Psarra *et al.*
BMC Medical Informatics and Decision Making (2024) 24:303
https://doi.org/10.1186/s12911-024-02708-8

BMC Medical Informatics and Decision Making

RESEARCH

Open Access

Permissioned blockchain network for proactive access control to electronic health records

Evgenia Psarra[1*], Dimitris Apostolou[1], Yiannis Verginadis[2,3], Ioannis Patiniotakis[3] and Gregoris Mentzas[3]

Abstract

Background As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient's health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. The research objective of this work is to develop a proactive access control method that can grant emergency clinicians access to sensitive health data, guaranteeing the integrity and security of the data, and generating trust without the need for a trusted third party.

Methods A contextual and blockchain-based mechanism is proposed that allows access to sensitive EHRs by applying prognostic procedures where information based on context, is utilized to identify critical situations and grant access to medical data. Specifically, to enable proactivity, Long Short Term Memory (LSTM) Neural Networks (NNs) are applied that utilize patient's recent health history to prognose the next two-hour health metrics values. Fuzzy logic is used to evaluate the severity of the patient's health state. These techniques are incorporated in a private and permissioned Hyperledger-Fabric blockchain network, capable of securing patient's sensitive information in the blockchain network.

Results The developed access control method provides secure access for emergency clinicians to sensitive information and simultaneously safeguards the patient's well-being. Integrating this predictive mechanism within the blockchain network proved to be a robust tool to enhance the performance of the access control mechanism. Furthermore, the blockchain network of this work can record the history of who and when had access to a specific patient's sensitive EHRs, guaranteeing the integrity and security of the data, as well as recording the latency of this mechanism, where three different access control cases are evaluated. This access control mechanism is to be enforced in a real-life scenario in hospitals.

Conclusions The proposed mechanism informs proactively the emergency team of professional clinicians about patients' critical situations by combining fuzzy and predictive machine learning techniques incorporated in the private and permissioned blockchain network, and it exploits the distributed data of the blockchain architecture, guaranteeing the integrity and security of the data, and thus, enhancing the users' trust to the access control mechanism.

*Correspondence:
Evgenia Psarra
jennypsarraemp@mail.ntua.gr
Full list of author information is available at the end of the article

Keywords Private and permissioned blockchain, Hyperledger fabric blockchain technology, Smart contacts, Personalized policies, Decision making, Emergency services, Attribute-based access control policies, Medical prognosis, Electronic health records, Machine learning

Background

Introduction

Access control to healthcare data is vital as the protection of the patient's sensitive data privacy, e.g. the health history, is of great importance. Access control models are associated with the rights an entity has upon managing particular data objects. These are based on user identity access control models, such as Role-Based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [1]. Contrarily to these static approaches, the Attribute-Based Access Control (ABAC) paradigm has been introduced, which is dynamic in nature [2]. In ABAC, there are connections' snapshots that are produced and dynamically altered based on the current context, instead of statically-defined lists of permissions that link entities with objects.

As digital healthcare services handle increasingly more sensitive health data, robust access control methods are required. Especially in emergency conditions, where the patient's health situation is in peril, different healthcare providers associated with critical cases may need to be granted permission to acquire access to Electronic Health Records (EHRs) of patients. A major challenge in this area is to enable trustworthiness and to achieve traceability of access control to personal health data in emergency situations. To address the challenges of access control trustworthiness and traceability, we explore the coupling of context-aware access control mechanisms with a private and permissioned blockchain architecture and we investigate the security and robustness of the resulting technology. In our previous work [3], machine learning methods (LSTM NNs) have been applied to the patient's recent health history so as to predict the criticality of the patient's medical state and to correspondingly grant emergency clinicians context-aware access to sensitive health data using fuzzy logic [4]. The research objective of this work is to develop a proactive access control method that utilized blockchain technology to guarantee the integrity and security of the access control mechanism, and guarantee trust without the need for a trusted third party. This work encompasses the above-mentioned predictive mechanism, along with fuzzy procedures developed in our previous work [4], in the smart contracts of this private and permissioned blockchain network based on Hyperledger Fabric blockchain technology. Additionally, this work examines the latency for committing a query transaction to this client application from the blockchain network per access control case. A proactive access control mechanism is built within the blockchain system that exploits smart contracts of the private and permissioned Hyperledger Fabric-based blockchain network, which examines recent health metrics of a patient and predicts the patient's health criticality assessment, effectively managing access to the patient's EHRs.

Blockchain technologies in the medical sector

Blockchain based technologies implemented in the medical sector hold various benefits, but also many challenges as well regarding the acceptance by the medical community. Even if the technology of blockchain has benefits such as system performance, collaborative ecosystem, or innovative technological features, its applications in healthcare are in their early stage [5]. The perceptions of the individual issues such as the lack of knowledge, the organizational issues such as the implementation, the technological issues such as the blockchain model types, and market-related issues such as regulatory concerns indicate that blockchain-based applications in healthcare constitute an emerging field. This study points out the practical implications and thus is capable to assist developers and medical managers in identifying possible issues in implementing, developing, and planning blockchain-based health information exchange systems. According to the author, tackling these barriers can assist the widespread usage of blockchain-based health information exchanges in various medical settings and facilitate connectivity and interoperability in community and regional health information networks. Additionally, barriers of acceptance include among others, usability constraints, lack of management commitment, lack of a security-oriented culture, lack of awareness regarding legislations and health information technology risks [6]. Nevertheless, blockchain is being explored by stakeholders to enable better use of healthcare-related data, enhance compliance, improve patient outcomes, lower costs, and optimize business processes [7]. Nonetheless, in assessing if blockchain can fulfill the hype of a technology described as disruptive and revolutionary, it is important to ensure that blockchain design elements take under consideration the actual medical needs of regulators, providers, patients, and consumers. It is worth mentioning that the authors point out that the most praiseworthy advantages of blockchain are yet to

be realized. However, the efforts of blockchain pilots will finally lead to the promise of patient-driven medical systems in the form of open health data markets and precision medicine, finally reaching the patient.

Hyperledger fabric blockchain platform

Hyperledger Fabric is an open-source enterprise-based permissioned distributed ledger technology platform, designed for utilization in business contexts, which delivers key differentiating capabilities over other popular blockchain platforms. The Hyperledger Fabric project is governed by maintainers of multiple organizations and has a configurable and modular architecture, enabling optimization, versatility and innovation for several industry use cases such as healthcare, or banking. Fabric is the first distributed ledger platform which supports smart contracts authored in general-purpose programming languages such as Node.js, Go and Java, instead of constrained domain-specific languages. Fabric platform is additionally permissioned, which means that, contrary to a public permissionless network, the users are known to one another, instead of anonymous and thus fully untrusted. More specifically, even if the participants may not entirely trust each other, a network can be operated under a governance model which is constituted of what trust does exist among users, like a legal agreement or framework for managing disputes. Fabric is able to utilize consensus protocols which don't require a native cryptocurrency to fuel smart contract execution or to incent costly mining.

Hyperledger's first project, Fabric, is a permissioned blockchain platform. It operates similarly to most blockchains, which maintains a ledger of digital events. The ledger events are structured as transactions and shared among users. These transactions are executed without a cryptocurrency, and are confidential, private, and secured. Fabric is able to exclusively be updated by consensus of the participants. At the time the records have been inputted, they cannot be modified. Fabric is a solution, focused on compliance with regulations and scalability. Each user must register proof of identity to membership services so as to yield system's access. Additionally, in Hyperledger Fabric, the absence of cryptographic mining operations signifies that the platform can be deployed with roughly the same operational cost as any other distributed system, while avoidance of a cryptocurrency reduces some significant risk. Apart from that, the medical history of the patient is very sensitive regarding private data and is protected by international laws. A successful medical system should minimize the risk of medical data leakage so as to protect patients according to regulations.

Furthermore, a channel supports the communication between the members of a private network and ensures the privacy of data and which in our application, corresponds to a hospital. The Hyperledger Fabric platform is a Private and Permissioned blockchain network, meaning only authorized users have read and write rights respectively, where all the members' actions could be traced by authorized administrators and where all members have their own identities. In this work a data access control is manipulated exclusively inside the channel, and thus, data security and integrity are achieved. The consensus of the action in the blockchain network between the members is based on the byzantine fault tolerant protocol which is dependent on the opinion of members' majority.

Methods

Proactive access control mechanism

In this section, it is described how we extend our previous works on context-aware access control policies in healthcare [8] by considering context-aware access policies for identifying the patient's current situation [4] and predicting the patient's future state based on the resent health history of the last five hours [3], where the data regarding the recent health history, were obtained from the publicly available online database [9]. This work couples the proactive access control mechanism [4] with a private and permissioned blockchain network by leveraging the Hyperledger Fabric blockchain platform.

The predictive mechanism of our previous study [3], implemented with LSTM, outputs the predictions of health values for the following two hours by receiving as input the recent health values from the Blockchain Fabric Host. Afterwards, the Enhanced Blockchain API Server assesses the criticality of the future health status of the patient, considering the patient's age, the current health metrics and the predicted health metrics for the following two hours. The criticality assessment defines the decision about emergency access permission by emergency medical team to the patient's sensitive EHRs, in case the requestor is valid.

In our previous work [4], we created a fuzzy logic-based mechanism for access control governed by fuzzy rules to determine critical situations. This fuzzy mechanism [4] used fuzzy rules that associate contextual attributes with fuzzy values and generated as output an assessment of the criticality of the patient's health state. The related contextual attributes, which are represented in a context model, are analyzed in our previous work [10]. In our previous our work [3], we extended the fuzzy access control mechanism by considering except from the patient's current status his future one as well, by predicting the patient's future medical state.

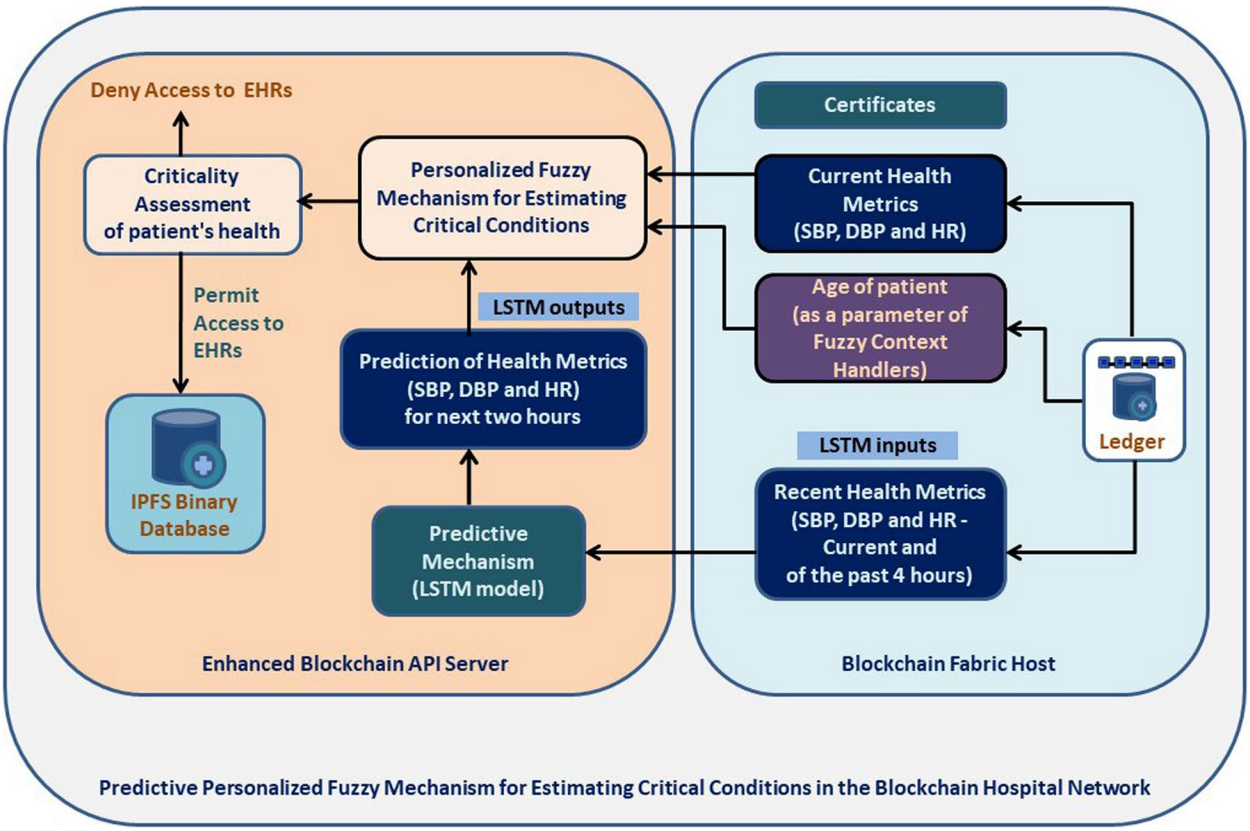

Fig. 1 Conceptual approach

The proactive mechanism (Fig. 1) queries the ledger of the blockchain, where the history of these metrics' transactions is stored. It receives the current health metrics of Systolic Blood Pressure (SPB), Diastolic Blood Pressure (DBP), and Heart Rate (HR), along with the same health metrics of the past four hours, and after predicting the health metrics for the next two hours, by leveraging the LSTM predictive machine learning integrated algorithm, it forwards the results to the fuzzy mechanism for assessing the criticality of the patient's situation. The mechanism receives the current heath metrics (SBP, DBP, and HR) from the ledger along with the parameter of patient's age and by leveraging the integrated fuzzy logic algorithm, it makes a decision about the criticality of the patient's health, by taking into consideration both the current and the predicted health metrics. Afterwards, if the assessment of patient's health is "Critical", the access to the medical binary database is permitted, else the access to patient's sensitive private health metrics is prohibited. This binary database, is an off-chain InterPlanetary File System (IPFS) [11], where each file's encrypted data are stored in multiple nodes, in case of large file volumes.

A numeric example of the functionality of the mechanism is illustrated in Fig. 2. The example is a case study of a 77-year-old patient with his health metrics (SBP, DBP, and HR) of the past four hours, as illustrated. In this example, the overall criticality result is deduced dependent on the three individual results of the patient's current and future status. In this case, even if based on the current situation the patient's condition is not deemed critical, it is critical for both after one and two hours. The overall critically result is deduced based on the Eq. (2) which states that even one of the current or future situations is critical, then if the requestor belongs in the emergency team, he can be granted access to the patient's sensitive EHRs.

Results

Implementation

Architecture of blockchain-based access control mechanism

In Fig. 3 the architecture of blockchain-based access control mechanism is illustrated. The certificates administrator issues and grants a personal identity card which includes the credentials, the role, and the digital signature of each specific user. In case of an emergency incident, a certified user, e.g. a member of the emergency

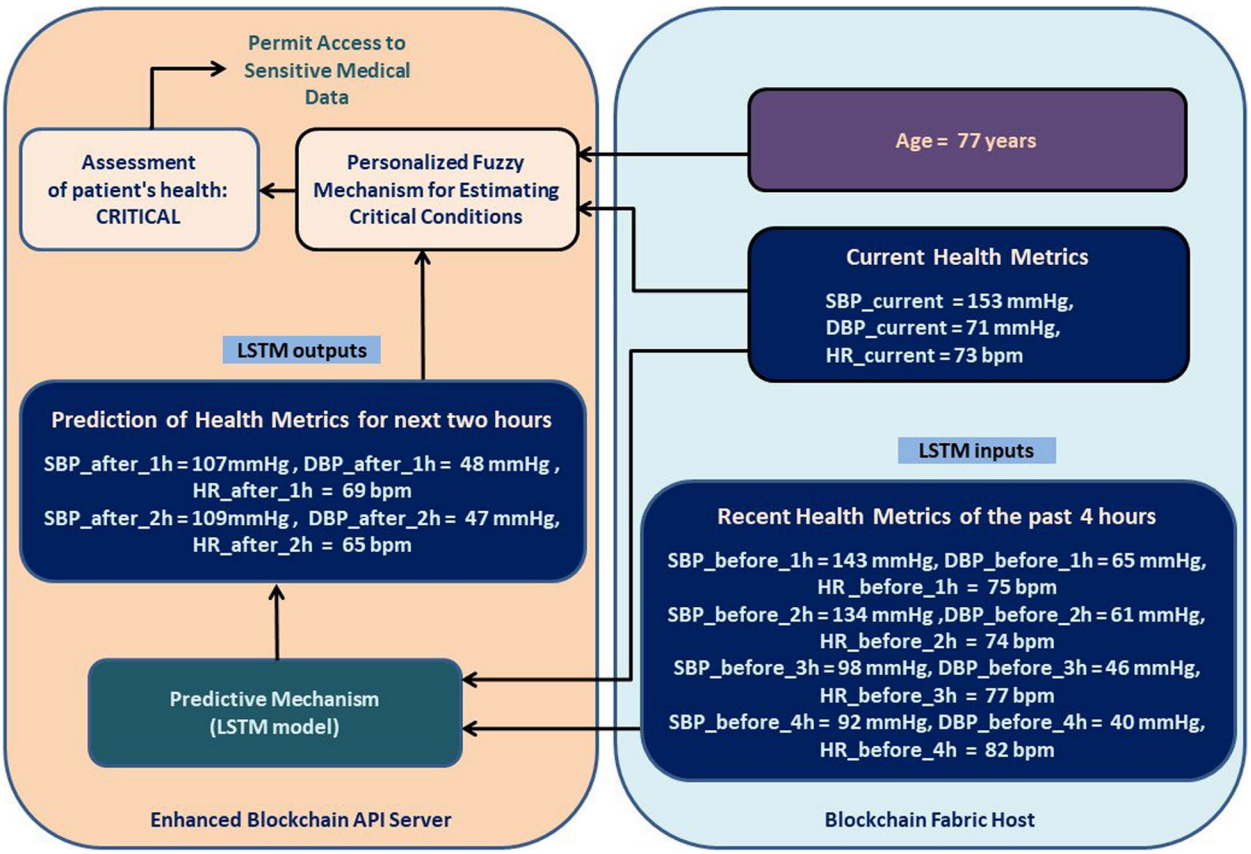

Fig. 2 Illustrative example

team, by using this identity card by a client application, requests access to a patient's sensitive medical data (IPFS database). Then the identification control of "Enhanced Blockchain Application Programming Interface (API) Server" confirms the user's identity features and rejects or proceeds the request accordingly. In case of successful identification, the request proceeds to the predictive personalized fuzzy mechanism for estimating critical situations, and triggers the relating algorithm of personalization. Finally, if the ultimate estimation about the patient's health is not critical then the request is finally rejected. On the contrary, if the ultimate estimation is critical then the requestor is granted access to IPFS database. Thus, a robust access control mechanism is achieved in emergency situations. In more details, in a critical situation where the life of a patient is in peril, the professional clinicians of an emergency team should be able to have immediate access to this patient's health data, so as to be able to help more successfully the patient.

Technical implementation

Hyperledger Fabric doesn't have by default its own API Server in order to communicate with front-end applications, so this work addresses this issue by creating an appropriate one, which is incorporated in the "Blockchain Network". An overview of the integrated system architecture is shown in Fig. 4. At the right, the "Blockchain Hospital Network" is illustrated which runs in Linux operating system and consists of the following two sub-components: i) "Blockchain Fabric Host" and ii) "Enhanced Blockchain API Server". Specifically, the "Blockchain Fabric Host" contains: a) the "Hospital Channel" which services the users of the network, b) the "Smart contract" where the rules of transactions are defined, and c) the ledger where the transactions are recorded. The changes in the health metrics (SBP, DBP, and HR) of patients are always registered as transactions in the ledger, and thus, the user can query all patients' health history from the ledger. Respectively, the "Enhanced Blockchain API Server" i) incorporates all the rules of the smart contract, ii) runs the blockchain network and handles the appropriate user certificates of blockchain network, iii) encompasses our "Predictive

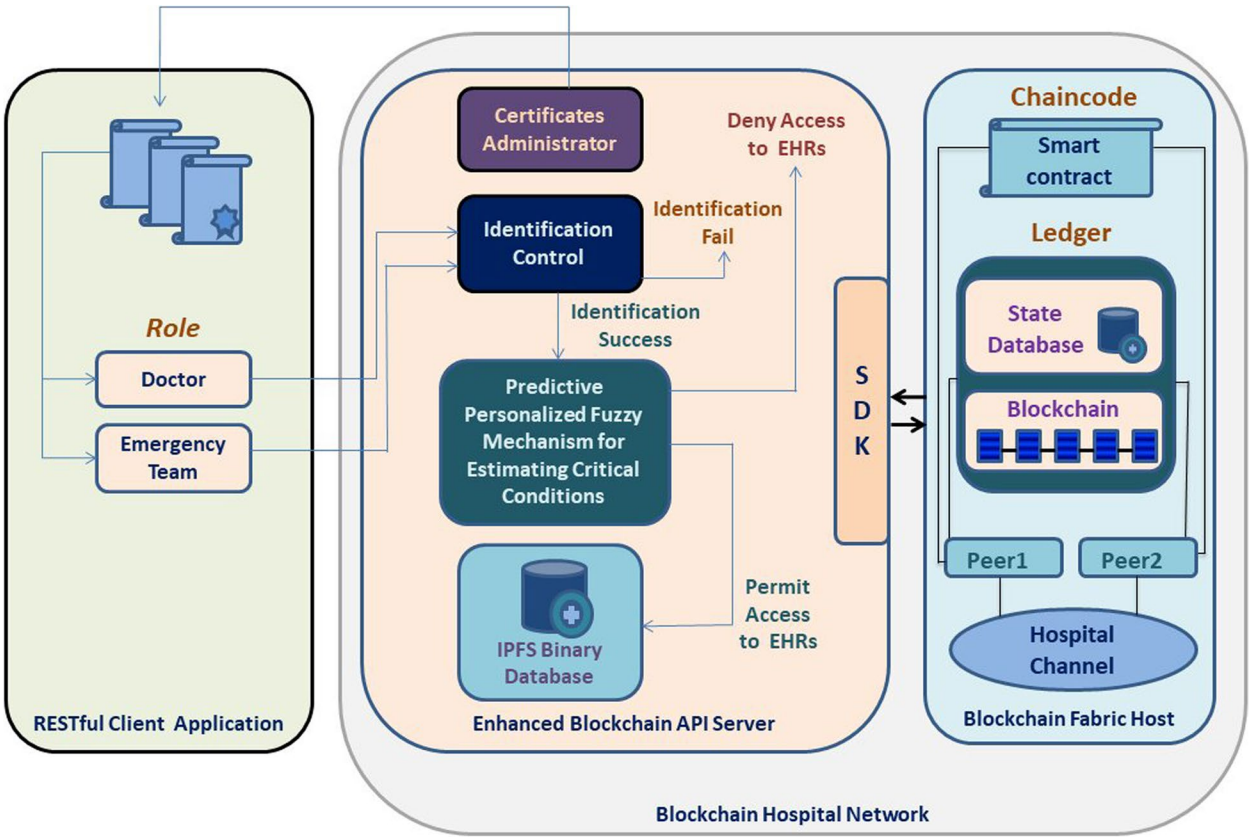

Fig. 3 Architecture of blockchain-based access control mechanism

Personalized Fuzzy Mechanism for Estimating Critical Conditions", and iv) provides and handles the communication between our "RESTful Client Application" with the "Blockchain Fabric Host". Additionally, at the left our "RESTful Client Application" is illustrated, which runs in Windows operating system, communicates with the blockchain network, and sends the adequate access control request and receives the respective response.

Contextual policies utilize context attributes to characterize allowable or not access requests and to permit or deny access to private information. Specifically, when a user requests access to specific healthcare data, the policy–based access control mechanism evaluates the related contextual policies exploiting attributes. This current research, encompasses the context-based, predictive access control mechanism of our previous work [3] in the Hyperledger Fabric platform, so as to enrich the blockchain network.

If a requestor who belongs in the emergency team needs to submit a query along with her appropriate credentials, in order to access the recent health history of a specific patient, and if the "Enhanced Blockchain API Server" deduces that the patient is indeed in danger, then the person who handles the front-end application receives in the "RESTful Client Application" is sent the patient's personal information as well as recent health history.

The several methods, which handle the read or write rights to the ledger of blockchain fabric hosts, are handled by the smart contract, which is known as chaincode. The smart contract of the blockchain fabric host is responsible for granting read or write access to the ledger along with implementing suitable related queries on its' data. The "Smart Contract Handling" mechanism of the "Enhanced Blockchain API Server" encapsulates the smart contract rules and is integrated with the predictive, personalized fuzzy mechanism so as evaluate the criticality of the patient's health by considering her current and predicted future health metrics, as well.

In case the access control response which has been sent to this client application is "Permit", then the requestor is granted access to patient's sensitive medical data and the patient's respective information is illustrated to the appropriate panes, as explained analytically in Fig. 6, so that the user such as the emergency doctor has a thorough initial view.

To build the LSTM RNNs trained model, components of tensorflow and keras in Linux are implemented. All

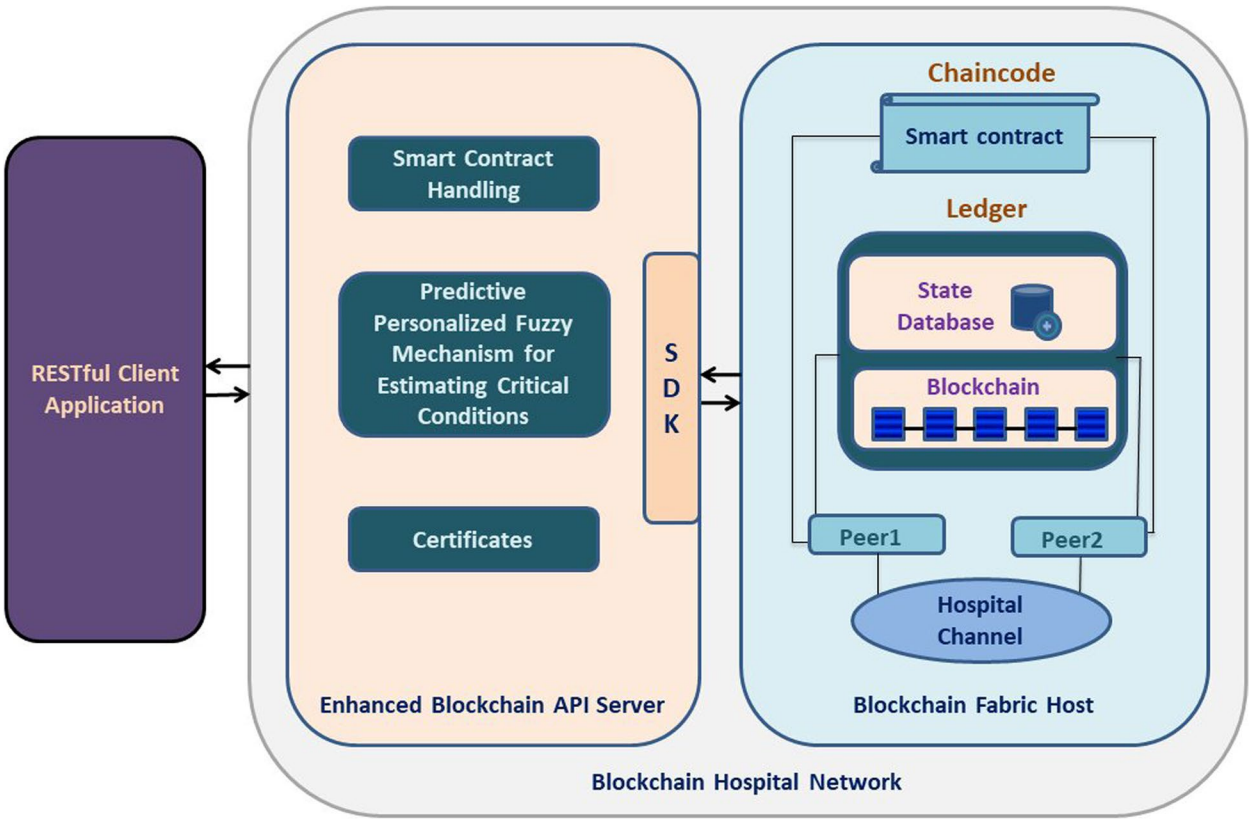

Fig. 4 Blockchain implementation (Custom API and Fabric Server)

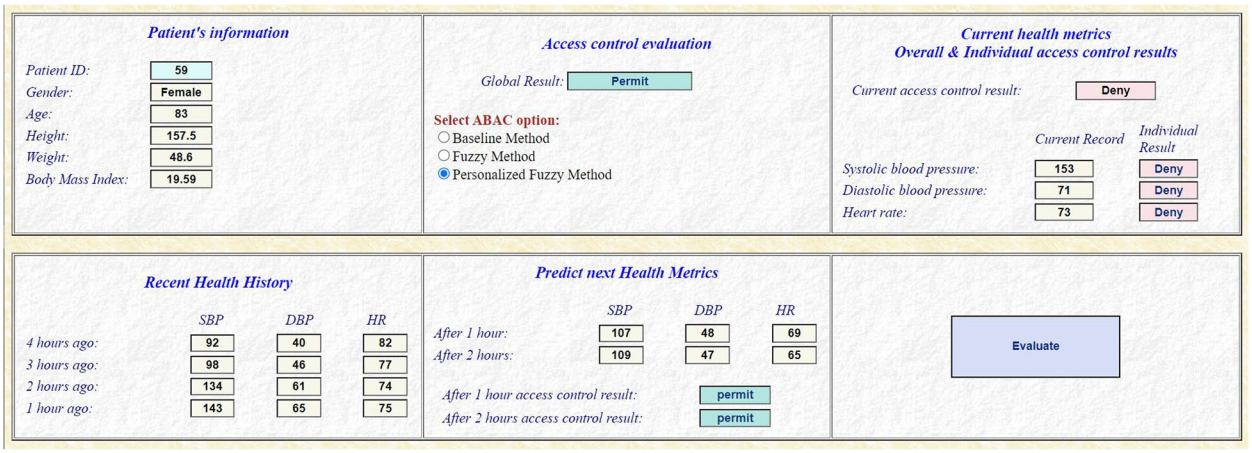

Fig. 5 RESTful client application, for communication with the blockchain network, for contextual predictive access control

trained models are integrated in this "Enhanced Blockchain API Server", so as to calculate on the fly the health metrics predictions by the corresponding incorporated trained neural network model per patient.

The RESTful client application comprises six panes (Fig. 5). In the upper left pane, the patient 's Body Mass Index (BMI), weight, height, age, gender, and ID are demonstrated, whereas in the upper center pane, the overall access result is demonstrated. Below this component, the access control selectable options are illustrated, which are the following: i) the baseline method, which considers basic thresholds as limits in order to grant access;

ii) the non-personalized method, which considers only the fuzzy inferencing process; and iii) the personalized method, which takes into account the fuzzy inferencing process and the personalization aspect of age. All the three already mentioned access control cases consider the health metrics of SBP, DBP and HR, based on the patient's diagnosis of present medical status. In the upper right pane, the patient's current health metrics are presented as well as the current medical state result of the prognostic access control case, which has already been checked on the previous pane, along with the individual access results per health metric referring to the patient's current medical state. In the lower left pane, the patient's recent medical history within the last five hours is demonstrated. In the lower center pane, the LSTM NNs mechanism predicts the health metrics' values for the following two hours as well as the respective access requests by using the fuzzy inferencing system [4]. Finally, in the lower right pane, the button 'Evaluate' provides the system's decision according to the chosen access control case.

Evaluation

Evaluation scenarios and datasets

The three predictive scenarios of baseline method, personalized fuzzy method, and personalized fuzzy method which inference the criticality of patient's health state, were tested. More information about how all three methods are implemented can be found in [3]. In this work, in all three scenarios the requestor is a member of the emergency medical team and wants to have an immediate and privileged access to sensitive data of a patient who is probably is a critical situation. The whole access control policy rules are implemented as follows in Eq. (1) and Eq. (2).

$$\begin{gathered}\text{If } (((\text{role\_of\_requestor} = \text{“Doctor”}) \text{ OR} \\ (\text{ role\_of\_requestor} = \text{“Emergency Team”}))\textit{AND} \\ (\text{ requestor\_credentials } = \text{“Valid”})) \\ \text{then (Identification Success)}\end{gathered} \tag{1}$$

$$\begin{gathered}\text{If((Identification Success) AND} \\ \text{context expression } ((\text{CRITICAL}_{\text{SITUATION\_CURRENT}} = \text{true}) \text{OR} \\ (\text{CRITICAL}_{\text{SITUATION\_AFTER\_1\_HOUR}} = \text{true}) \text{ OR} \\ (\text{CRITICAL}_{\text{SITUATION\_AFTER\_2\_HOURS}} = \text{true}))) \\ \text{then (Critical Situation)}\end{gathered} \tag{2}$$

In this work the three scenarios utilizing the public dataset [9] were tested, including four thousand patients and comprising one file per patient. Each patient file, among others, includes SBP, DBP and HR health metrics history. These time-series sequential data are taken sporadically every ten minutes, or twenty minutes or even one hour or more. We built an additional software component, in [3] to extract the health metrics of every hour, while all the files that had time gaps more than one hour were excluded. For more information regarding the data pre-processing, please refer to [3]. This research integrates the health metrics data used in our previous work [3] by incorporating their health metric values in the smart contract as initial values. More particularly, the EHRs per patient were inserted programmatically, in adequate format in the smart contract file. This file in Go programming language is handled, which is the default language for creating the smart contracts in Hyperledger Fabric.

Evaluation results

The response time of the system from the moment an emergency team member is measured, by communicating with API server using the client application, asks permission to access the patient's sensitive medical data, until he is finally granted this access or not, which is considered as a query transaction. This response time of committing a query transaction so that the "Enhanced Blockchain API Server" responds to the RESTful client application in milliseconds (ms) is demonstrated in Table 1. Three cases are taken under consideration. In the first case the "Non-Predictive Personalized Fuzzy Method" of our previous work [4] is examined where only the fuzzy mechanism is integrated in the blockchain network, by considering only the current situation and without taking into consideration the prediction of the patient's future state. In the second case, the "Predictive Personalized Fuzzy Method—with trained LSTM models" is examined where the LSTM models, which are used for the prediction, are trained in advance by using a considerable amount of data, and are then implemented in the predictive mechanism for the evaluation. In the third case, the "Predictive Personalized Fuzzy Method—with training LSTM models" is examined, where these models are trained by the whole amount of available data "on the fly" at the exact

Table 1 Latency for committing a query transaction to our client application from the blockchain network per access control case

Blockchain access control case	Time (ms)
Non-Predictive Personalized Fuzzy Method (integrating the fuzzy mechanism, without the LSTM prediction)	1887
Predictive Personalized Fuzzy Method (with trained LSTM models)	5104
Predictive Personalized Fuzzy Method (with training LSTM models)	14736

moment of the access request and are right away implemented and incorporated in the predictive mechanism which proceeds to the estimation of the patient's state. It is deduced from Table 1 that the first blockchain access control case of the "Non-Predictive Personalized Fuzzy Method" has the shortest response time for committing a query transaction, while the third case of the "Predictive Personalized Fuzzy Method—with training LSTM models" corresponds to the longest response time. To our knowledge not a scientific work was published up till now that incorporates predictive fuzzy techniques in estimating a patient's critical health state in order to provide access control on a blockchain network system and thus there is not time comparison with similar access control cases. Nevertheless, our mechanism enhances trustworthiness and achieves traceability of access control to personal health data in emergency situations. This work could contribute to the review work of Sookhak et al. [12] by introducing the latency due to the integration of a predictive fuzzy personalized mechanism within the hyperledger-based blockchain network.

Discussion

Access control schemes in critical medical conditions

Yielding access to patient's medical information constitutes a sensitive concept due to the fact that there is the danger for patient's private information to be exposed to malicious subjects. Granting access to EHRs in critical conditions improves medical decision-making and increases the quality of patient's life [13]. Povey et al. [14] suggest a retrospective access control method so that the system isn't misused, and where transactions are used to assure the integrity of the system is able to be recovered during a data breach case. The authors suggest an informative break-glass approach regarding misuse before its activation, while stating that in an emergency case, the users are able to operate the tool but, after the event, the users must inform the system's administrator to avoid a penalty.

Saberi et al. [15] present a synthesis of IPFS with blockchain technology. Blockchain is used as a secure incorporated system for ABAC break-glass mechanisms, and as an IPFS that creates a distributed file storage infrastructure to store big files of medical data. Furthermore, the conceptual model of Saberi et al. [16] was based on the blockchain technology, on an IPFS and on ABAC, that doesn't necessitate circumventing the access control system so as to constitute the patient's healthcare data. Particularly in emergencies, the medical professionals are permitted access to the EHRs in time based on the attribute-related security rights that are decided by the patients.

Manasa et al. [17] introduced an access control scheme for patient-centric privacy regarding medical data in critical states. The model of Tsegaye et al. [18] assures the EHRs confidentiality based on ABAC and RBAC, whereas ensuring integrity by the exploitation of Clark–Wilson model for safeguarding the EHRs from both unauthorized entities and authorized medical professionals. Additionally, by implementing their paradigm, the EHRs are protected and any access problems are dealt with whereas yielding access of medical records in emergencies.

Farinha et al. [19] introduced an implementation of the break-glass paradigm in a real-life scenario to enhance the legislation regarding genetics. In addition to this, the authors evaluated the process of encompassing legislation into the healthcare practice and the impact of break-glass usage by reaching a consensus that the break -glass features were able to filter the non-authorized accesses that wouldn't be prevented otherwise. Georgakakis et al. [20] created the spatio-temporal Emergency RBAC scheme dependent on spatiotemporal context of location, time, and roles' hierarchy to grant exception access in emergencies. In their scheme, users are able to access resources either through the common process of assigned roles based on the security policy of the organization or demand access to a resource through the emergency access procedure.

Marinovic et al. [21] suggested a break-glass paradigm which builds a break-glass policy by determining the reason why the access wasn't granted. Their scheme represented missing and conflicting data, allowing the policy to produce a more informed decision when faced with inconsistent or missing knowledge. Maw et al. [22] introduced an access control scheme, in networks of body area and wireless sensor networks that supports a flexible emergency access control of accessing data. Guan et al. [23] suggested a paradigm leveraging the patients' fingerprints to assist doctors to have temporary access of medical information. If a patient is in a coma, the doctor needs to access the patient's medical records immediately to take efficient aid measures. Künzi et al. [24] introduced an access mechanism in critical conditions for EHR systems which encompass digital rights protection of health records. Their approach for emergency situations, mitigates the emergency key distribution problem and can be integrated in distributed environments.

Contextual attributes for access control in critical medical conditions

Context identifies a specific condition by considering the circumstances where an event arises. Each contextual attribute serves as a quantitative primitive, like

the location of the requestor. Attributes in ABAC are divided in the four following categories [25]: i) subject attributes identify the user requesting access, like age; ii) action attributes identify the requested action like read; (c) object attributes identify the resource of access like a medical record; and (d) environment attributes are related with factors of dynamic access control, like time.

In the healthcare domain, contextual information that identifies a patient's medical critical condition should be characterized in managing access to the medical sensitive data so as to assure the most effective treatment. Correspondingly, the implementation of access control models that incorporate the context notion, like the concept of dynamically altering contextual attributes that characterize the current status, is needed. More particularly, context is deemed as any information identifying the status of an entity, like an object, place or person, based on the relation between a requestor and an application [26]. Using contextual information assists the implementation of access control policies by considering the conditions of access requests' evaluation. As an example, in emergency cases, an emergency medical professional intends to access the patient's medical information to efficiently address a critical situation. The values of contextual information are collected, for example, from IoT devices, like a wearable which measures blood pressure. In emergency situations, the emergency healthcare teams must be able to gain access instantly to the patients' healthcare records.

The following works are reviewed to identify context-based information for facilitating the evaluation of critical healthcare conditions. Nomikos et al. [27] examined patients' conditions using attributes, like the time when the stroke happened, the age, the DBP, the SBP, the Glasgow and the Scandinavian coma scales that characterize the patient's consciousness level. Mahmood et al. [28] estimated the crisp values of blood pressure parameters from the HR. Djam et al. [29] proposed a fuzzy expert system for the hypertension management utilizing the fuzzy logic paradigm. As fuzzy inputs, BMI, age, DBP, and SBP were deemed to estimate the risk for hypertension.

Manasa et al. [17] considered contextual attributes like the patient's medical history, allergies, prescriptions, and basic profile. Furthermore, an emergency attribute is considered for emergency access. A fuzzy expert system for estimation of heart diseases, that utilizes the approach of cuckoo search, is suggested by Moameri et al. [30] by considering the attributes of age, type of chest pain, blood pressure, electrocardiogram results, maximum HR, and cholesterol level.

Few studies take under consideration users' specificities for the evaluation of access policies. For instance, the increased HR is considered as critical for a specific patient in case that his healthcare situation, his activity levels or his age are taken into account. Zerkouk et al. [31] suggested an adaptable access control paradigm and its related architecture, where the security policy is based on an analysis of the user's monitored behavior. Røstad et al. [32] introduced a mechanism for personalized access control in health records. Their scheme combines properties and concepts of RBAC and DAC to manage the desired properties. Additionally, the authors deem a set of common policies that cannot be edited by the patient, along with a set of personal policies updated by the patient. Petković et al. [33] suggested security and privacy enhancements in a RBAC paradigm. Their system includes personalized access control which is a combination of user-managed and role-based access control, along with a cryptographic enforcement, that includes effective key management for accessing medical data.

Son et al. [34] suggested a dynamic access control paradigm, for preserving the personal health information security in a cloud environment by considering contextual attributes for dynamic access. Their model utilizes the ontological concept of 5W1H to process context-based attributes for dynamic access. Their approach refers to the dynamic access control in medical sector.

Hyperledger fabric blockchain for access control in critical medical conditions

Various implementations have been proposed which utilize the Hyperledger Fabric blockchain for managing the access control in emergency medical situations. First of all, Son et al. [35] propose an emergency access control management framework to safeguard the patients' data. Their framework is formed dependent on permissioned blockchain Hyperledger Fabric, and defines regulations and rules by utilizing smart contracts and time duration to manage emergencies. Additionally, in their system the patients restrict the time to access the data in emergency conditions. Additionally, Le et al. [36] propose a Hyperledger Fabric-based system which deals with the problem of yielding access to patients' sensitive information when emergency situations arise and deals with the problems of setting appropriate rules for accessing the emergency control management of personal health records. Furthermore, Morelli et al. [37] present an audit-based framework which leverages the Hyperledger Fabric distributed ledger in order to increase accountability and decentralize the authorization decision process of Attribute-Based Access Control policies by using smart contracts,and implementing it in the use case of EHR access control.

Additionally, various research works refer to the inclusion of blockchain for medical access control in

non-emergency cases by leveraging the Hyperledger Fabric blockchain platform. Firstly, Chenthara et al. [38] develop a privacy-preserving framework called "Healthchain" based on blockchain technology which maintains integrity, security, privacy, and scalability of the e-health information. More specifically, the blockchain is built on Hyperledger Fabric, which is a permissioned distributed ledger solution by utilizing Hyperledger composer and stores EHRs by using IPFS to implement their "Healthchain" framework. Additionally, Zhan et al. [39] propose a paradigm which encourages the growth of healthcare data by enabling stakeholders to collaborate and share EHR trust. More specifically, the authors recommend a Hyperledger Fabric-based strategy to support the exchange of EHR models. By leveraging the Hyperledger Fabric blockchain, EHR stakeholders can be brought into the channel to facilitate data sharing. ABAC permits users to design the data access control policy, which can improve security. All the records stored in the blockchain are viewed utilizing the Hyperledger Fabric feature and cannot be destroyed or altered, supporting data traceability. Furthermore, Khan et al. [40] introduced a blockchain Hyperledger Fabric-enabled consortium architecture for handling sensitive medical data in a serverless peer-to-peer network.

Additionally, non-healthcare solutions based on Hyperledger Fabric were introduced. Indicatively, Khan et al. [41] used blockchain Hyperledger Fabric and a metaheuristic-enabled genetic algorithm for fog node management.

Non-hyperledger fabric blockchain-based for access control in critical medical conditions

However, various blockchain-based implementations rely on different blockchain platforms, which aren't based on the Hyperledger Fabric platform, for medical access control. Firstly, in the work of Sultana et al. [42] blockchain was utilized to keep an audit trail of medical data transmissions. Their suggested model comprises two users who share health data. In medical image sharing, the medical technologist who generates X-ray files etc. is the sender, patient is the receiver, and the data in question are the medical image files. Additionally, the patient can share information with a doctor by having the patient as the sender and doctor as the receiver. More specifically, their model uses a public blockchain such as Ethereum that utilizes proof-of-work consensus mechanism in order to validate nodes. Their work provides an overview of their decentralized trustless model that aims to deal with security issues based on storing and sharing of health records and images in an EHR system. More specifically, their work enhances the security of health images and medical records transmission based on a combination of zero trust principles and blockchain. Furthermore, according to Ma et al. [43] blockchain is able to be utilized to query genomic dataset audit trail and build a space and time efficient log. Thus, it provides a promising solution for distributing genomic information with accountability requirement across various sites. Additionally, Gursoy et al. [44] develop a particular smart contract to query and store gene-drug interactions utilizing a multi-mapping index-based method by leveraging the Ethereum blockchain. Their smart contract stores each pharmacogenomics observation, a gene-variant-drug triplet with outcome, in a mapping by a unique identifier, permitting for space and time adequate query and storage.

Additionally, non-healthcare solutions based on non-Hyperledger Fabric blockchain platform were introduced. Indicatively, first of all, Khan et al. [45] proposed a solution for small and medium-sized enterprises which incorporates a blockchain structure with IoT-enabled permissionless network. Moreover, Khan et al. [46] introduced a Hyperledger Sawtooth solution which incorporates a peer-to-peer network and applied for testing in exchanging information between connected devices of industrial internet-of-things. Furthermore, Khan et al. [47] proposed an IoT-blockchain-based collaborative technology applied in a Hyperledger Sawtooth architecture, so as to investigate digital multimedia forensics. In addition to this, Dhasaratha et al. [48] investigate the applicability of a distributed reinforcement learning approach in a Federated Learning multi-disciplinary reinforcement system which handles post-COVID-19 patient data of IoMT applications.

Positioning

As seen in the research papers' comparison in Fig. 6, this work examined research articles by considering the following criteria: i) medical access control, ii) emergency Medical Situations, iii) Hyperledger Fabric based blockchain network, iv) predicting emergency medical situations with LSTM NNs mechanism, and v) fuzzy logic. To our knowledge up till now only this work fulfills all the above-mentioned criteria, which encompasses the integration of a predictive fuzzy personalized mechanism within a Hyperledger based blockchain network by predicting emergencies in the healthcare sector.

Conclusions

In critical medical conditions, the patients' health criticality should be taken under consideration when allowing access to their sensitive EHRs. Thus, identifying life threatening cases in automated healthcare access control systems is imperative. This work introduces a permissioned blockchain network for access control

Research Works	Medical Access Control	Emergency Medical Situations	Hyperledger Fabric based Blockchain Network	Predicting Emergency Medical Situations with LSTM NNs Mechanism	Fuzzy Logic
Son et al., 2021 [35]	√	√	√		
Le et al., 2022 [36]	√	√	√		
Morelli et al., 2019 [37]	√	√	√		
Chenthara et al., 2020 [38]	√		√		
Zhan et al., 2022 [39]	√		√		
Yin et al., 2021 [49]		√		√	
Kadri et al., 2019 [50]		√		√	
Tsai et al., 2017 [51]		√		√	
Cheng et al., 2020 [52]		√		√	
Nwakanma et al., 2021 [53]		√		√	
Reddy et al., 2018 [54]		√		√	
Moameri et al., 2018 [30]		√			√
Guzman et al., 2017 [55]		√			√
de Oliveira et al., 2023 [56]	√	√			
de Oliveira et al., 2022 [57]	√	√			
Jakhar et al., 2024 [58]	√		√		
Jena et al., 2024 [59]	√		√		
Byeon et al., 2024 [60]	√				√
Khan et al., 2022 [40]	√		√		
Our current work	√	√	√	√	√

Fig. 6 Positioning of proposed method [30, 35–40, 49–60]

management in emergency health situations, which incorporates machine learning techniques along with a personalized fuzzy mechanism for estimating the patient's future health metrics, related to his recent history.

The developed access control mechanism provides secure access for emergency clinicians to sensitive information and simultaneously safeguards the patient's private data. The proposed permissioned blockchain network is capable of securing patient's sensitive information based on the personalized policies in the blockchain network. Furthermore, this approach is proactive because it provides access control based on near-future predictions about the criticality of the patient's situation. Moreover, it has the ability to track the history of who and when gained access to the sensitive patient's data so that trust is achieved as well. Additionally, in this work the integration this fuzzy predictive mechanism with machine learning techniques in the private and permissioned blockchain network assures the data security and enhances the users' traceability. One of the main challenges of this work was the integration of the fuzzy and predictive mechanism within the blockchain network. The combination of the fuzzy logic and the LSTM NNs algorithms with the rules of the smart contracts addressed this problem. Limitations of this approach include the incorporation of a small number of health metrics to characterize the criticality of a patient's situation. Additional metrics, such as drinking or smoking habits, the oxygen and the glucose levels in blood, existence of chronic diseases, or BMI could be taken under consideration in a future work. Furthermore, while, this work focuses solely on emergency situations where identifying the patient's current and future state is vital for the patient's survival, in a future work the integration of the prediction of diseases could be investigated to help the doctor to make the final diagnosis. In a future the encapsulation of additional predictive algorithms within the blockchain network could be investigated. Additionally, as future work the fuzzy predictive inferencing system of this work could be integrated to other blockchain-based platforms as well, such as Hyperledger Sawtooth.

Abbreviations

EHRs	Electronic Health Records
LSTM	Long Short Term Memory
NNs	Neural Networks
RBAC	Role-Based Access Control
DAC	Discretionary Access Control
MAC	Mandatory Access Control

ABAC	Attribute-Based Access Control
DBP	Diastolic Blood Pressure
SBP	Systolic Blood Pressure
HR	Heart Rate
BMI	Body Mass Index
IPFS	InterPlanetary File System
API	Application Programming Interface

Acknowledgements
This research has received funding from the EU, project H2020 826093, Asclepios (https://www.asclepios-project.eu/).

Authors' contributions
Conceptualization, E.P., D.A., Y.V., I.P. and G.M.; methodology, E.P., D.A., Y.V., I.P. and G.M.; software, E.P.; validation, D.A. and I.P.; formal analysis, D.A. and G.M.; investigation, D.A., Y.V., I.P. and G.M.; resources and data curation, E.P. All authors read and approved the final manuscript.

Funding
This research has received funding from the EU, project H2020 826093, Asclepios (https://www.asclepios-project.eu/, accessed on 22 September 2022). The funding bodies played no role in the design of the study and collection, analysis, and interpretation of data and in writing the manuscript.

Availability of data and materials
PPG-BP Database dataset: https://figshare.com/articles/dataset/PPG-BP_Database_zip/5459299 accessed on 8 April 2022; PHYSIONET Dataset https://physionet.org/content/challenge-2012/1.0.0/ accessed on 8 April 2022.

Declarations

Ethics approval and consent to participate
All methods used in this study were carried out in accordance with relevant guidelines and regulations.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1]Department of Informatics, University of Piraeus, Karaoli & Dimitriou 80, 18534 Piraeus, Greece. [2]Department of Business Administration, School of Business, Athens University of Economics and Business, Patission 76, 10434 Athens, Greece. [3]Institute of Communications and Computer Systems, Iroon Polytechniou 9, 15780 Zografou, Greece.

Received: 18 April 2023 Accepted: 1 October 2024
Published online: 15 October 2024

References

1. Ferrari E. Access control in data management systems. Synth Lect Data Manage. 2010;2(1):1–117. https://doi.org/10.2200/s00281ed1v01y201005dtm004.
2. Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to attribute based access control (ABAC) definition and considerations. 2014. https://doi.org/10.6028/nist.sp.800-162
3. Psarra E, Apostolou D, Verginadis Y, Patiniotakis I, Mentzas G. Context-based, predictive access control to electronic health records. Electronics. 2022;11(19):3040. https://doi.org/10.3390/electronics11193040.
4. Psarra E, Verginadis Y, Patiniotakis I, Apostolou D, Mentzas G. Accessing electronic health records in critical incidents using context-aware attribute-based access control. Intellig Decision Technol. 2022;15(4):667–79. https://doi.org/10.3233/idt-210214.
5. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based Health Information Exchange (HIE): A qualitative study from physicians' perspectives. BMC Medical Informatics and Decision Making. 2022 Mar 28;22(1). https://doi.org/10.1186/s12911-022-01815-8.
6. Natsiavas P, Rasmussen J, Voss-Knude M, Votis K, Coppolino L, Campegiani P, et al. Comprehensive user requirements engineering methodology for secure and Interoperable Health Data Exchange. BMC Med Inform Decision Making. 2018;18(1). https://doi.org/10.1186/s12911-018-0664-0.
7. Mackey TK, Kuo T-T, Gummadi B, Clauson KA, Church G, Grishin D, et al. 'fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine. 2019;17(1). https://doi.org/10.1186/s12916-019-1296-7.
8. Psarra E, Patiniotakis I, Verginadis Y, Apostolou D, Mentzas G. Securing access to healthcare data with context-aware policies. 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA. 2020 Jul 15; https://doi.org/10.1109/iisa50023.2020.9284393
9. Silva I, Moody G, Scott DJ, Celi LA, Mark RG. Predicting in-hospital mortality of ICU patients: the physioNet/computing in cardiology challenge 2012. Comput Cardiol. 2010;2012(39):245–8.
10. Psarra E, Verginadis Y, Patiniotakis I, Apostolou D, Mentzas G. A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain. In: Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020). Springer International Publishing; 2020. p. 1133–42. Available from: https://link.springer.com/chapter/10.1007/978-3-030-44038-1_104
11. Benet J. IPFS - Content Addressed, Versioned, P2P File System. arXiv [cs.NI]. 2014. Available from: http://arxiv.org/abs/1407.3561. Cited 2024 Apr 10.
12. Sookhak M, Jabbarpour MR, Safa NS, Yu FR. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. J Netw Comput Appl. 2021;178(102950). https://doi.org/10.1016/j.jnca.2020.102950.
13. Ben-Assuli O, Ziv A, Sagi D, Ironi A, Leshno M. Cost-effectiveness evaluation of EHR: simulation of an abdominal aortic aneurysm in the emergency department. J Med Syst. 2016;40(6):1–13. https://doi.org/10.1007/s10916-016-0502-9.
14. Povey D. Optimistic security. Proceedings of the 1999 workshop on New security paradigms. 1999 Sept;40–5. https://doi.org/10.1145/335169.335188
15. Saberi MA, Adda M, Mcheick H. Towards an ABAC Break-Glass to access EMRs in case of emergency based on Blockchain. 2021 IEEE International Conference on Digital Health (ICDH). 2021 Sept;220–2. https://doi.org/10.1109/icdh52753.2021.00041
16. Saberi MA, Adda M, Mcheick H. Break-glass conceptual model for distributed EHR management system based on blockchain, IPFS and ABAC. Proc Comput Sci. 2022;198:185–92. https://doi.org/10.1016/j.procs.2021.12.227.
17. Manasa D, Khanna KR. Sharing of PHR's in cloud computing. Int J Comput Sci Netw Secur (IJCSNS). 2015;15(11):86.
18. Tsegaye T, Flowerday S. A Clark-Wilson and ANSI role-based access control model. Inform Comput Secur. 2020;28(3):373–95. https://doi.org/10.1108/ics-08-2019-0100.
19. Farinha P, Cruz-Correia R, Antunes L, Almeida F, Ferreira A. From Legislation to Practice-A Case Study of Break the Glass in Healthcare. In: International Conference on Health Informatics. SciTePress; 2010. p. 114–20. Available from: https://www.scitepress.org/PublishedPapers/2010/27482/.
20. Georgakakis E, Nikolidakis SA, Vergados DD, Douligeris C, Spatio temporal emergency role based access control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism. In,. IEEE Symposium on Computers and Communications (ISCC). IEEE. 2011;2011:764–70. Available from: https://ieeexplore.ieee.org/abstract/document/5983932?casa_token=eltduNxBMFYAAAAA:7Jpwgq4b9pbTG6zNfGNgQRrCvqHtmVffaJhr2N-mwFDQeWHEcLs8aJbsO5K-jabdHA2q3VVXAw.
21. Marinovic S, Craven R, Ma J, Dulay N. Rumpole: A flexible break-glass access control model. In: Proceedings of the 16th ACM Symposium on Access Control Models and Technologies. ACM Digital Library; 2011. p. 73–82. Available from: https://dl.acm.org/doi/abs/10.1145/1998441.1998453?casa_token=gd3i95XCk-8AAAAA:lrsPwDqbh1SLrqdH6KY6HGh5nLAF1bVEP8FuHqaToWJl5kWq4_A0jyLqJ-T_0u-FON1Ws6Q8NpHu.
22. Maw HA, Xiao H, Christianson B, Malcolm JA. An evaluation of break-the-glass access control model for medical data in wireless sensor networks. In: 2014 IEEE 16th International Conference on e-Health Networking,

Applications and Services (Healthcom). IEEE; 2014. p. 130–5. Available from: https://ieeexplore.ieee.org/abstract/document/7001829.
23. Guan S, Wang Y, Shen J. Fingerprint-based access to personally controlled health records in emergency situations. Science China Information Sciences. 2017;61(5). https://doi.org/10.1007/s11432-017-9188-8.
24. Künzi J, Koster P, Petković M. Emergency Access to Protected Health Records. ebooks.iospress.nl. IOS Press; 2009. p. 705–9. Available from: https://ebooks.iospress.nl/publication/12753. Cited 2024 Apr 11.
25. Covington MJ, Sastry MR. A contextual attribute-based access control model. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 1996–2006. Available from: https://link.springer.com/chapter/10.1007/11915072_108.
26. Dey AK. Understanding and using context. Pers Ubiquit Comput. 2001;5(1):4–7. https://doi.org/10.1007/s007790170019.
27. Nomikos GD, Dounias G, Tselentis G, Vemmos K. Conventional vs. fuzzy modeling of diagnostic attributes for classifying acute stroke cases. In: Proceedings of the ESIT-2000, European Symposium on Intelligent Techniques. Aachen, Germany: Citeseer; 2000. p. 192–200. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9007a9af374e928ae25cf8b9c6eed1e2bfefd772.
28. Mahmood U, Al-Jumaily A, Al-Jaafreh M. Type-2 fuzzy classification of blood pressure parameters. In: 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE; 2007. p. 595–600.
29. Djam XY, Kimbi YH. Fuzzy expert system for the management of hypertension. Pac J Sci Technol. 2011;12(1):390–402.
30. Moameri S, Samadinai N. Diagnosis of coronary artery disease via a Novel Fuzzy expert system optimized by CUCKOO SEARCH. Int J Eng. 2018;31(12):2028–36.
31. Zerkouk M, Mhamed A, Messabih B. A user profile based access control model and architecture. Int J Comput Netw Commun. 2013;5(1):171–81.
32. Røstad L, Nytrø Ø. Personalized access control for a personally controlled health record. In: Proceedings of the 2nd ACM workshop on Computer security architectures. ACM; 2008. p. 9–16.
33. Petković M, Conrado C, Hammoutène M. Cryptographically enforced personalized role-based access control. In: Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006). Springer US; 2006. p. 364–76. Available from: https://link.springer.com/chapter/10.1007/0-387-33406-8_31.
34. Son J, Kim J-D, Na H-S, Baik D-K. Dynamic access control model for privacy preserving personalized healthcare in cloud environment. Technol Health Care. 2015;24(s1):S123–9.
35. Son HX, Le TH, Quynh NTT, Huy HND, Duong-Trung N, Luong HH. Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems. In: Mobile, Secure, and Programmable Networking: 6th International Conference, MSPN 2020. Springer International Publishing; 2021. p. 44–56. Available from: https://link.springer.com/chapter/10.1007/978-3-030-67550-9_4.
36. Le HT, Thanh LNT, Vo HK, Luong HH, Tuan KNH, Anh TD, et al. Patient-chain: Patient-centered healthcare system a blockchain-based technology in dealing with emergencies. In: Parallel and Distributed Computing, Applications and Technologies. Cham: Springer International Publishing; 2022. p. 576–83.
37. Morelli U, Ranise S, Sartori D, Sciarretta G, Tomasi A. Audit-based access control with a distributed ledger: Applications to healthcare organizations. In: International Workshop on Security and Trust Management. Cham: Springer International Publishing; 2019. p. 19–35.
38. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using Blockchain Technology. PLOS ONE. 2020;15(12). https://doi.org/10.1371/journal.pone.0243043.
39. Zhan W, Chen C-L, Weng W, Tsaur W-J, Lim Z-Y, Deng Y-Y. Incentive EMR sharing system based on consortium blockchain and ipfs. Healthcare. 2022;10(10):1840. https://doi.org/10.3390/healthcare10101840.
40. Khan AA, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA. BIoMT: A state-of-the-art consortium Serverless Network Architecture for healthcare system using blockchain smart contracts. IEEE Access. 2022;10:78887–98. https://doi.org/10.1109/access.2022.3194195.
41. Khan AA, Laghari AA, Gadekallu TR, Shaikh ZA, Javed AR, Rashid M, et al. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Comp Electr Eng. 2022;102:108234. https://doi.org/10.1016/j.compeleceng.2022.108234.
42. Sultana M, Hossain A, Laila F, Taher KA, Islam MN. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med Inform Decis Mak. 2020;7(20):1–10. https://doi.org/10.1186/s12911-020-01275-y.
43. Ma S, Cao Y, Xiong L. Efficient logging and querying for blockchain-based cross-site Genomic Dataset Access Audit. BMC Med Genomics. 2020;13(S7):1–13. https://doi.org/10.1186/s12920-020-0725-y.
44. Gürsoy G, Brannon CM, Gerstein M. Using ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Med Genomics. 2020;13(1):1–11. https://doi.org/10.1186/s12920-020-00732-x.
45. Khan AA, Laghari AA, Li P, Dootio MA, Karim S. The collaborative role of Blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. Scientific Reports. 2023;13(1). https://doi.org/10.1038/s41598-023-28707-9.
46. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S. Internet of things (IOT) security with blockchain technology: A state-of-the-art review. IEEE Access. 2022;10:122679–95. https://doi.org/10.1109/access.2022.3223370.
47. Khan AA, Shaikh AA, Laghari AA. IOT with multimedia investigation: a secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. Arab J Sci Eng. 2022;48(8):10173–88. https://doi.org/10.1007/s13369-022-07555-1.
48. Dhasaratha C, Hasan MK, Islam S, Khapre S, Abdullah S, Ghazal TM, et al. Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. CAAI Transact Intell Technol. 2024. https://doi.org/10.1049/cit2.12287.
49. Yin J, Han J, Xie R, Wang C, Duan X, Rong Y, et al. MC-LSTM: Real-time 3D human action detection system for intelligent healthcare applications. IEEE Trans Biomed Circuits Syst. 2021;15(2):259–69. https://doi.org/10.1109/tbcas.2021.3064841.
50. Kadri F, Baraoui M, Nouaouri I. An LSTM-based deep learning approach with application to predicting hospital emergency department admissions. In: 2019 International Conference on Industrial Engineering and Systems Management (IESM). IEEE; 2019. p. 1–6.
51. Tsai F-S, Weng Y-M, Ng C-J, Lee C-C. Embedding stacked bottleneck vocal features in a LSTM architecture for automatic pain level classification during emergency triage. In: 2017 Seventh International Conference on Affective Computing and Intelligent Interaction (ACII). IEEE; 2017. p. 313–8.
52. Cheng N, Kuo A. Using Long Short-Term Memory (LSTM) neural networks to predict emergency department wait time. Stud Health Technol Inform. 2020;272:199–202. https://doi.org/10.3233/SHTI200528.
53. Nwakanma CI, Islam FB, Maharani MP, Kim D-S, Lee J-M. IoT-based vibration sensor data collection and emergency detection classification using long short term memory (LSTM). In: 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). IEEE; 2021. p. 273–8.
54. Reddy BK, Delen D. Predicting hospital readmission for lupus patients: An RNN-LSTM-based deep-learning methodology. Comput Biol Med. 2018;101:199–209. https://doi.org/10.1016/j.compbiomed.2018.08.029.
55. Guzman J, Melin P, Prado-Arechiga G. Design of an optimized fuzzy classifier for the diagnosis of blood pressure with a new computational method for expert rule optimization. Algorithms. 2017;10(3):79. https://doi.org/10.3390/a10030079.
56. de Oliveira MT, Verginadis Y, Reis LHA, Psarra E, Patiniotakis I, Olabarriaga SD. AC-ABAC: attribute-based access control for electronic medical records during acute care. Expert Syst Appl. 2023;213:119271. https://doi.org/10.1016/j.eswa.2022.119271.
57. de Oliveira MT, Reis LH, Verginadis Y, Mattos DM, Olabarriaga SD. SmartAccess: Attribute-based access control system for medical records based on Smart Contracts. IEEE Access. 2022;10:117836–54. https://doi.org/10.1109/access.2022.3217201.
58. Jakhar AK, Singh M, Sharma R, Viriyasitavat W, Dhiman G, Goel S. A blockchain-based privacy-preserving and access-control framework for electronic health records management. Multimed Tools Appl. 2024;19:1–35. https://doi.org/10.1007/s11042-024-18827-3.
59. Jena SK, Kumar B, Mohanty B, Singhal A, Barik RC. An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in

the healthcare industry. Decision Anal J. 2024;10:100411. https://doi.org/10.1016/j.dajour.2024.100411.
60. Byeon H, Tammina MR, Soni M, Kuzieva N, Jindal L, Keshta I, et al. Enhancing online health consultations through fuzzy logic-integrated attribute-based encryption system. J Intell Fuzzy Syst. 2024;6:1–19. https://doi.org/10.3233/jifs-235893.

Publisher's Note