A Mobile/Tablet App-Based Patient Records Management System Using Blockchain

Deepesh Rago, Visham Ramsurrun(✉), Mrinal Sharma, Karel Veerabudren, and Amar Seeam

Middlesex University, Uniciti, Flic-en-Flac, Mauritius
DR661@live.mdx.ac.uk, {v.ramsurrun,m.sharma,k.veerabudren, a.seeam}@mdx.ac.mu

Abstract. As of 2022, the healthcare industry plays a crucial role in enhancing the quality of life as well as the overall well-being of individuals as it offers an extensive array of services across the globe. With the emergence of new technologies in the medical field, the healthcare universe is drastically evolving to provide better medical care, and such an example is the EHR systems. They changed the manner that patient medical health information is registered, stored, and shared. The traditional paper-based records systems have completely been replaced with its digital counterparts that offer superior benefits like better management of patients' medical records, raise in healthcare productivity, superior decision-making at managerial level and finally, a reduction in the overall healthcare expenditures. With the new EHR systems, patients can have access to their health records and take control over its management. However, the EHR systems are yet to be perfectionated and currently face numerous challenges like serious concerns related to data privacy, data interoperability, data ownership and date security, amongst others. Additionally, patient misidentification and misdiagnosis, are becoming a prevalent occurrence in medical care institutions that will have serious repercussions over patients' health or lives if this issue is not tackled at the earliest. Therefore, this project aims at developing the PatientCare Mauritius application. It is a mobile app-based patient records management system that makes use of blockchain technology with IPFS system to store and secure the patients' medical health records against cyber-attacks and other vulnerabilities as well as incorporating the NFC technology with patients' photo ID. The combination of NFC with photo ID contributes to accurately identifying patients at medical facilities to prevent patient misdiagnosis. To further uphold the acceptance and usability of the PatientCare Mauritius application, the Technology Acceptance Model (TAM) was adopted, and it made use of five constructs. The outcome was that the application obtained a TAM score of 4.33, implying that the PatientCare Mauritius application was valuable and user-friendly.

Keywords: EHR · Medical Health Records · Record Management · NFC · Blockchain · Ethereum · IPFS · Data Security · Smart Contract

A. Seeam et al. (Eds.): InterSol 2023, LNICST 541, pp. 113–130, 2024.
https://doi.org/10.1007/978-3-031-51849-2_8

1 Introduction

In the wake of the 2020 and ongoing outbreak of the COVID-19, the world has witnessed one of the most recent, disastrous pandemics which significantly affected all nations worldwide. Thereupon, mankind has unprecedented expectations from the healthcare industry to contain this disease which uncovered the underlying challenges currently present in this medical sector [1, 2]. One such shortcomings is the patient records management system presently in use in Mauritius. Indeed, most of the medical institutions are still making use of paper-based techniques to log patients' medical records that, inevitably, have considerable limitations. EHR is a key element in the medical industry [3–6]. This industry manages extremely sensitive information that ought to be handled very securely and EHR, too, is not an exception. EHR constitutes of private and confidential information about patients, such as, patients' identity, home address, contact details, health history and insurance details amongst others. This sensitive information is indispensable, not only for the patient but also for the medical institution as well as for the healthcare insurance firms. The medical and financial institutions, under any circumstances, cannot allow this crucial information to be leaked in the public, as it would enormously affect all the concerned parties.

1.1 Background

To have a robust and efficient healthcare system, it is mandatory that the past medical records of patients are promptly available and are accurate. Nonetheless, it is challenging and tedious to manage medical records over several hospitals [7]. Still, adopting a centralised solution for the storing of patients' medical data is not feasible as it leads to a single point of failure [8] and constitutes of various other constraints, namely, cyberattacks, as well as wrongful handling of medical data [9]. Other critical concerns are recurrently, medical staff wrongly identify and incorrectly link patients to their respective medical records that, eventually, lead to the patients being receiving the wrong treatment or medications. As a matter of fact, the Institute of Medicine has set forth that around 26%–32% of adult patients have incorrectly been administered medication, while the accounted number for paediatric convalescents is approximately between 4% to 60% [10, 11]. Therefore, the need to have a convenient electronic patients records management system, along with appropriately identifying the in-patients, is of paramount importance. The number of phishing attacks in the healthcare sector has recently been escalating because of the high demand of personal information in the black market. Indeed, at the 2011 Digital Health Congress, a group of experts stated that a simple EHR data in the black market was worth 50 USD as compared to 0.25 USD for a bank credit card details [12, 13].

Therefore, it is crucial to come up with unique and advanced technologies to tackle these challenges in the healthcare industry. Blockchain technologies have been acknowledged to address those issues whilst making the patient records management system, better known as the Electronic Health Record (EHR), more efficient and safer since blockchain is decentralised [14]. Blockchain can help in safeguarding and providing logs for electronic health records for medical lawsuits or insurance claims [15]. Additionally, the need to have a convenient electronic patients records management system, along with appropriately identifying the patients, is integral. Adopting the Near Field Communication (NFC) technology in the healthcare sector, will surely minimise these blunders whereby the patients will be bonded to an NFC tag upon their visit at the hospital. Doctors and nurses will have to scan these NFC tags before diagnosing and inputting patients' vitals readings respectively [10].

1.2 Aims and Objectives

Thus, this work intends at developing a mobile application, entitled as PatientCare Mauritius (PCM), for managing and securing patients' medical health records by incorporating blockchain and NFC technologies in electronic health record system. These technologies will enormously reduce the current limitations of the paper-based health record system and the existing EHR systems as well as any cyber-attacks targeted at the existing EHR systems. The application will secure patients' personal information along with their medical data. Patients will have ownership of their medical health data as they can control whether to grant access to doctors to view their medical health history records. The mobile application will make use of NFC sensor, embedded in the mobile or tablet, to allow medical personnel to accurately identify patients in the medical facility. Hence, ensuring that patients are getting the right treatment, while all the medical information are correctly logged for that patient respective electronic health record. The application will also allow the patients to directly book or manage their medical appointments with their doctors on their mobile phones itself, saving time and no need for paperwork.

2 Literature Review

In the contemporary healthcare industry, security of data and its ownership are two significant concerns that should be addressed at the earliest. As patients' medical records presently do not feature a proper and reliable data structure, it induces to data breaches and other cyber-attacks, which have a devastating impact on the patients, medical institutions, and other implicated organisations. According to the Department of Health and Human Services' Office for Civil Rights, in 2018, they have been informed of multiple data breaches whereby more than 13 million of medical records were compromised [15, 16].

Over the last few years, IT experts have constantly been looking for proper and viable systems to retain patients' medical records. Most of the contemporary EHR systems are cloud-based solutions whereby they are fully depended on reliable and centralised third-party entities that have no concerns with data security and data privacy. They only provide the basic protection to secure the data [17–19]. These cloud environments are vulnerable to single point of failure, among other drawbacks like data privacy issues when transmitting data over public networks. Centralised cloud-based systems have a high running cost as well as occupy more storage space as the systems scale up.

2.1 Electronic Health Record System

The healthcare institutions produce considerable volume of medical data daily. It consists of patients' diagnostic reports and radiology reports like MRI scans and X-ray amongst others. EHR is better described as the patients' digital compilation of their medical dossier, consisting of their health medical history, their past treatments, their personal information, their allergies, laboratory test results, medications amongst others. Typically, each health facility maintains his own EHR system and does not involve any kind of interoperability. Hence, a particular patient could be having different medical records at different medical facilities [20].

Medical institutions, normally, do not share their patients' medical records with other health facilities. These medical records are stored physically on servers at their respective data centres or, simply, to cloud-based storage systems. It requires many skills as well as planning when managing and maintaining such crucial medical data storage on premise. Typically, it involves high costs and proper facilities to ensure data redundancy, in the event of a system crash, malfunction or data loss amongst others. To avoid such system failures, numerous medical institutions seek refuge in cloud storage. However, these cloud-based systems, too, have their constraints. Recently, there had been some ransomware attacks along with Distributed Denial-of-Service (DDoS) attacks that brought down the centralised EHR systems across various healthcare institutions. These institutions were unable to operate and provide the required health service to their patients [20]. Centralised EHR systems are also vulnerable to other cyber-attacks that could cause further damage to both patients and the healthcare providers by leaking patient-sensitive information to the public. In the end, such malicious attacks lead to the fact that the concerned healthcare institutions have their reputation tarnished whereby their share value drop drastically in the stock market.

Therefore, adopting a decentralised EHR system will, notably, revolutionise the way medical institutions store patients' medical records, especially, regarding the security aspect. With the new decentralised approach, the totality of the constraints of the centralised systems is dealt with and will further be secured through Blockchain and Inter Planetary File System (IPFS).

Embracing a decentralised approach for the EHR systems will minimise the shortcomings of centralised EHR systems; for instance; the new system will support interoperability by allowing both patients and medical personnels to gain access to electronic medical records, without compromising data security and privacy. The system will prevent any wrongful use of data by ensuring that the data remains undisclosed. Implementing the blockchain technology in conjunction with IPFS system will bring down the above-mentioned deficiencies of the centralised EHR systems. IPFS is a decentralised system whereby data is stored and shared using a distributed approach, that will help in managing privacy and availability of medical data. Indeed, IPFS operates by breaking down the data that needs to be stored into numerous fragments that will eventually be dispersed over the whole distributed network. This technique of scattering data over the decentralised network is highly effective, for instance, in a situation where a hacker takes over control of a server in the network, the latter cannot interpret or leak data from the compromised server. Additionally, distributed systems offer other practical benefits, like minimum downtime in situations where a server is offline, while data can still be retrieved from other online servers in the network. This feature of decentralised system is a boon for the medical industry as we cannot allow any downtime when retrieving or accessing patients' medical records, especially, in emergency circumstances where time is a critical factor in rescuing patients' lives [20].

2.2 NFC Technology in Healthcare

Near Field Communication, better known as, NFC is derivative of the RFID technology and is, today, incorporated in most, if not all, smart devices (smartphones, tablets, smartwatches) in the 2022 era. The initial incentive of embedding NFC sensors in these smart devices was to allow rapid and effective transmission of data throughout mobile applications [10]. As NFC makes use of lightweight sensors, and are already embedded in smartphones and tablets, it swiftly succeeded over the RFID in the healthcare industry. It was convenient as there was no need to get specialised readers to read the NFC tags that were allocated to patients, through silicone bracelets. Thus, patients could easily and accurately be identified at the tap of the smart device and the NFC-based silicone bracelet through a mobile application [10].

Other application of the NFC technology in the healthcare varies from medication administration to precisely linked patients to their respective medical records, reports, laboratory tests, amongst others. Using NFC technology and a specialised mobile application, partially sighted patients could use their smartphones to tap on the NFC tag affixed on medication bottles caps that would read aloud the medication name, instructions, and dosage for their medication consumption. NFC technology can, undoubtedly, be effective in other medical applications whereby it can work alongside with other medical sensors to help medical staffs in their daily medical tasks.

By automating these data captures, it will help in optimising the time taken to carry out these tedious and repetitive tasks which will eventually enable the medical staffs to boost their efficiency and work productivity. The goal behind incorporating NFC technology with electronic health record is to radically improve the current healthcare industry by simplifying the capture, storage, and exchange of medical data among patients, health care workers and the management. Ultimately, these changes will relieve the operational costs and will boost the overall quality of medical service [10, 21].

2.3 Security in Healthcare

In the contemporary, IT systems and other advanced technologies work closely together to offer the best of healthcare facilities. Most of these systems are online and are always connected with one and another, to seamlessly transmit and store data in view of reducing time and costs. Nowadays, the EHRs involve high-end medical equipment along with smart devices like wearables, embedded sensors, and micro-chips. These devices allow to continuously monitor patients' health and trigger alarms in case of emergencies or abnormal vital signs readings.

With these advents in the healthcare sector, it is of paramount importance to ensure that these technologies and systems are secured and work accurately, because they involve patients' medical records that are highly sensitive data. The developing EHR systems are capable of handling numerous tasks, namely, managing the whole patients' medical records; from scheduling the medical appointments, the proper diagnosis of patients' ailments, prescribing drugs, to storing all these medical records for future use or references. Therefore, security is a must in healthcare because medical data stored in these EHR systems, need to be assured and protected from any cyber-attacks, for the proper running of the medical institutions [22, 23].

The volume of medical data generated by big data is enormous across various systems and generally, these data are complexed and rarely optimised. Since the medical records need to be accessible across the various networks of the medical institutions, it is often the case that the medical data gets duplicated. This leads to data being inaccurate, as upon changes made to medical data, are not effected to all locations where these data are stored. It can have severe repercussion as medical records need to be error-free for doctors to make the correct diagnosis of their patients. Duplication of data also result in wastage of storage space on the system. Having a weak data management of sensitive medical records will, eventually, induce cyber-attacks and other data breaches. Other security measures involve that, only authorised personnels should have access to patients' sensitive information. The former should only be limited to restricted views depending on their nature of their jobs.

2.4 Blockchain Technology in Healthcare

Blockchain technology has constantly been in the spotlight following the inception of Bitcoin by Nakamoto back in 2008 [24, 25]. Blockchain can best be described as a Peer-to-Peer, better known as P2P, network that constitutes of computing nodes that interact with one another [3, 26]. P2P network signifies that the network is a decentralised one; which is one of the fundamental characteristics of the blockchain technology. Other attributes of this technology are distributed database, and to ensure tone,all P2P transactions are verified. In blockchain, data that needs to be stored, is maintained in a block whereby the blocks are connected to other blocks which, eventually, develop into a chain, known as, the blockchain. As a rule, the blocks are bound to the previous ones through a hash value as well as with a timestamp, implying that once a transaction has been generated in blockchain, it cannot be changed [3, 26]. Blockchain assigns this timestamp feature because it associates an identity to all the workflow before circulating the copies amid each node in the network, to ensure that integrity of data is maintained between the endpoints, while there is no human intervention implicated [3, 27]. Therefore, a typical block incorporates the previous hash of the block, the hash of the current block, a nonce and finally a digital signature. The position and the sequence of the block is determined by the stored hash numbers [1, 25]. Furthermore, blockchain technology is greatly resilient to cyber-attacks because the hacker needs to take over control of all the blocks of the blockchain at the same time, as each block are interlinked through the block's hash pointer. Therefore, it is practically impossible for the hacker to own the entire blockchain.

Blockchain has the potentiality to revolutionise the healthcare industry through the enhancement of patients' records privacy, security of data and interoperability. It is viewed as an optimistic and viable solution in the medical world [24, 28]. Given the numerous features of blockchain technology, it could be utilised in various applications in the healthcare sector, for instance, to enhance the various health monitoring devices with their health mobile applications, the management of patients' medical records in terms of their storage and sharing, the insurance and clinical trials and the management of supply chain, amongst others [15]. Blockchain will make a significant impact on EHR as it will allow to efficiently store patients' medical information which was once dispersed over numerous healthcare providers. Blockchain will allow the patients to have full and secured access to view their medical data and be able to manage who can access their medical history. This ability will significantly empower the patients to have better control over their personal data, which, in turn, will boost both privacy and confidentiality [9, 29]. EHR involves highly sensitive information about patients and their health status that must be always readily available, especially during emergency situations. Hence, blockchain is ideal for storing this category of data because blockchain employs a peer-to-peer network that can serve as a redundant resource, upon failure of any component of the system or, any other deficiencies. Therefore, using blockchain technology will eliminate the risk of any single point of failure (SPOF) of the system [1]. Additionally, blockchain strongly advocates to be a tamper-resistant technology that promotes non-repudiation, as any data stored in the blockchain network, is immutable.

Limitation of Blockchain Technology in Healthcare. One major drawback of Blockchain technology is the cost of running the blockchain system. Every transaction that occurs on the blockchain, the end user is required to remunerate for this data processing whereby in Ethereum network, this remuneration is established in 'gas', pay out in 'Ether'. Ether, better known as ETH, is the native cryptocurrency of the Ethereum Blockchain and as of April 2023, its value is 1,877 USD [15]. Therefore, even though blockchain is efficient against tampering of records, it is not convenient for maintaining a significant amount of data [17, 30]. Considering the amount of data and transactions that would be generated daily for the medical sector, especially when dealing with imaging laboratory reports like X-ray, CT scan and MRI, the cost would be exorbitant. Hence, it is impractical to store the whole EHR data on the blockchain itself, as the latter is a high-priced storage medium. Also, the block size in blockchain is very restricted and adding-on for new blocks, too, is expensive. Consequently, the feasible approach to use blockchain technology is to use it to protect the EHR data, rather than a storage tool for the medical records [1].

Therefore, the desirable solution is to store these medical records in an off-chain storage. IPFS, Interplanetary file system, is deemed to be the most feasible system to safeguard and store these highly sensitive data. IPFS constitutes of a Peer-to-Peer (P2P) protocol and a distributed storage technique that intends to connect every computing machine to a single file system, whereby making it possible to store enormous amounts of medical records [3]. IPFS involves making use of a cryptographic hash which serve as a distinctive fingerprint, that is, a unique key for every data within the IPFS. Since IPFS prohibits the data's hashing value to be altered, IPFS is said to be an immutable and permanent storage platform. With IPFS, only the hash address of the patients' medical records will be kept in the blockchain network, rather than the actual records themselves [3, 31], which will further secure the data stored since blockchain, too, is a distributed network.

2.5 Existing Systems

MediQuick. MediQuick is a patient management android application that was developed by [32]. It makes use of blockchain and Quick Response (QR) code technologies to provide a secured and efficient platform for storing and accessing highly sensitive data like patients' medical records. Within the application, the patients have access to book medical appointments with doctors as well as to view their medical data and their medications [32]. All the patients who visit the hospital or use its medical services, are allocated with a unique QR code which firstly, allow the medical staff to accurately identify the patients to prevent any kind of misidentification and secondly, the codes allow both the patient and medical personnels to access the former's medical records from the hospital protected database. The hospital database is secured using the blockchain technology.

The MediQuick application was developed to eliminate the traditional patient records management system which was paper-based, and all entries were being done manually by medical staffs. Hence, the existing system had various limitations, exposed to security threats and was tedious as well as time consuming. Consequently, MediQuick will store all the patients' medical records digitally and secured same in a database using the blockchain technology, which will speed up most of the hospital services, increasing its productivity.

MediQuick application bears a strong resemblance to PatientCare Mauritius application, which is also a patient records management system that will utilise blockchain technology to secure its sensitive information, but PatientCare Mauritius differs in the sense that it adopts NFC technology instead of QR code because NFC is more secured as it involves an authentication procedure when configuring the NFC tags and also, NFC is quicker as communication is established through a quick and simple tap. Patients' medical records are extensive in size, directly storing this data on blockchain will not only impair performance when retrieving data, but also, is extremely costly to sustain. Hence, PatientCare Mauritius shall use an off-chain storage like IPFS, a distributed storage platform, to store all its medical records. IPFS hashes all these information whereby these hash keys are finally stored on blockchain. This procedure not only relieves the load on the blockchain, but also, provides an additional security measure for the sensitive data. The PatientCare Mauritius application will also incorporate the patient's photo in its NFC tag, as a means for medical staffs to accurately identify patients.

NFC Tag-Based mHealth Patient Healthcare Tracking System. To tackle the problem of misidentification and misdiagnosis of patients on hospital premises, [10] built a patient healthcare management information system that will incorporate NFC technology to provide a better healthcare service [10]. Patient misidentification and misdiagnosis have been prevailing for quite some time and have been recurrent worldwide due to various reasons, namely, poor patient management by medical staffs, hospitals overcrowded with patients during peak time or medical staffs using less efficient patient management systems. Therefore, adopting the NFC technology, along with photo ID, to accurately identify patients using NFC silicone bracelets that are issued to the patients upon the registration at the hospital, will greatly minimise this delicate situation. It is a must to properly identify patients at hospitals because they need to be correctly linked to their respective medical records, especially, when it concerns with medical health test reports as doctors refer to these test reports to provide the appropriate treatment to their patients.

Although PatientCare Mauritius and NFC tag based Mhealth application both use NFC technology with Photo ID, they differ in the way they store patients' medical health records. [10]'s system makes use of centralised MySQL database that are prone to various cyber-attacks, performance limitations as well as no redundancy in case of failure of the system. Meanwhile, concerning PatientCare Mauritius, which shall use a distributed and tamper-proof storage mechanism, in terms of blockchain technology and IPFS system, to store patients' medical records. The system will also be resilient against single point-of-failure attacks.

3 Design and Development

The study intents to build a modern EHR system that will facilitate both the healthcare provider to better store and manage patients' medical records as well as the patients to benefit from better medical care services. The methodology, proposed system and list of tools that will be used to develop the system are listed out.

3.1 Research Methodology

As this project intents at determining a solution to a real-life issue, the type of research to be accomplished shall be an applied research. Consequently, a prototype application system was implemented. This methodology was beneficial as it helped enormously in detection of design faults and other shortcomings that were fixed accordingly during early development of the system.

3.2 Proposed System

The aim is to build a system that will incorporate a mobile based application that will manage patients' medical health records and secured them using blockchain technology and IPFS storage system. It will also make use of NFC technology to readily identify patients on the hospital premises, to avoid misidentification of patients. During the registration process, the hospital admin will issue the patient with a silicone bracelet fitted with an NFC tag that contains a unique code to identify the patient. Then, the admin will capture a live picture of the patient that will be used as a 'Photo ID'. A link to this Photo ID is stored in the same NFC tag of the patient. Nurses and doctors will have to scan the patient's NFC bracelet first to confirm the latter's identity before proceeding to upload the latter's vitals readings to the mobile application and carry out patient's diagnostics respectively. The doctor can then update and save the patient's medical information on the application. The patients will have control over their medical data and control access to this sensitive data. They can also schedule medical appointments with doctors based on their availability as well as make call to emergency services like fire station, hospital, police station amongst others.

3.3 Tools and Technology

PatientCare Mauritius Mobile App. The mobile application was developed in Visual Studio (VS) Code using Dart Programming Language as Dart natively supports asynchronous programming that help to develop apps that are more responsive and efficient. Also, VS Code allow app development for multi-platform, and it has strong debugging capabilities (Fig. 1).

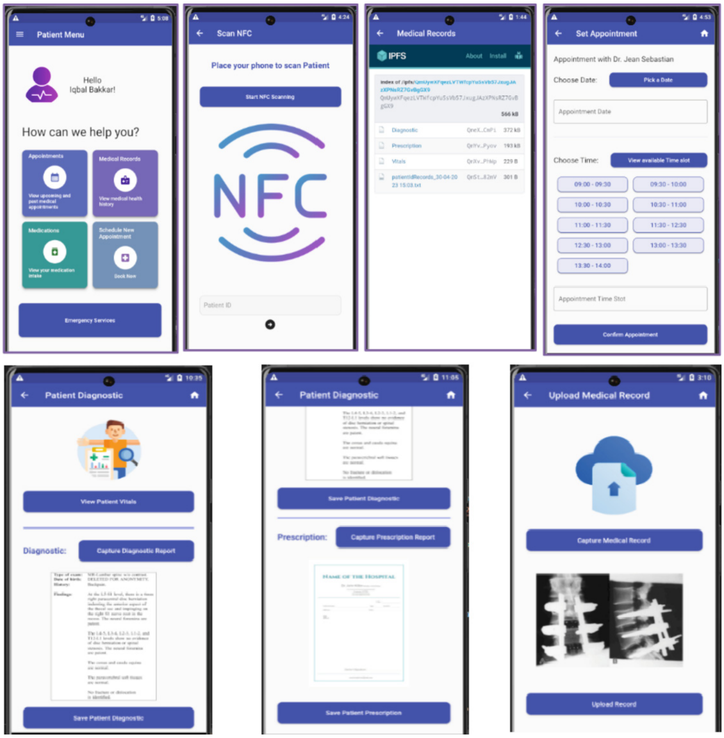

Fig. 1. PatientCare Mauritius application screens

Blockchain Network Technology. Ethereum blockchain is used for the PatientCare Mauritius as it is an open-source, decentralised and public blockchain platform that provides a P2P network that is capable of securely run and validate application code, better known as smart contracts, that enable participants of the blockchain to perform transactions altogether without the need of a trusted central authority. It allows to simulate a blockchain environment in a virtual manner without the need to implement a real one, which is costly. Ganache is used to create dummy or mock Ethereum accounts which are loaded with free of charge test Ether (ETH) cryptocurrency. This ETH which is a virtual currency, is utilised for the transactions to pay for the miner nodes. A Metamask cryptocurrency wallet is used to manage the spending and use of the Ether coin to pay for the transactions. For the users to be able to use this wallet, their accounts should be linked to the Metamask wallet with the private key of their Ethereum account. Remix IDE is used for the development, testing and deployment of the smart contracts on the Ethereum network. It is a lightweight IDE as well as it is ideal for the rapid testing and deployment of smart contracts. As we shall be using Solidity programming language to explicitly build the smart contracts, Remix will be hugely beneficial as it features a Solidity compiler.

NFC Technology, NFC Tag and its Application Model. NFC technology is chosen over Bluetooth one as NFC is simple and can readily communicate. A simple touch of the NFC reader to the NFC tag, is all what is required for communication to occur [10]. NFC consumes less power, and it is already incorporated in most of the modern smart devices, therefore, no need of additional NFC reading equipment. For the PatientCare Mauritius project, we shall be using the NFC chip, NTAG216, as it can store much data like patient's identity information and is future proof whereby we can store additional information, should the need arise in the future. As for the NFC Tag Application Model, we shall use the silicone NFC bracelets as it is more practical since the NFC chips are embedded in wearables, and it is more comfortable for the patients as they can adjust the bracelets according to their wrist size. The silicone bracelets are non-irritation and unscented as well as waterproof and will not be affected by sweat, water or other liquid that may get into contact with the bracelets [10]. The NFC silicone bracelet is as follows in Fig. 2.

Fig. 2. NFC Chip embedded in Silicone Bracelet

3.4 System Architectural Diagram

The PatientCare Mauritius system architectural diagram is represented in Fig. 3.

The PatientCare Mauritius is a two-tier architecture, consisting of a client (mobile application) and datastore. We make use of Firebase and IPFS as storage. The mobile application authenticates its users using firebase authentication and data is stored on the firebase storage. However, patients' medical data records are stored in IPFS which is a decentralised storage and is widely known to be used as an off-chain storage solution when dealing with colossal files. For the Ethereum network, Ganache is used which comes with predefined accounts of 100 ethers. To transfer these ethers to the mobile application, metamask wallet is used. Thus, ethers from the Ganache account are transferred to the metamask wallet. Smart contracts are written in Solidity programming

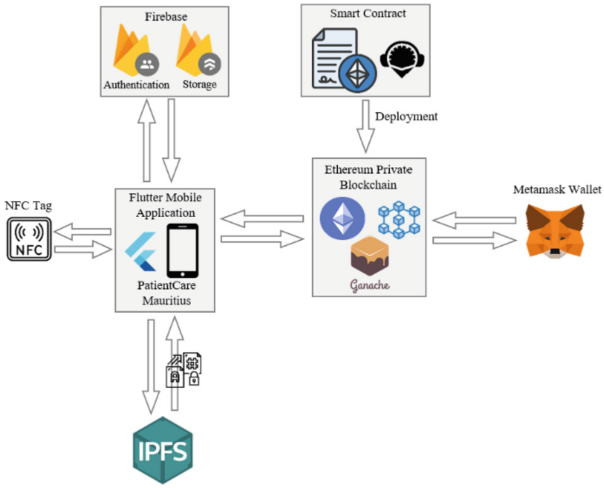

Fig. 3. PatientCare Mauritius System Architectural Diagram

language and deployed using Remix IDE. The flutter mobile application communicates with the Ethereum network such that whenever, a patient medical record is saved, the IPFS generates a CID hash, and that hash is saved on the blockchain. Therefore, whenever a patient wishes to retrieve his health medical records, the CID is retrieved from the blockchain and then passed to the IPFS URL gateway, and the file is retrieved.

4 Testing and Evaluation

To ensure that PatientCare Mauritius mobile application is indeed an efficient EHR system and is achieving all its intended objectives, various testing scenarios have been conducted. These testing varies from unit testing, integration testing, system testing, User Acceptance Testing (UAT) and Technology Acceptance Model (TAM).

With unit testing, the different functionalities of the system were tested independently of the other modules. The aim was to discover any shortcomings which may have occurred during the implementation of the new system. Integration testing was performed immediately after the unit testing of the different elements of the software, had been accomplished. These elements that were tested individually, now, needed to be put together to be tested as a whole component. Errors or any malfunctioning that went undetected in unit testing, were discovered in integration testing because the different components of the software behave differently when they work collectively. Following integration testing, system testing was carried out which main objective was to establish the new system reliability in various situations or surroundings, namely, accuracy tests or performance tests. We should determine whether the system produced the desired results under heavy load or factors affecting environmental conditions.

UAT and TAM are similar, and they were the most requisite type of testing when developing a new system because it required a real user to run and go through the new system. It was mandatory that this user did not have any implications or involvements in the creation of the new system, including from the early stages to the final implementation of the new system. The concept was that a real user who might or might not have a developer background, had more potential in identifying shortcomings or bugs of the new system, that the developer could have missed out. The user would go through the different functionalities of the app, and he was in a strong position to better assess the overall look and feel of the new system in terms of its user-interface. Also, he would be able to determine whether the application accomplished its purpose regarding its proposed requirements. To further confirm that the PatientCare Mauritius mobile application would be well adopted by end-users, the TAM was carried out as it is a prominent evaluation model and it would help to evaluate the level of user acceptability of the various features of the PatientCare Mauritius app. According to TAM, the factors that influenced an end-user to accept and use a technology are perceived usefulness (PU), perceived ease of use (PEOU), perceived convenience (PC), continuance intention to use (CIU) and attitude towards use (ATU). Therefore, these factors, also known as constructs, were listed in the TAM questionnaire to obtain a reliable technology acceptance level for the PatientCare Mauritius system. Other criteria of the TAM were that adequate number of participants, at least 45 participants, were required to participate in the testing of the system. They had various tasks to undertake which consisted of the different features of the mobile application like scanning patients' NFC bracelet, updating patients' vitals, requesting access to view patients' medical history, making diagnostics, scheduling, or cancelling medical appointments and calling the emergency services, amongst others. Those participants had to carry out these tasks and navigate through the application without any prior training on the system. The participants' interaction with the mobile app were captured for future analysis to determine the level of usability as well as to improve the application's user-interface if required. Afterwards, those participants had to fill in a predefined questionnaire consisting of the previously mentioned TAM constructs whereby these constructs were rated in a scale of '1' to '5'. '1' being Strongly Disagree and '5' being Strongly Agree. The participants could also make suggestions on the different sections of the questionnaire. Finally, following the completion of the data capture, a final check was done to ensure no data were unreliable or incoherent, and statistical analysis was carried out to finalise the testing and evaluation process (Table 1).

Table 1. TAM Constructs Definitions

TAM Constructs	Definition
Perceived Usefulness (PU)	It describes the extent a technology will contribute to facilitating a task
Perceived Ease of Use (PEOU)	It describes the point where end-users will feel that the technology is easy to use
Perceived Convenience (PC)	It describes the amount of convenience that the users will feel when executing an action of the technology
Continuance Intention to Use (CIU)	It describes how eager the users are to continue to use the new technology
Attitude Towards Use (ATU)	It describes the users' attitude towards using the technology in the near future

5 Results

Out of the 50 participants who agreed to go through that study, 20 were males and 30 were females. Their age group varied from 22 years old to 58 years old. The participants were all computer literate and familiar to use smartphones in their everyday life. Also, all the participants had a thorough medical knowledge.

Table 2. Results of the TAM Constructs

	Score					Avg. Score	Avg. Construct Score
Constructs	1	2	3	4	5		
PC1: PCM is similar to other existing mobile apps	0	0.02	0.1	0.68	0.2	4.06	4.3
PC2: Using PCM is engrossing	0	0	0.08	0.4	0.52	4.44	
PC3: Using PCM suits my occupation	0.04	0.04	0.14	0.3	0.48	4.14	
PC4: Using PCM is useful and diminish patient misdiagnosis	0	0	0.06	0.32	0.62	4.56	
PEOU1: Learning to use PCM was straightforward	0.02	0.04	0.12	0.36	0.46	4.2	4.23
PEOU2: Learning to operate PCM would be straightforward	0	0.02	0.06	0.5	0.42	4.32	
PEOU3: I think interacting with the PCM would be unambiguous	0	0.02	0.16	0.44	0.38	4.18	
PEOU4: I think going through where I want in PCM, would be easy	0.02	0.02	0.1	0.44	0.42	4.22	
PU1: With PCM, it would facilitate patient identification	0	0	0.06	0.5	0.44	4.38	4.26
PU2: With PCM, it would diminish patient misdiagnosis	0	0.02	0.08	0.48	0.42	4.3	
PU3: PCM would improve my efficacy on my job	0.02	0.06	0.06	0.4	0.46	4.22	
PU4: Using PCM is highly beneficial for my profession	0.02	0.02	0.1	0.48	0.38	4.18	
PU5: With PCM, I can better focus on other critical areas of my profession	0	0.04	0.14	0.4	0.42	4.2	

(*continued*)

Table 2. (*continued*)

Constructs	Score 1	2	3	4	5	Avg. Score	Avg. Construct Score
ATU1: PCM has a positive effect for me	0	0.02	0.06	0.46	0.46	4.36	4.43
ATU2: The development of PCM was an excellent initiative	0	0	0.12	0.4	0.48	4.36	
ATU3: PCM greatly reduces patient misidentification and misdiagnosis	0	0.04	0.04	0.3	0.62	4.5	
ATU4: I expect that PCM to be readily available at my workplace	0	0.02	0.02	0.4	0.56	4.5	
CIU1: Should I be granted access to PCM, I would be using it	0	0.02	0.04	0.46	0.48	4.4	4.45
CIU2: I would definitely be using PCM	0	0.02	0.04	0.46	0.48	4.4	
CIU3: I would like to have further understanding about EHR, Blockchain and NFC Technologies	0	0.02	0.02	0.36	0.6	4.54	
TAM AVERAGE SCORE							**4.33**

Following the overall TAM score of **4.33** as illustrated in Table 2, it can be deduced that implementing the PatientCare Mauritius system in real life, will definitely contribute to assisting medical care personnels as well as facilitating their daily tasks. It will also yield better productivity of the staffs. As the PCM system is convenient to use, it was well appreciated by the participants as the average score for PC was 4.3. Having a PEOU score of 4.23, signify that the overall user interface and UX of the application were well built and participants had no serious issues in going through the application. With the PU average score being 4.26, it implies that most of the participants found the new system to be effective and would help in improving their work. However, in the future, the system can further be improved as well as implementing new functionalities to better facilitate the medical staffs' daily tasks and improving the overall medical services of the healthcare institutions.

6 Conclusion and Future Works

In this paper, the traditional paper-based patient records system was critically contrasted to the EHR which is viewed as a viable system for the management of patient records. Yet, EHR systems are subjected to other significant challenges pertaining to data security, data privacy and data interoperability. As a patient records management system involves highly sensitive data, it is obligatory to defend the system through all possible ways. Also, common patient records management systems do not involve a special technological mechanism to accurately identify patients in hospital premises which may lead to wrongful diagnosis and treatment of the patients.

PatientCare Mauritius mobile application has successfully solved these shortcomings using Ethereum blockchain technology with IPFS system. Incorporating the blockchain technology in PatientCare Mauritius app, guarantees that patients' sensitive records are secured, immutable, tamper-proof, and resistant to cyber-attacks, while the mobile application itself, enables both the patients and medical staff members to access and share medical information in real-time. Moreover, since PatientCare Mauritius is a blockchain-based patient records management system, it eliminates Single Point of Failure in the EHR system, and it improves patient privacy as the latter is in total control of his medical health records. PatientCare Mauritius app also makes use of NFC technology with Photo ID feature to precisely identify patients throughout their entire visit at the hospital which contribute to patient safety, diminish medical errors, and boost the overall efficiency and productivity in healthcare delivery.

Finally, in view to ensure that the PatientCare Mauritius mobile application truly succeeded in achieving all its objectives, and is fully operational, various kinds of tests were carried out, namely, unit testing, system testing, user acceptance testing (UAT) and Technology Acceptance Model (TAM). Therefore, it can be deduced that the PatientCare Mauritius has been well developed and it is a promising tool that will surely contribute to enhancing healthcare services.

Nonetheless, the PatientCare Mauritius application can be improved by integrating an electronic prescription functionality that will allow the patients to instantly view their list of medication as well as their doses. Based upon the time interval set by doctors, it will automatically remind patients when it is due time to consume these medications. Also, smart medical sensors or wearables can be used to automatically read patients' vitals and upload same directly onto the mobile application, without any human intervention. This will allow the nurse personnels to carry out other crucial tasks as well as to increase hospital productivity. Additionally, the NFC-based bracelets can be used for other purposes, rather than patient identification. For instance, using the NFC bracelets to track patients' whereabouts as they move from one department to another.

References

1. Tan, T.L., Salam, I., Singh, M.: Blockchain-based healthcare management system with two-side verifiability. PLOS ONE **17**(4) (2022). https://doi.org/10.1371/journal.pone.0266916
2. Herper, M.: The coronavirus exposes our health care system's weaknesses. We can be stronger (2020). https://www.statnews.com/2020/03/02/the-coronavirus-exposes-our-health-care-systems-weaknesses-we-can-be-stronger/
3. Sabu, S., Ramalingam, H.M., Vishaka, M., Swapna, H.R., Hegde, S.: Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. Glob. Trans. Proc. **2**, 429–433 (2021)
4. Reen, G.S., Mohandas, M., Venkatesan, S.: Decentralized patient centric e-health record management system using blockchain and IPFS. In: 2019 IEEE Conference on Information and Communication Technology (2019). https://doi.org/10.1109/CICT48419.2019.9066212
5. Le., T.G., Wang, J.W., Le, D.H., Wang, C-C., Nguyen, T.N.: Fingerprint enhancement based on tensor of wavelet subbands for classification. IEEE Access **8**, 6602–6615 (2020). https://doi.org/10.1109/ACCESS.2020.2964035

6. Shivappriya, S.N., Karthikeyan, S., Prabu, S., Pérez de Prado, R.P., Parameshachari, B.D.: A modified ABC-SQP-based combined approach for the optimization of a parallel hybrid electric vehicle. Energies **13**(17), 4529 (2020). https://doi.org/10.3390/en13174529
7. Sethia., D., Gupta., D., Saran, H.: Smart health record management with secure NFC-enabled mobile devices. Smart Health **13**, 100063 (2019). https://doi.org/10.1016/j.smhl.2018.11.001
8. Chouhan, A.S., Qaseem, M.S., Basheer, Q.M.A., Mehdia, M.A.: Blockchain based EHR system architecture and the need of blockchain inhealthcare. Mater. Today Proc. **80**, 2064–2070 (2023).https://doi.org/10.1016/j.matpr.2021.06.114
9. Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S.: Blockchain technology applications in healthcare: an overview. Int. J. Intell. Netw. **2**, 130–139 (2021). https://doi.org/10.1016/j.ijin.2021.09.005
10. Ebere., O., et al.: NFC tag-based mHealth Patient Healthcare Tracking System. IEEE (2022)
11. Koppel, R., Wetterneck, T., Telles, J.L., Karsh. B.T.: Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety. J. Am. Med. Inform. Assoc. **15**(4), 408–23 (2008). https://doi.org/10.1197/jamia.M2616
12. Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M.H., Kerrache, C.A.: The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain Res. Appl. **2**(1) (2021). https://doi.org/10.1016/j.bcra.2021.100012
13. Adefala, L.: Healthcare experiences twice the number of cyber attacks as other industries. IDG Communications, Inc. (2018). https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html
14. Huang, G.J., Foysal, A.A.: Blockchain in healthcare. Technol. Invest. **12**, 168–181 (2021). https://doi.org/10.4236/ti.2021.123010
15. Chen, H.S., Jarrell, J.T., Carpenter, K.A., Cohen, D.S., Huang, X.: Blockchain in healthcare: a patient-centered model. Biomed. J. Sci. Tech. Res. **20**(3), 15017–15022 (2019)
16. HIPAA Journal (2018) Largest Healthcare Data Breaches of 2018. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/
17. Costa, T.B.D.S., Shinoda, L., Moreno, R.A., Krieger, J.E., Gutierrez, M., Coração, I.D.: Blockchain-based architecture design for personal health record: development and usability study. J. Med. Internet Res. JMIR Publications Inc., Toronto, Canada (2022). https://www.jmir.org/2022/4/e35013. Accessed 17 Feb 2023
18. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J. Med. Syst. **42**, 140 (2018). https://doi.org/10.1007/s10916-018-0995-5
19. Cao, S., Zhang, G., Liu, P., Zhang, X., Neri, F.: Cloud-assisted secure ehealth systems for tamper-proofing EHR via blockchain. Inf. Sci. **485** (2019). https://doi.org/10.1016/j.ins.2019.02.038
20. Khadse, D.B., Nikam, U., Mate, N.: DAPP to store electronic medical health records on ethereum blockchain and IPFS. Int. J. Adv. Res. Sci. Commun. Technol. (IJARSCT) **2**(2), 732–741 (2022)
21. Devendran, A., Bhuvaneswari, T.: Mobile healthcare -proposed NFC architecture. Int. J. Sci. Res. Publ. **2**(1), 1–3 (2012)
22. Godwin, P.C.: Design and Development of a Custom Blockchain-based Health Record System As an efficient management and tracking solution. Thesis (Masters), MiddleSex University London (2021)
23. Hathaliya, J., Tanwar, S., Tyagi, S., Kumar, N.: Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. Comput. Electr. Eng. **76** (2019). https://doi.org/10.1016/j.compeleceng.2019.04.017
24. Meier., P., Beinke., J.H., Fitte., C., Brinke, J.S., Teuteberg., F.: Generating design knowledge for blockchain-based access control to personal health records. Inf. Syst. e-Bus.

Manag. Springer (2021). https://ideas.repec.org/a/spr/infsem/v19y2021i1d10.1007_s10257-020-00476-2.html
25. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at (2009). https://metzdowd.com
26. Khan, F., Asif, M., Ahmad, A., Alharbi, M., Aljuaid, H.: Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustain. Cities Soc. **55**, 102018 (2020). https://doi.org/10.1016/j.scs.2020.102018
27. Onik, M.M.H., Aich, S., Yang, J., Kim, C.S. and Kim, H.C.: Chapter 8 - Blockchain in healthcare: challenges and Solutions. Advances in ubiquitous sensing applications for healthcare. Big Data Analytics for Intelligent Healthcare Management, pp. 197–226. Academic Press (2019)
28. Mettler, M.: Blockchain technology in healthcare: the revolution starts here, pp. 1–3 (2016). https://doi.org/10.1109/HealthCom.2016.7749510
29. Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., Ylianttila, M.: Blockchain Utilization in Healthcare: Key Requirements and Challenges (2018). https://doi.org/10.1109/HealthCom.2018.8531136
30. BigchainDB 2.0 the blockchain database (no date). https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf. Accessed 22 Jan 2023
31. Kumar, R., Marchang, N., Tripathi, R.: Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In: 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 1–5 (2020). https://doi.org/10.1109/COMSNETS48256.2020.9027313
32. Solidity. (2021). https://docs.soliditylang.org/en/v0.8.15/