transactions. Experimental results show that the proposed scheme improves the effectiveness and performance range of the data-sharing system.

Hurst et al. [24] introduced a new machine learning (ML) approach for security management in electronic health records. ML approach detects the exact problems which are presented in health-care centers. A decision tree is also used here that classifies the threats based on certain conditions and patterns. A decision tree reduces the complexity of security management systems. The introduced approach increases the safety and security of user data, enhancing the systems' efficiency and reliability level.

Chen et al. [25] introduced a secure electronic medical record (EMR) authorization method for cloud computing environments. The actual goal of the proposed method is to track the key values for the encryption process. EMR contains various sensitive values which provide necessary information for the diagnosis process. Both private and public clouds are used here that provide various data for further processes. The proposed method improves the accuracy in decision-making that maximizes the security level of health-care centers.

Abbas et al. [26] proposed a blockchain-assisted secure data management framework (BSDMF) for Internet of Medical Things (IoMT) based health information analysis systems. IoMT contains a huge amount of data that contains various information and values for further detection and diagnosis processes. Blockchain secures the datasets, which enhances the accuracy of decision-making processes. Experimental results show that the proposed BSDMF increases the security and privacy range in data security processes.

Tan et al. [27] designed a secure privacy-preserving sharing scheme for personal health records. Multi-party pre-authorization verification is implemented in health-care centers to secure the authentication process's accuracy. The proposed scheme is a cypher encryption sharing approach that detects the threats in data sharing. Both challenges and threats are identified based on the priorities and conditions of patients. The proposed scheme increases the security and privacy protection range in health-care centers.

Zaabar et al. [28] developed a blockchain-based health-care data management system. The main aim of the proposed method is to detect the decentralized files which are presented in electronic health records. Cyber-attack threats are also identified by blockchain, increasing the centers' security ratio. The proposed method reduces both the time and energy consumption ratio in identification processes. When compared with other methods, the proposed method achieves high performance and effectiveness in health-care centers.

Masud et al. [29] introduced a robust and lightweight secure access control scheme for cloud-based electronic health-care data (EHR). The proposal addresses the potential cyberthreats that occur during data sharing and decision-making processes. A key derivation function (KDF) is used here to protect patient data from third-party members. The introduced scheme provided the energy-efficiency level for the systems. The introduced scheme increases the overall privacy and security range of EHR data.

Kiourtis et al. [30] proposed a secure device-to-device (D2D) protocol that may be utilized by software applications on top of Bluetooth technologies to facilitate the transmission of health data between individuals and health-care providers. Although several European Union (EU) nations are creating virtual or centralized national repositories of individuals' health information using electronic health records (EHRs), EU citizens have relatively little say over their health data. Via HIE, medical records for patients may be updated and corrected much more quickly. The D2D protocol facilitates a secure data exchange procedure with few user inputs and rapid response times. It allows people to take charge of their health-care data and get consultation data directly, without a middleman.

Chen et al. [31] proposed a method for sharing and integrating EHRs in health-care clouds and examine the resulting privacy and security concerns. One common health IT architecture that helps with EHR exchange and integration is the cloud computing model. The approach addresses a major shortcoming of the present EHR setup. All information related to the patient is encrypted. In most cases, a hospital or clinic requesting access to patient data will first provide advance notice to the data owner. A third-party auditor may check the accessibility in case of an emergency.

3. Methods

3.1. Endorsed Joint Security Scheme

The EJS scheme is designed to improve the wireless security for the EHR database and is administered for all IoT applications and end users connected based on discrete and continuous data observations. The input EHR database is observed from the users through the surveillance process. The end users' processes on IoT are monitored and observed at any time interval for managing security. Processes such as data access, storage and amendments are performed sequentially with mutual authentication. This endorsed joint security scheme aims to identify the EHR utilization and variations in different processes to prevent adversarial interruption. The challenging task in this article is access control and storage modification based on the EHR database processing sequence and amendment process recognized with previously stored data. The EHR database sequences are stored as

records from observing previous user health condition data in the IoT platform. This EJSS is portrayed in Figure 1.

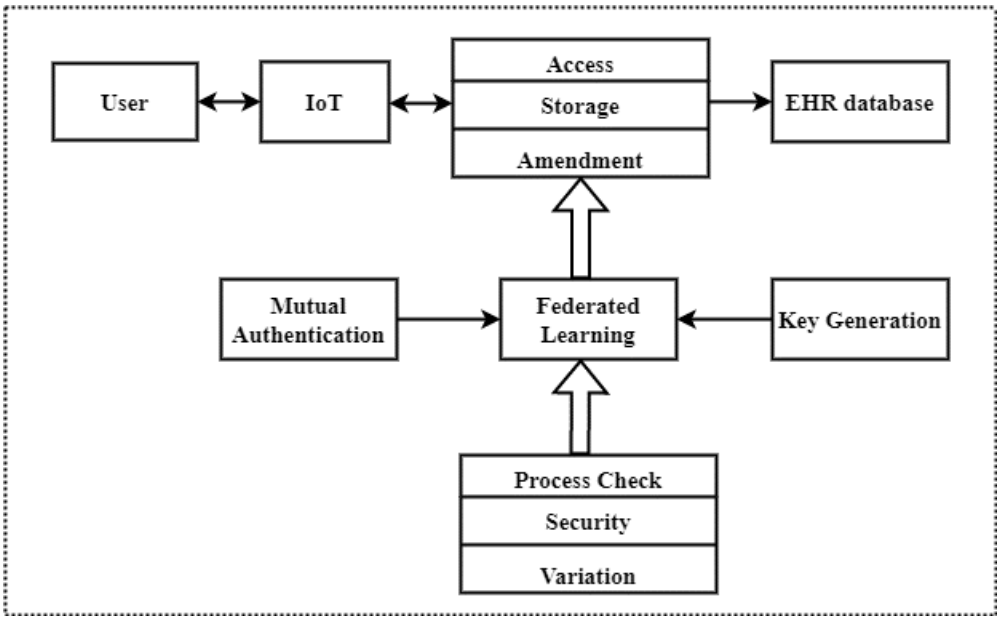

Figure 1. EJSS illustration.

The EHR database contains a large quantity of end user information that can be monitored and observed through wireless wearable sensors placed over the body surface or wrist of the application users. After the EHR observations, security is provided for three processes, namely, data accessing, storage, and amendment are jointly managed. In continuous EHR database accessing, the required health condition data of a particular user is to be analyzed with the previously stored data for any variations and secure user information. Similarly, a large amount of EHR database can be stored for performing operations in the storage process. Instead, an amendment process detects variations occurring in stored data, if any variations are identified, then the amendment is performed to modify already stored health-care data of a user with a current condition. Access control and storage modification improve surveillance security and recognize the variations by causing interruptions. The interruption occurrence is observed as a sequence of irrelevant data accessing and third-party users modifying the health-care data particular user without the knowledge of that user. The proposed endorsed joint security considers such variations in different processes, with users generating mutual keys to protect their health-care data using a federated learning paradigm. An initial joint security scheme using EHR database processing $EHR_D(P)$ means the user's health-care data sequence is observed and monitored in a given interval. The security for the different processes is estimated as

$$\left.\begin{array}{c} \exists(P) = EHR_D(P) - V * m(P) \\ such\ that \\ arg\min\limits_{T} \sum V(P) \forall EHR_D(P) + m(P) \end{array}\right\}. \quad (1)$$

where the variable V denotes the variations in that processes with sustainable security for access control $\exists(P)$ and monitoring process $m(P)$ depending on how the accumulated health-care database is processed with already stored data in different time intervals. The objective of variation minimization on the security processing for all $EHR_D(P) \in \exists(P)$ is defined as augmenting the security of user information. The end user performance in IoT is divided into three processes—data access (D_α), storage (S_β) and amendment (A_γ)—based on the current health condition of a user. The constraint $P = D_\alpha + S_\beta + A_\gamma$ is processed cumulatively using a common paradigm such that EHR utilization is recognized

between D_α instances and so on. If ε used to denote the number of processes and their security measures, therefore, $D_\alpha = (\varepsilon \times T) - A_\gamma$ is the data accessing instance that is to be performed with mutual authentication to secure the data for future use. Let $\varphi(D_\alpha)$, $\varphi(S_\beta)$ and $\varphi(A_\gamma)$ represent the security for $EHR_D(P)$ identified in different T intervals and V is detected in all amendment processes such that

$$\varphi(D_\alpha) = \varepsilon(D_\alpha) : EHR_D(P) \; \forall \; d^e = 0 \tag{2}$$

$$\varphi(S_\beta) = S_\beta(\varepsilon(D_\alpha)) : EHR_D(P) \; \forall \; d^e \neq 0 \tag{3}$$

$$\varphi(A_\gamma) = \frac{\varepsilon(D_\alpha)}{d^e} A_\gamma : EHR_D(P) \; \forall \; d^e \neq 1 \tag{4}$$

Based on Equations (2)–(4), the electronic health-care record utilization is recognized using the condition $\varepsilon(D_\alpha)$ and $\frac{\varepsilon(D_\alpha)}{d^e} A_\gamma$ for the sequences that require access control and storage modification is identified. Based on the processes, the data processes and security measures as in the above equations, Equation (1) is rewritten as shown in Equation (5)

$$\exists(P) = \begin{cases} \left(\varphi(D_\alpha) + \varphi\left(S_\beta\right)\right) = \varepsilon(D_\alpha) + S_\beta(\varepsilon(D_\alpha)) : EHR_D(P), \; \forall \; V = 0 \\ \left(\left(\varphi(D_\alpha) + \varphi\left(S_\beta\right)\right) - \varphi(A_\gamma)\right) = \varepsilon(D_\alpha) + S_\beta(\varepsilon(D_\alpha)) - \frac{\varepsilon(D_\alpha)}{V} A_\gamma : EHR_D(P), \; \forall \; V \neq 0 \end{cases} \tag{5}$$

As per the above expanded EHR database processes, the consequence of $D_\alpha \in P$ is to be previously performed processes for identifying the first end user data access and storage modification as in Equation (6). This is evaluated to identify variations in the processes based on EHR utilization for mutual key sharing between the data-accessing user and EHR database using federated learning. The security implementation for different V detection is illustrated in Figure 2.

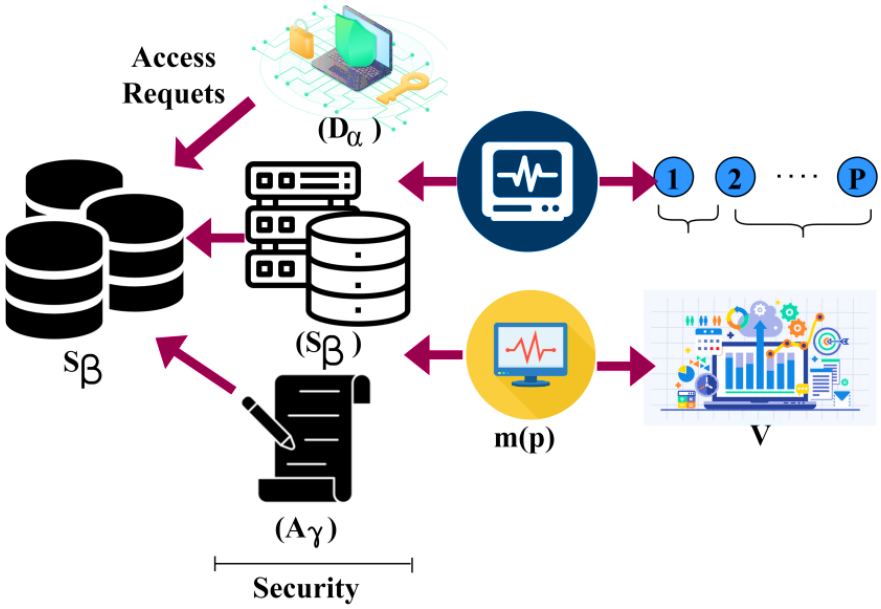

Figure 2. V Detection.

The S_β is accessed through P for identifying V across different $\exists(P)$. This $\exists(P)$ is required for securing access for identifying $\varphi(D_\alpha)$ and $\varphi(S_\beta)$ concurrently. The process is required for identifying V between successes $P \; \forall \; A_\gamma$. If A_γ is true, then P is modified for confining V; the security modifications prevent adversaries (Figure 2). The access control and storage modification is performed by the user with security using an EHR database in

an IoT platform through a common paradigm. For each process, the sequence of $\varepsilon \in D_\alpha$ is defined as

$$\varepsilon(D_\alpha) = \left(1 - \frac{A_\gamma}{\varepsilon}\right) T_{d-1} + \frac{D_\alpha}{\varepsilon} \sum_{i=1}^{T} \frac{\left(1 - \frac{D_\alpha}{A_\gamma}\right)^{\varepsilon-1} . T_{d-1}}{V * T} \tag{6}$$

Equation (6) computes the consequence of previous data analysis T_{d-1} for identifying variations for access control and storage modifications using the output. The previous data analysis and its privacy measures are used to modify the security to improve decision-making and the continuous surveillance process. Therefore, based on the access control and storage modification sequence, $\exists(P) = \left(\left(\left(\varphi(D_\alpha) + \varphi\left(S_\beta\right)\right) - \varphi(A_\gamma)\right) * (1 - \varepsilon(D_\alpha))\right)$ is the final process output for $V \neq 0$ conditions. The mutual key sharing between accessing users (X_{D_α}) and EHR database $\left(Y_{S_\beta}\right)$ for individuals and groups require relative security at the first level is given by Equation (7) as

$$X_{D_\alpha} = \sum_{i=1}^{\varepsilon} \left(\frac{\varphi(A_\gamma) \cdot T}{\sum_{P \in T} [\varepsilon(D_\alpha) + EHR_D(P)]_i} \right) \tag{7}$$

$$Y_{S_\beta} = \sum_{P=1} \left(\frac{T\left(\varphi(D_\alpha) + \varphi\left(S_\beta\right)\right)}{\sum_{P \in T} \left(\varepsilon(D_\alpha)\right)_i \left\{ \left[1 - \varepsilon(A_\gamma)_i\right] \times \varphi\left(S_\beta\right) \right\}_i} \right) \tag{8}$$

Equations (7) and (8) follow the relative security required for an electronic health-care database for access control and storage modifications at the time of data accessing and storage allocation for the user information in T interval that can be processed using the previous data observation. In this initial security scheme process, the identification of the first user key changes based on X_{D_α}, Y_{S_β}, $\varphi(D_\alpha)$ and $\varphi\left(S_\beta\right)$ are the serving inputs for the federated learning paradigm. The mutual key-sharing process is illustrated in Figure 3.

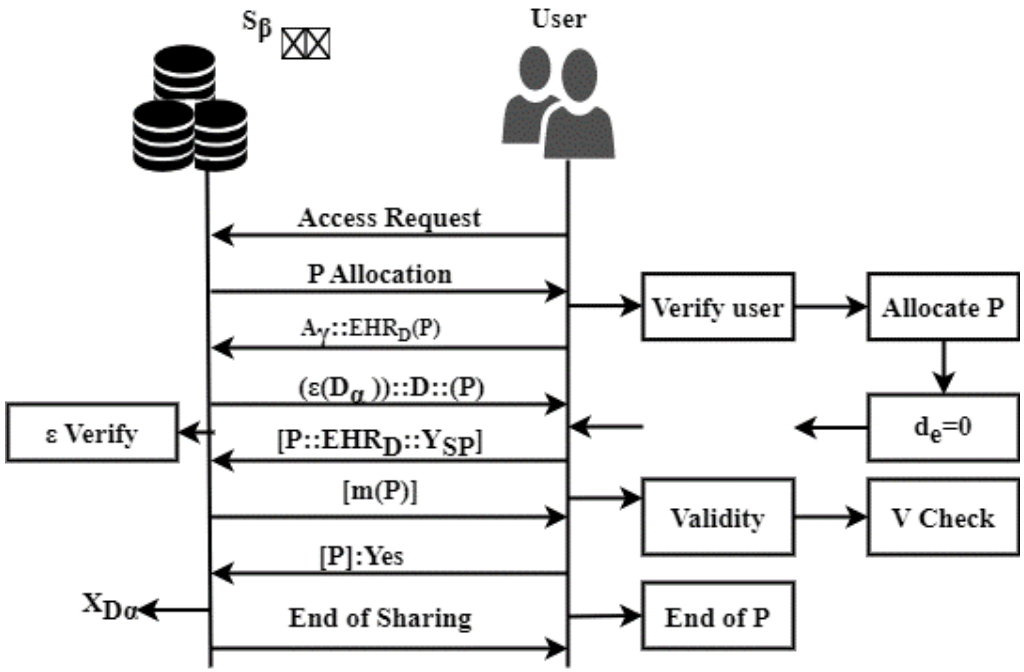

Figure 3. Mutual key sharing.

The mutual authentication is provided for P such that $[A_\gamma :: EHR_D]$ is mapped $\forall$ 1 to P. The initial verification is the $V = 0$ or $V \neq 0$ case, wherein the $d^e = 0$. If a variation (V) between any consecutive P is observed, then $\varepsilon(D_\alpha)$ is analyzed. Considering this case, the end of P is awaited, and therefore the interval validity $\forall \times D_\alpha$ is verified. The other case of ε verification and $\varphi(A_\gamma)$ is preceded to prevent any other adversary (Figure 3).

The consecutive security processing and different privacy measures help identify the interruptions in data access and storage. This federated learning process is discussed in the following section.

3.2. Federated Learning for Joint Security Verification

In the variation identification process, federated learning is used for identifying the adversarial interruptions in X_{D_α}, Y_{S_β} and recognizing V in different processes. As this learning paradigm relies on already stored information, the precise recommendation is achievable through access control. The number of processes may vary for variations or modifications in the stored database helps to provide security based on end user information through surveillance process and $\varepsilon(D_\alpha)$ are analyzed for all at T intervals. In particular, this federated learning performs three processes: process check, security, and variation. In the different processes check, D_α and S_β are monitored and analyzed to improve the security of electronic health-care databases. In the security process, the user can generate a key for their information based on the aforementioned processes. Instead, in the variation analysis, different health-care database analysis and storage allocation processes are performed to improve access control along with better computation and recognition of EHR utilization with mutual authentication. The inputs for federated learning are $A(t)$ and T. The computation of $EHR_D(P) \in T$ performed under access control and storage modification relies on the occurrence of variations.

In the learning paradigm, $EHR_D(P)$ and the time interval is computed independently through a process check. The process checking is performed for all end users with mutual authentication and used to modify the initial EHR database information. The process check output sequence is represented as $(\varnothing_1 \; to \; \varnothing_T)$ and is approximated using Equation (9) as

$$\begin{array}{c|c} \varnothing_1 = D_{\alpha_1} & \vartheta_1 = D_\alpha \\ \varnothing_2 = 2D_{\alpha_2} - 2\left(S_\beta\right)_2 - \varphi(A_\gamma)_1 & \vartheta_2 = 2(D_\alpha) + \varphi(A_\gamma)_1 \\ \varnothing_3 = 3D_{\alpha_3} - 3\left(S_\beta\right)_3 - \varphi(A_\gamma)_3 & \vartheta_3 = 3(D_\alpha) + \varphi\left(S_\beta\right)_1 - \varphi(A_\gamma)_2 \\ \vdots & \vdots \\ \underbrace{\varnothing_T = \varepsilon(D_\alpha)_T - \varepsilon\left(S_\beta\right)_T - \varphi(A_\gamma)_{T-1}}_{Accessing\ User\ process\ output} & \underbrace{\vartheta_T = \varepsilon(D_\alpha)_T + \varphi\left(S_\beta\right)_{T-1} - \varphi(A_\gamma)_{T-2}}_{EHR\ Database\ Variation\ sequence} \end{array} \quad (9)$$

Figure 4a shows the model of the federated learning process for security reasons. Federated learning prevents users from submitting their personal training data to a central server, contributing to the training (tensor flow federated model) of a global model. The process checking of an electronic health-care database analyzes two outputs, namely, access control and storage modifications from $\varnothing_1$ to $\varnothing_T$ sequences, and identified variation/modification instances ϑ_1 to ϑ_T. Now, the security is processed using the common paradigm based on the variation occurring in the different processes. The condition $T \in \varnothing$ must not equal $T \in \vartheta$ as the process checking constraint. If there are interruptions in the first data accessing instance, then variation is performed using the amendment process. For each process, the end user performance is analyzed as per the EHR utilization of interruption occurrence and identified, and then $\varepsilon(D_\alpha)_T + \varphi\left(S_\beta\right)_{T-1} - \varphi(A_\gamma)_{T-2}$ is performed for modifying the discrete user information. In the security process, the first user data are secured through $(\varnothing_T, D_\alpha)$ from which (ϑ_T, A_γ) is processed using the learning paradigm. In this process check, the comparison of access control and storage modification is computed to verify the security independently. The first verification for variation sequence analysis for access is analyzed in Figure 4b.

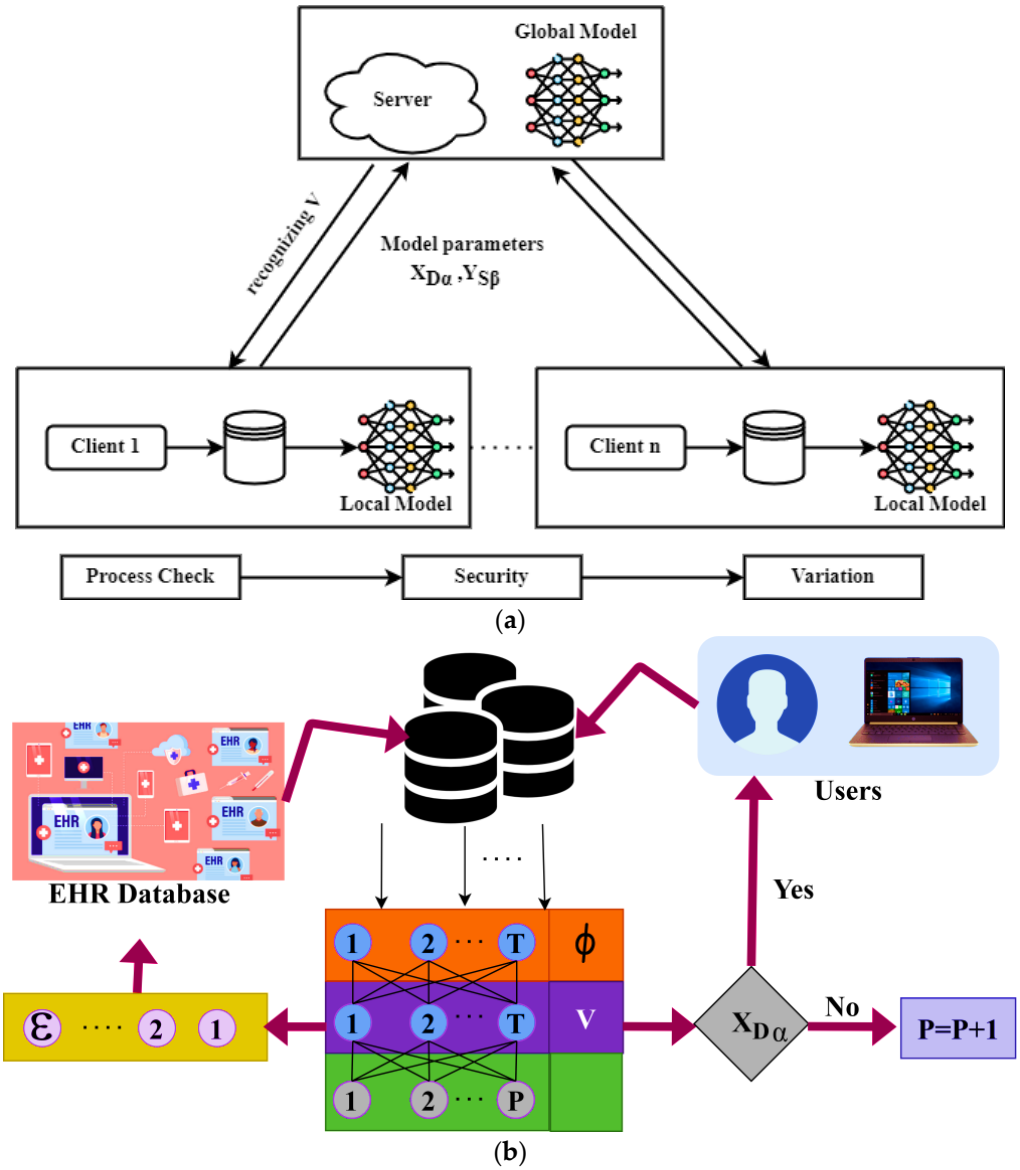

Figure 4. (**a**) Federated learning process. (**b**) Variation sequence for access.

The leaving for D_α is verified for $\varepsilon \in P$ such that ϕ synchronizes with T. For the synchronized T, the ε is preventive by verifying if X_{D_α} is true or false. If the verification is true, then the user is provided with P, so change in $\exists(P)$ is ensured. Therefore, the Y_{S_β} is revoked in the particular P and hence v is identified. The identification is performed for current P other than ϕ_1 to ϕ_T. Therefore, the learning segregates ϕ and v independently, preventing new interrupts for the varying access and storage (refer to Figure 4). The variation in the already stored data is performed at its first level from which the security processes are verified using mutual key sharing. After process checking, the remote accessing of the discrete user information in IoT-based application technology is administered with sustainable security based on $\varphi(A_\gamma)$ occurring instances. Here, the concurrent adversaries identified in the various processes initiated at the same time are computed using $\varphi(A_\gamma)$ and A_γ and the variation in the EHR database is used for differentiating adversaries under each process. First, the key generation of the IoT user is designed using federated learning. In this mutual key generation, the variable Q and R privacy and public key for the user information and $EHR_D(P)$ are generated. A_γ and $EHR_D(P)$ are computed for the first user at a similar time to reduce interruptions. If the condition $X_{D_\alpha} < Y_{S_\beta}$ is achieved, then the data access and storage process does not contain any variations. Instead, if $X_{D_\alpha} > Y_{S_\beta}$ is

achieved, then the different process identifies concurrent adversaries in the EHR database; therefore, the new sequence of D_α and storage is processed using a mutual key. Based on the aforementioned processes, the condition $X_{D_\alpha} > Y_{S_\beta}$ results in "1" whereas $X_{D_\alpha} < Y_{S_\beta}$ results in "0" for continuous electronic health-care database access and monitoring. Now, the surveillance processes with required related security are to be verified by the federated learning process and variation also identifies from the EHR database.

The common paradigm using data access computation is performed and variation occurs the proposed EJS scheme identifies instances. In this end user performance analysis, first, the amendment identified user is used for sharing mutual key for preventing adversarial interruptions. In the process, mutual authentication for data access is the considering factor for process checking for identifying the individual extracted attributes under each process. In the EHR database, information modified using the individual amendment is recognized for differentiating adversaries to verify if any problem occurred in the application. If A_γ occurs, then $\varphi(A_\gamma)$ is computed as per the above equation. Therefore, the amendment sequence is modified with the current data. Here, the process check, security and variation are different for each process, as expressed using (10) and (11), respectively.

$$\left.\begin{array}{c} \varnothing_1 = D_{\alpha 1} \\ \varnothing_2 = 2D_{\alpha 2} + \varphi(S_\beta)_1 + V_1 \\ \varnothing_3 = 3D_{\alpha 3} + \varphi(S_\beta)_2 + V_2 \\ \vdots \\ \varnothing_T = T(D_{\alpha T}) + \varphi(S_\beta)_{T-1} + V_{T-1} \end{array}\right\}, \textit{ for access control based sequence} \tag{10}$$

$$\left.\begin{array}{c} \varnothing_1 = 0 \\ \varnothing_2 = \varphi(A_\gamma)_1 + 2S_\beta - V_1 \\ \varnothing_3 = \varphi(A_\gamma)_2 + 3S_\beta - V_2 \\ \vdots \\ \varnothing_T = \varphi(A_\gamma)_{T-1} + T(S_\beta) - V_T \end{array}\right\}, \textit{ for storage modification based sequence} \tag{11}$$

The above equation represents the occurrence of amendments in the EHR database at different time intervals and the adversarial interruption occurrence leads to access control and storage modification. In this data accessing and storage, modification achieves $\varnothing_1 = 0$ for the previous output. In this time, any amendment takes place such that the mutual authentication strengthens individual attributes, where the variation in D_α is 0. Hence the security changes are not processed in the individual surveillance process. For each process check, the variation is identified before the EHR database storage is updated, as in Equation (12)

$$\left.\begin{array}{c} \vartheta_1 = \frac{1(D_{\alpha 1}) + T_{d-1}}{V_1} \\ \vartheta_2 = \frac{2(D_{\alpha 2}) + T_{d-2}}{V_2} - \varphi(A_\gamma)_1 \\ \vartheta_3 = \frac{3(D_{\alpha 3}) + T_{d-3}}{V_3} - \varphi(A_\gamma)_2 \\ \vdots \\ \vartheta_T = \frac{\varepsilon(D_{\alpha T}) + T_{d-T}}{V_T} - \varphi(A_\gamma)_{T-1} \end{array}\right\} \tag{12}$$

The EHR database modification is performed at the end of all data access and storage expansion processes. The modification for security (access and storage) decisions is performed as a process illustrated in Figure 5.

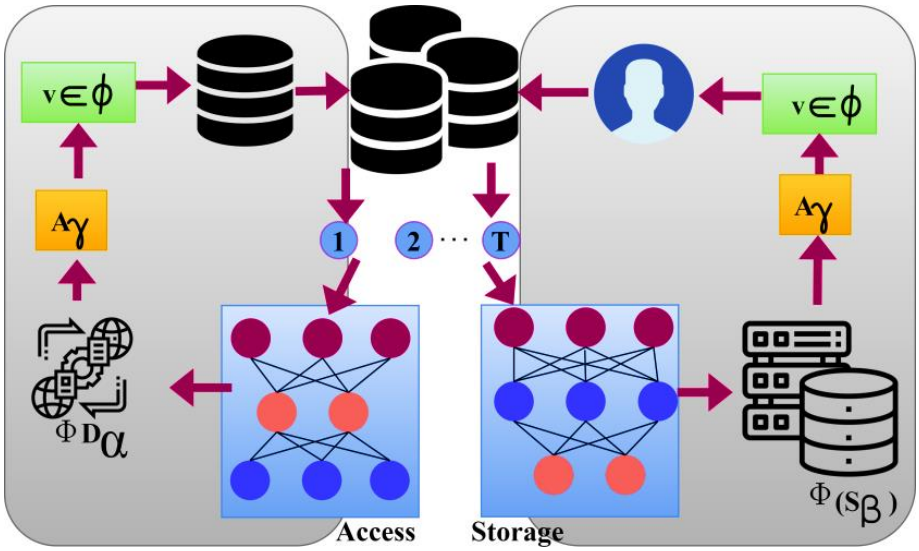

Figure 5. Modification Illustration through learning.

The variations in P are verified through $\varepsilon(D_\alpha)$ and $\varepsilon(S_\beta)\forall v \in \varphi$ in both classifications. Considering the Y_{SB} validity and X_{D_α} $\forall$ P, the above verification is jointly performed. Depending on the available (current) $\varphi(D_\alpha)$ and $\varphi(S_\beta)\forall$ resources, the assessment for A_γ is performed. If either condition fails, then the V between two P's is identified using federated learning conditions on X_{D_α} and $m(P)$. Therefore, a new A_γ is presented for maximizing secure storage access of the next $P+1$ (Figure 5). In the EHR, a database update is performed along with data access and storage is also updated. Now, the individual attributes of all end users are monitored and analyzed based on data access, and storage modification with mutual key is processed at the same time for improving surveillance efficiency.

4. Results and Analysis

4.1. Self-Analysis

The proposed scheme is verified using the dataset the synthea dataset Jsons SyntheaTM, open-source and free software for creating synthetic patients and simulating their medical records [32]. The goal is to provide comprehensive synthetic patient data and health records that are very life-like but not real. The activity overview of this dataset is shown in Figure 6. These data provide ECG observation of 45,152 patients with 12 fields and 12,000+ entries. The information is presented as a CSV file that provides both patient and observation data in various sessions. Access to selective resources is provided through queries from a dedicated user interface. The sharing server generates a 128-bit mutual key in the query processing. First, the storage is a single split 50 GB space that is distinguished after access denial. First, the D_α acceptance and failure for the varying P is analyzed with the A_γ is presented in Figure 7.

The declined D_α is identified between two successive P and therefore the $\varepsilon(D_\alpha)$ is modified to prevent new access. In the consecutive access control, the validations for improving authentication and EHR access are pursued by verifying P for preventing adversaries. Therefore, the A_γ is guided from S_β access and non-distinguishing $\phi_T \forall \varphi(D_\alpha)$. This is alone considered for introducing A_γ in the next P for maintaining a low neglection of D_α. Therefore, the A_γ varies with the requests and its sessions for preventing adversary impacts (Figure 7). In the consecutive analysis of D_α the access to both storages is split (i.e.,) the A_γ impacts $\varphi(S_\beta)$ for reducing the authentication lag. For this purpose, the single storage is split for different EHR access (concurrent) and thus preventing adversaries. Now, the V in D_α and S_β are concurrently handled after the new P. This analysis is presented in Figure 8.

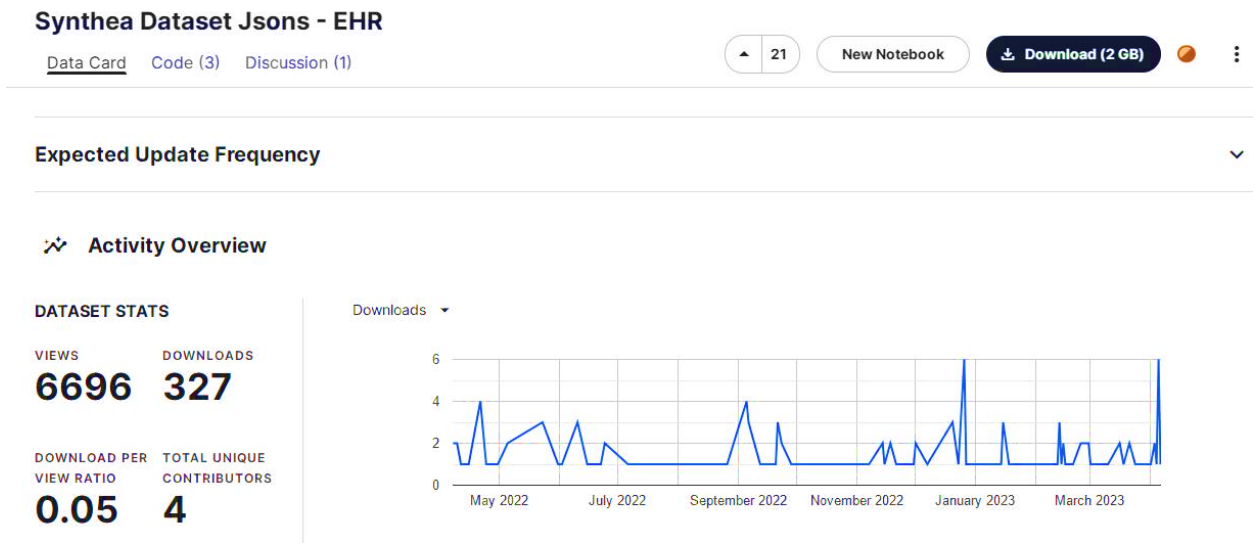

Figure 6. Activity overview of Synthea Dataset Jsons.

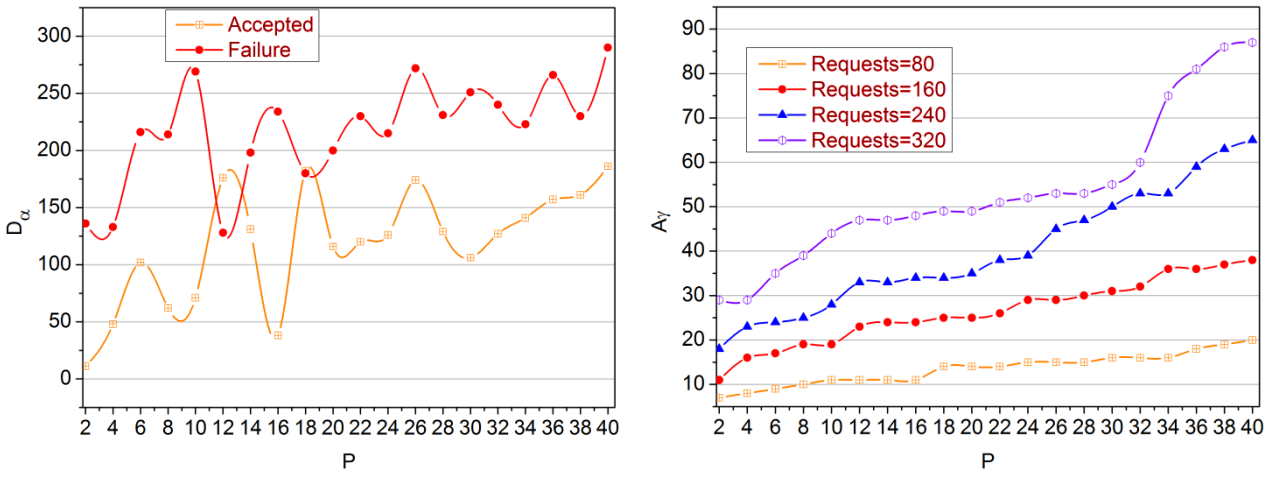

Figure 7. D_α and A_γ analysis.

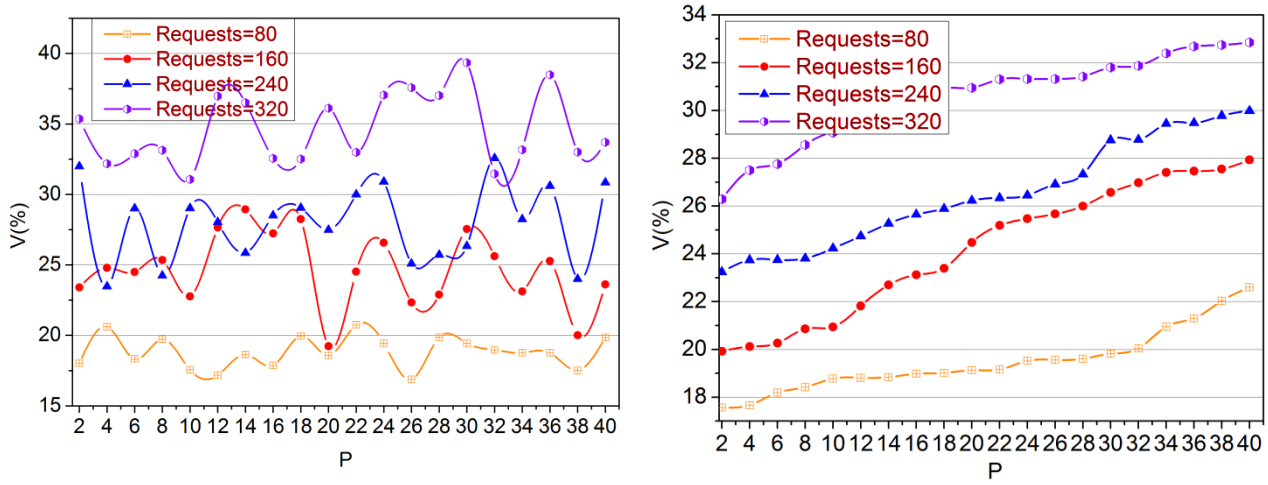

Figure 8. D_α and S_β -based V analysis.

The access and storage level security rely on the actual requests between to P. Considering the concurrency in variations (both), the next allocation is performed. The learning segregates ϕ and v for $\varphi(S_\beta)$ and $\varphi(D_\alpha)$ using A_γ. Therefore, the amendments are precise for the varying access time and $\varepsilon(D_\alpha)$. The learning decision over (XD_α) using Y_{S_β} determines the access and verification time. Therefore, the V detection is eased if the above conditions are unsatisfied and a new P with new Y_{S_β} is instigated. As the re-instigation occurs, the authentication lag for P occurs and its analysis for the varying $EHRs$ is presented in Figure 9.

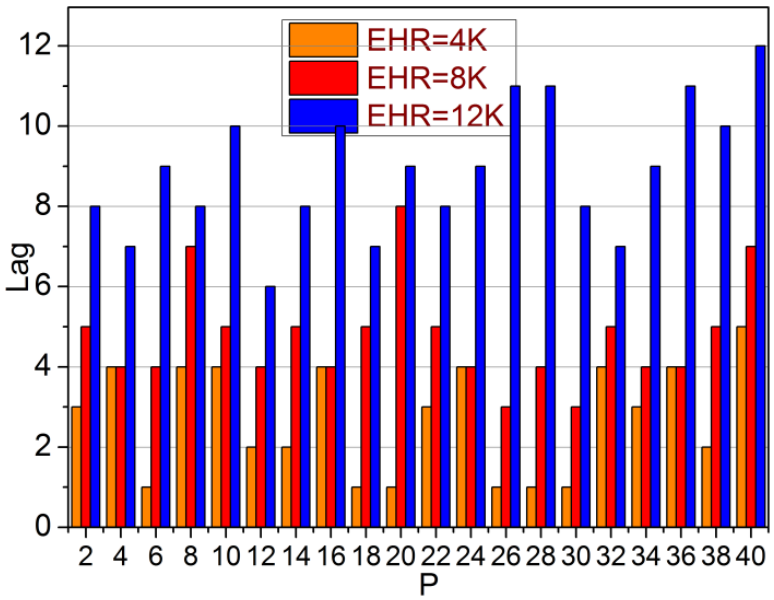

Figure 9. Lag analyses.

The lag for the controlled EHR is less, whereas the increasing $D \in EHR$ requires more P. As P becomes concurrent, the authentication sequence requirements are high. Therefore, XD_α and Y_{S_β} are congruently required for preventing interruptions and failures. If this is secured, the need for new authentication is less mandatory, preventing adversaries. Therefore, the suppression (lag) is performed before the access requests are validated through the learning process (Figure 9).

4.2. Comparative Analysis

Comparative analysis is performed using the metrics interrupt detection, authentication time, access time, access failures, and authentication lags. The EHR is varied between 1 K and 12 K and the requests are varied between 20 and 320. The methods FEACS [22], RS-HABE [19], and BSDMF [26] are considered along the proposed scheme in this comparative analysis.

4.3. Interrupt Detection

In Figure 10, the user health-care data access and storage modification with mutual keys in IoT-based application technology increases the e-health-care users through the surveillance process for the aforementioned services. Federated learning does not authenticate the health-care data for each process, and the individual user can generate a key for their information in time intervals. The storage allocation and user authentication analysis are modified based on the end user's performance using mutual key sharing for the single-user application for security, preventing adversarial interruptions. The variations in different processes are addressed using a surveillance system to satisfy this condition $EHR_D(P) \in \exists(P)$ and $D_\alpha = (\varepsilon \times T) - A_\gamma$ for the successive user, process check for access control, preventing authentication time and access failures. Therefore, the health-care data access and amend-

ment analysis are identified for precise process checks and user verification. Therefore, the individual user data accessing process relies on storage modification, preventing high interrupt detection due to modifications in key generation in IoT applications.

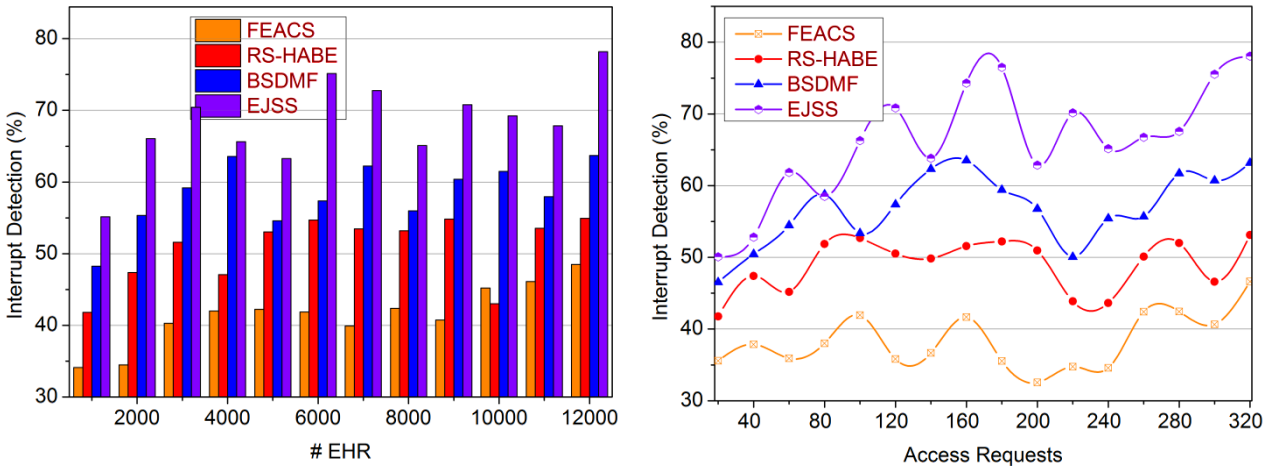

Figure 10. Interrupt detection comparisons.

4.4. Authentication Time

The remote access of end user performance shared between the accessing users and the EHR database in IoT-based applications using mutually shared keys for securing user-sensitive information for reducing failures and lags are illustrated in Figure 11. This proposed scheme for robust data security satisfies less authentication time and the federated learning identifies high data access. Based on the data access, the individual user's storage and service allocation is monitored and the sequence is analyzed at different time intervals for access control and storage modification. In this remote data accessing process using an EHR database processing instance, the input medical data of the user are monitored and analyzed in the three processes $\varphi(D_\alpha)$, $\varphi(S_\beta)$ and $\varphi(A_\gamma)$ with security. The consecutive process is based on health condition data access, storage, and amendments based on the current instance. The mutual key is provided for health-care data processing with high security due to third-party users being able to modify the details of EHR computed using Equations (5)–(8). In this proposed scheme, the user process and data process are monitored continuously based on shared keys for further service access. Therefore, the authentication time is less compared to the other factors in IoT application technology for secured medical data. The authentication time is less for different processes based on the user data access.

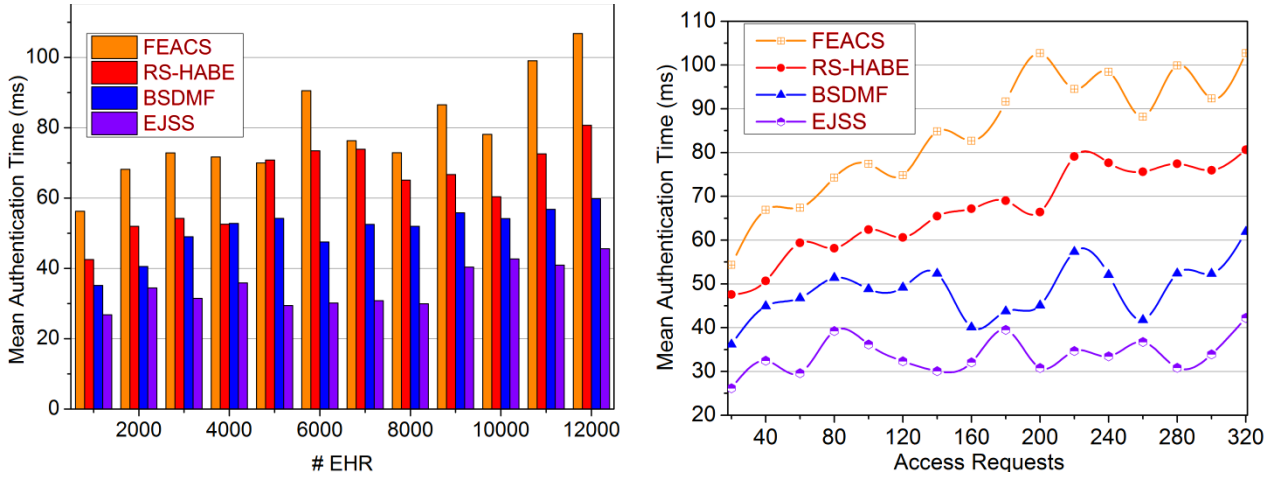

Figure 11. Authentication time comparisons.

4.5. Access Time

In Figure 12, the access control and storage modification of the electronic health-care record system performs different processes for sustainable security in IoT applications using mutual keys for remote data access and identifies variations as it does not allocate storage. The sequential monitoring of users and their medical data is analyzed to identify adversarial interruptions at different intervals. The user verification and variation analysis rely on wireless security and is analyzed using a common paradigm for information security to prevent access failures in the sequence for process checks of the EHR database. This access failure and variations are addressed using the mutual key in IoT application identified from the already stored data, preventing failures. The three processes in federated learning are sequentially performed without any interruptions for data access and storage modification with user-generated keys in different time intervals for medical data security. Therefore, the secured EHR database for future data access and different processes for which the proposed scheme satisfies less access time.

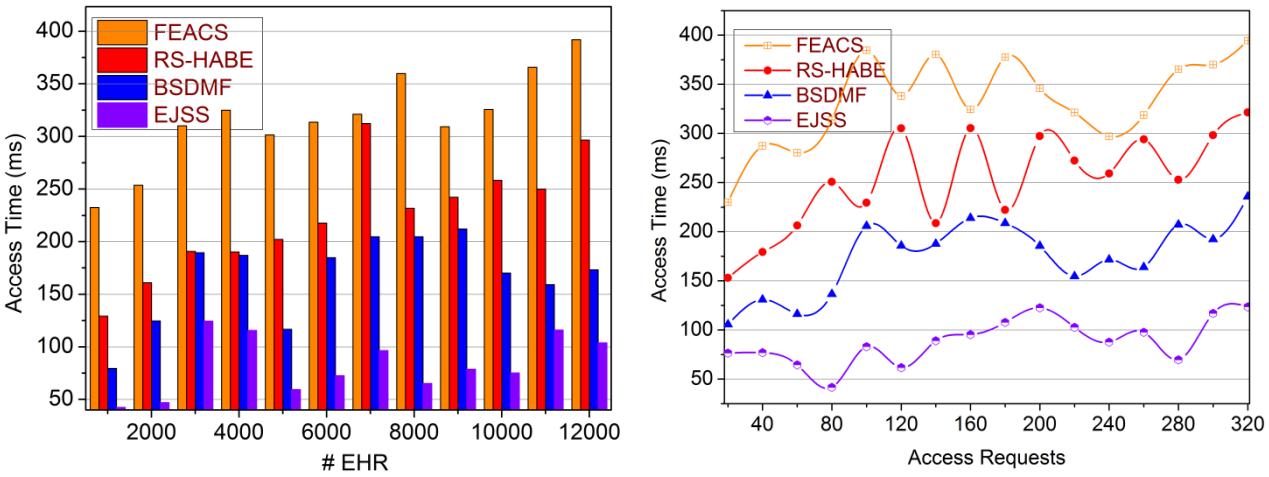

Figure 12. Access time comparisons.

4.6. Access Failures

The wireless security-administered application technology-like IoT platform-assisted e-health-care data access and storage management for information security and user process verification for preventing theft occurrence is represented in Figure 13. In this proposed joint security scheme, the storage changes and access control require relative security using a shared mutual key satisfies fewer access failures, and time is identified using federated learning. The individual attributes analyze the security strength and surveillance efficiency for differentiating the adversaries in different intervals through a learning paradigm. In this health-care record, monitoring for identified concurrent adversaries in the different processes with $EHR_D(P) \in T$ computed under access control and storage modification depends on the occurrence of variations. Based on the sequence, the medical data access and mutual authentication are strengthened, using individual attributes for the identification of adversarial interruptions in the EHR database processing with security. The authentication lag is identified in a different process based on the application technology process.

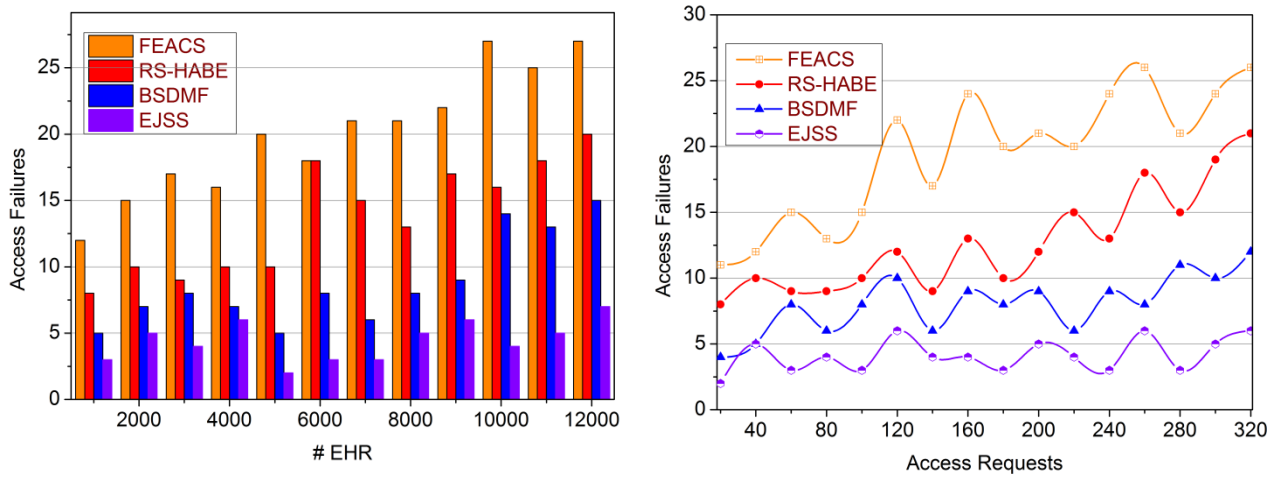

Figure 13. Access failures comparison.

4.7. Authentication Lag

In this proposed remote electronic health-care data access and monitoring using the mutual key in IoT application, the authentication time and inspection lag are identified at the time of processing service between the users and database. User process checking is computed for all end users with mutual authentication used to analyze any modification performed to initial EHR database information. The identified variation is updated in the EHR database for access control and storage modification to identify authentication lag during process check and user verification using learning. If any adversary interruptions or variations are identified in different processes, then the key changes based on the aforementioned process identify EHR utilization. The already stored data and user key are used to access particular user information in different time intervals using federated learning, preventing access failures and time. The data access and amendment process can be secured through mutual authentication and key generation for the medical data and the further process is performed without increasing the authentication lag. The proposed scheme generates a key for individual users to reduce failures and analyze security variation to achieve less authentication time, as presented in Figure 14. The comparative analysis summary is given in Tables 1 and 2 for the EHRs and access requests.

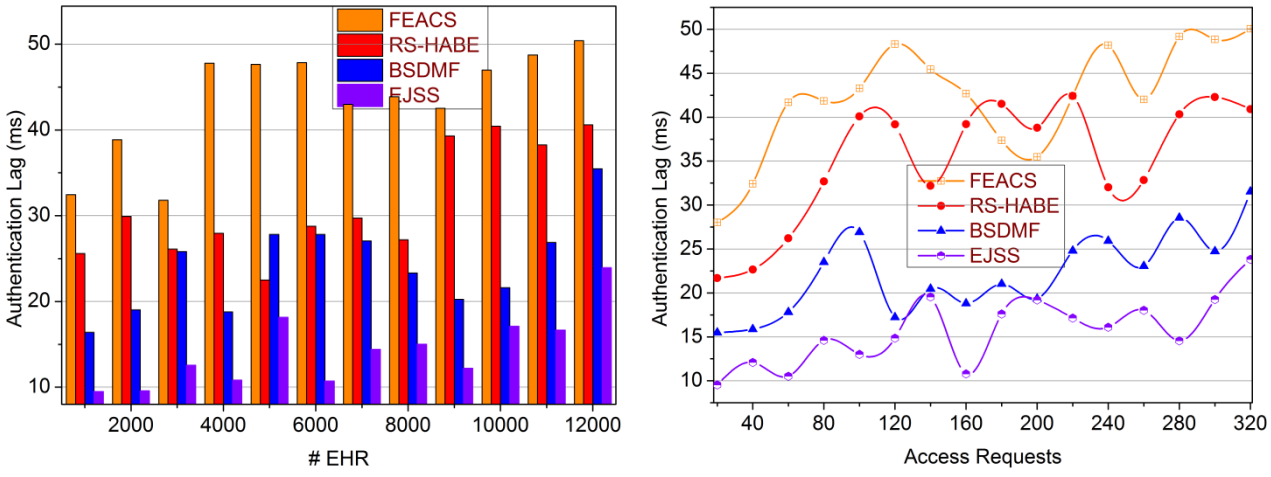

Figure 14. Authentication lag comparisons.

Table 1. Comparative analysis summary for # HER.

Metrics	FEACS	RS-HABE	BSDMF	EJSS
Interrupt Detection (%)	48.49	54.95	63.7	78.195
Mean Authentication Time (ms)	106.81	80.71	59.82	45.628
Access Time (ms)	392.01	296.55	173.17	103.82
Access Failures	27	20	15	7
Authentication Lag (ms)	50.41	40.59	35.48	23.935

Summary—The proposed scheme achieves 11.24% high interrupt detection, 7.44% less authentication time, 10.64% less access time, 11.02% less access failures, and 7.2% less authentication lag.

Table 2. Comparative analysis summary for access request.

Metrics	FEACS	RS-HABE	BSDMF	EJSS
Interrupt Detection (%)	46.63	53.12	63.17	78.061
Mean Authentication Time (ms)	102.73	80.67	61.92	42.243
Access Time (ms)	394.41	321.33	235.72	123.567
Access Failures	26	21	12	6
Authentication Lag (ms)	50.07	40.91	31.53	23.819

Summary—The proposed scheme achieves 11.88% high interrupt detection, 8.06% less authentication time, 7.34% less access time, 11.58% less access failures, and 6.9% less authentication lag.

4.8. Discussion

This article presents an endorsed joint security plan for strengthening the safety of surveillance in the aforementioned services. The proposed approach uses a federated learning decision-making mechanism to ensure that the access and storage procedures are sequential across various security measures. Jsons SyntheaTM is free and open-source software for producing synthetic patients and mimicking their medical records, and it is used to validate the proposed approach. There is a wide range of EHRs (1–12 K) and requests (20–320. The analysis considers the FEACS, RS-HABE, and BSDMF methods in addition to the proposed one. Health-care data access and amendment analysis are identified for precise process checks and user verification utilizing metrics interrupt detection, which allows for a comparison analysis to be done. As a result, IoT applications rely on storage modifications to avoid interrupt detection rates of up to 11.24 percent as a result of user-initiated changes to key generators. With federated learning identifying high data access and strong data security requiring just around 7.44% of the time for authentication, this setup is ideal. Certain operations have shorter authentication times depending on the context in which the user data are being accessed. The sequential monitoring of users and their medical data is examined to detect hostile disruptions at varying intervals, resulting in 10.66% less access time. Electronic health record systems carry out several procedures on access control and storage modification for long-term security in IoT applications. The IoT platform helps e-health-care data access and storage management for information security and user process verification to avoid theft in the case of access failures thanks to wireless security managed application technology. The authentication time and inspection lag are discovered at the time of processing service between the users and database in authentication delay electronic health-care data access and monitoring using the mutual key in IoT application. Mutual authentication and key generation for medical data may safeguard the data access and modification process without adding significant delay to the authentication procedure (by a margin of 7.2%).

5. Conclusions

In the article, the endorsed joint security scheme is described as an approach to improve the privacy of patients' stored electronic health records in health-care organizations. The proposed plan focuses on sensitive medical information about patients being stored and accessed securely. Utilizing wireless communication technology, doctors can keep an eye on patient information at all occasions. Access and storage processes in the proposed scheme are performed in order across different security measures based on decisions made by federated learning. The conditions analyzed by the learning paradigm, which can be accessed by the leaders of a health-care organization, are used to make decisions about how to tell when security changes between two consecutive sequences. Access-level security is handled with the help of a multikey authentication system that works until the acquired sequence. In the sequence-level administration, changes are looked for in the order of the series, so variation detection keeps access and storage functions from being interrupted by an adversary. The process is based on a free-flowing model where decisions about sharing keys and safe access to health records are made based on what is learned. The proposed scheme detects interrupts 11.24% more often, takes 7.44% less time to authenticate, takes 10.64% less time to access, has 11.02% fewer access failures, and takes 7.2% less time to authenticate. This plan makes security better, but the security method it uses takes a long time because it involves repeatedly starting the sequence. Lightweight authentication and integrity verification schemes are planned to be added to the future proposal to keep the same level of security. The blockchain paradigm will also be used in future work to make it easier to work on different things simultaneously.

Author Contributions: Conceptualization, Z.D.; methodology, Z.D.; software, F.S.; data curation, Z.D.; writing—original draft preparation, Z.D.; writing—review and editing, F.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jusak, J.; Mahmoud, S.S.; Laurens, R.; Alsulami, M.; Fang, Q. A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Testbed. *IEEE Access* **2021**, *10*, 1082–1095. [CrossRef]
2. Qu, Z.; Zhang, Z.; Zheng, M. A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things. *Inf. Sci.* **2022**, *612*, 942–958. [CrossRef]
3. Attarian, R.; Hashemi, S. An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. *Comput. Netw.* **2021**, *190*, 107976. [CrossRef]
4. Mahajan, H.B. Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap. *Wirel. Pers. Commun.* **2022**, *126*, 2425–2446. [CrossRef]
5. Chen, L.; Zhang, N.; Sun, H.-M.; Chang, C.-C.; Yu, S.; Choo, K.-K.R. Secure search for encrypted personal health records from big data NoSQL databases in cloud. *Computing* **2020**, *102*, 1521–1545. [CrossRef]
6. Li, Q.; Zhang, Y.; Zhang, T.; Huang, H.; He, Y.; Xiong, J. HTAC: Fine-Grained Policy-Hiding and Traceable Access Control in mHealth. *IEEE Access* **2020**, *8*, 123430–123439. [CrossRef]
7. De Oliveira, M.T.; Reis, L.H.A.; Verginadis, Y.; Mattos, D.M.F.; Olabarriaga, S.D. SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts. *IEEE Access* **2022**, *10*, 117836–117854. [CrossRef]
8. Xiang, X.; Cao, J.; Fan, W. Decentralized authentication and access control protocol for blockchain-based e-health systems. *J. Netw. Comput. Appl.* **2022**, *207*, 103512. [CrossRef]
9. Huang, Y.-T.; Chiang, D.-L.; Chen, T.-S.; Wang, S.-D.; Lai, F.-P.; Lin, Y.-D. Lagrange interpolation-driven access control mechanism: Towards secure and privacy-preserving fusion of personal health records. *Knowl.-Based Syst.* **2022**, *236*, 107679. [CrossRef]
10. Yuan, W.-X.; Yan, B.; Li, W.; Hao, L.-Y.; Yang, H.-M. Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control. *Multimed. Tools Appl.* **2022**, *82*, 16279–16300. [CrossRef] [PubMed]

11. Xue, Z.; Zhou, P.; Xu, Z.; Wang, X.; Xie, Y.; Ding, X.; Wen, S. A Resource-Constrained and Privacy-Preserving Edge-Computing-Enabled Clinical Decision System: A Federated Reinforcement Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 9122–9138. [CrossRef]
12. Ghayvat, H.; Sharma, M.; Gope, P.; Sharma, P.K. SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 5609–5618. [CrossRef]
13. Ibrahim, A.; Gebali, F. Compact modular multiplier design for strong security capabilities in resource-limited telehealth IoT devices. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 6847–6854. [CrossRef]
14. Usman, M.; Qamar, U. Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. *Procedia Comput. Sci.* **2020**, *174*, 321–327. [CrossRef]
15. Symvoulidis, C.; Kiourtis, A.; Mavrogiorgou, A.; Kyriazis, D. Healthcare Provision in the Cloud: An EHR Object Store-based Cloud Used for Emergency. *Healthinf* **2021**, *1*, 435–442. [CrossRef]
16. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [CrossRef]
17. Madine, M.M.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Al-Hammadi, Y.; Ellahham, S.; Calyam, P. Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records. *IEEE Access* **2020**, *8*, 225777–225791. [CrossRef]
18. Wang, Y.; Zhang, A.; Zhang, P.; Qu, Y.; Yu, S. Security-Aware and Privacy-Preserving Personal Health Record Sharing Using Consortium Blockchain. *IEEE Internet Things J.* **2021**, *9*, 12014–12028. [CrossRef]
19. Wei, J.; Chen, X.; Huang, X.; Hu, X.; Susilo, W. RS-HABE: Revocable-storage and Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 2301–2315. [CrossRef]
20. Zhu, H.; Guo, Y.; Zhang, L. An improved convolution Merkle tree-based blockchain electronic medical record secure storage scheme. *J. Inf. Secur. Appl.* **2021**, *61*, 102952. [CrossRef]
21. Zaghloul, E.; Li, T.; Ren, J. d-EMR: Secure and distributed electronic medical record management. *High-Confid. Comput.* **2022**, *3*, 100101. [CrossRef]
22. Olakanmi, O.; Odeyemi, K. FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems. *Internet Things* **2020**, *12*, 100278. [CrossRef]
23. Shuaib, K.; Abdella, J.; Sallabi, F.; Serhani, M.A. Secure decentralized electronic health records sharing system based on blockchains. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5045–5058. [CrossRef]
24. Hurst, W.; Tekinerdogan, B.; Alskaif, T.; Boddy, A.; Shone, N. Securing electronic health records against insider-threats: A supervised machine learning approach. *Smart Health* **2022**, *26*, 100354. [CrossRef]
25. Chen, C.-L.; Huang, P.-T.; Deng, Y.-Y.; Chen, H.-C.; Wang, Y.-C. A secure electronic medical record authorization system for smart device application in cloud computing environments. *Hum.-Cent. Comput. Inf. Sci.* **2020**, *10*, 1–31. [CrossRef]
26. Abbas, A.; Alroobaea, R.; Krichen, M.; Rubaiee, S.; Vimal, S.; Almansour, F.M. Blockchain-assisted secured data man-agement framework for health information analysis based on Internet of Medical Things. *Pers. Ubiquitous Comput.* **2021**, 1–14.
27. Tan, K.-L.; Chi, C.-H.; Lam, K.-Y. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification. *Wirel. Netw.* **2022**, 1–23. [CrossRef]
28. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [CrossRef]
29. Masud, M.; Gaba, G.S.; Choudhary, K.; Alroobaea, R.; Hossain, M.S. A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3043–3057. [CrossRef]
30. Kiourtis, A.; Mavrogiorgou, A.; Menesidou, S.-A.; Gouvas, P.; Kyriazis, D. A Secure Protocol for Managing and Sharing Personal Healthcare Data. *Stud. Health Technol. Inform.* **2020**, *275*, 92–96. [CrossRef]
31. Chen, Y.-Y.; Lu, J.-C.; Jan, J.-K. A Secure EHR System Based on Hybrid Clouds. *J. Med. Syst.* **2012**, *36*, 3375–3384. [CrossRef] [PubMed]
32. Available online: https://www.kaggle.com/datasets/krsna540/synthea-dataset-jsons-ehr (accessed on 18 July 2022).