IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 18, 2022, accepted March 16, 2022, date of publication March 25, 2022, date of current version April 21, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162218

A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain

AHMED G. ALZAHRANI[1,2], AHMED ALHOMOUD[3], AND GARY WILLS[2]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.
[3]Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

Corresponding author: Ahmed G. Alzahrani (a.g.m.alzahrani@soton.ac.uk)

This work was supported by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia.

ABSTRACT The healthcare sector is suffering from inefficiencies in handling its data. Many patients and healthcare organisations are frustrated by the numerous hurdles to obtaining current, real-time patient information. Patients are also frustrated at trying to schedule appointments at health organisations that have outdated contact information. The healthcare sector's attention has been drawn to blockchain technology as a part of the solution, especially since this technology has been successfully applied in the financial sector to improve the security of transactions. The aspect of interoperability is resolved adequately by blockchain technology, because it has the potential to store, manage and share EMRs safely in the healthcare community. Therefore, the technology is having a positive impact on healthcare outcomes for various stakeholders. Interoperability in healthcare eases the exchange of health-related data, such as EMRs, between healthcare entities so that records may be shared and distributed among clinical systems. To handle data in this sector without violating privacy is a challenge, whether in the collection, storage, or analysis. Poor security, which increases data breaches, endangers patients both mentally, socially, and financially. A lack of data-sharing in the healthcare sector is considered a significant issue worldwide. This research focuses on this gap by investigating the benefits of using blockchain at the Ministry of Health in Saudi Arabia, providing a detailed analysis of the healthcare sector, and evaluating how blockchain technology improves data-sharing security. This research proposes a framework that identifies the factors supporting data-sharing using blockchain among healthcare organisations. It has three categories: healthcare systems factors; security factors; and blockchain factors. A triangulation technique achieved reliable results in three steps: a literature review; an expert review; and a questionnaire. This gave a comprehensive picture of the research topic, validating and confirming the results. To construct the framework, factors were comprehensively extracted from the literature then analysed, cleared of duplicates, and categorised. As a result, the final framework is confirmed as being based on the literature and expert review, and it is supported by the practitioners' survey.

INDEX TERMS Blockchain, healthcare systems, sharing data, privacy, security, Saudi Arabia.

I. INTRODUCTION

Advances in Health Information Technology (HIT) have improved the delivery of healthcare services to consumers, as well as creating products and services previously unavailable in the healthcare sector. As such, HIT is increasingly seen as one of the most promising ways in which to improve the operation of healthcare, including patient safety, records management, the efficiency of delivery, and the overall quality of treatments. HIT cuts the paperwork, extends real-time communication, and improves healthcare quality [7]–[9].

Blockchain technology has been successfully adopted to improve the security of transactions in financial services, particularly those involving digital currencies. The same concepts can be borrowed by the healthcare sector to improve security in how health records and patient information are stored, retrieved, and shared. Many studies in the sector have evaluated the potential of blockchain technology [10], [11].

This research provides an analysis of the healthcare sector with a particular focus on the Kingdom of Saudi Arabia (KSA). It reviews the health systems currently in place

The associate editor coordinating the review of this manuscript and approving it for publication was Claudio Agostino Ardagna.

and KSA's culture as it relates to the adoption of technology and the potential of blockchain technology in this sector. This study aims to identify and understand the factors that support data-sharing using blockchain among healthcare organisations.

II. BACKGROUND

This section reviews healthcare information systems and blockchain, and discusses the KSA context.

A. HEALTHCARE SYSTEMS

New kinds of HIT provide an avenue along which the health sector can continue growing and improving, while maintaining quality through minimising the cost of accessing healthcare and enhancing patients' experience of healthcare facilities [12]. Healthcare is an intensive domain of data and a huge amount is accessed, created, and stored on a daily basis [8]. Technology can play an important role in boosting the quality of patients' treatment and reducing the cost of deploying resources such as practitioners and equipment [8]. There are various kinds of HIT to achieve these objectives, and the ultimate focus is on improving patients' outcomes and enhancing their experience of healthcare facilities [1]. Among the key issues and concepts for consideration in HIT are the following.

B. ELECTRONIC MEDICAL RECORDS

Since they play an important role in enhancing quality and patient experience while reducing costs, several systems have been considered or actually applied by clinics. Among them is Electronic Medical Records (EMRs), collections of digital records containing vital medical information on individuals such as their health history, for instance previous diagnoses, medicines, tests, allergies, immunisations, and treatment plans. EMRs are the computerised digitised equivalent of the manual paper records kept by healthcare organisations and institutions, and are used by health professionals in patient diagnosis and treatment [13].

Existing EMR-sharing technologies involve two main challenges. While they are good at sharing data, they negatively affect the level of control over those data [5]. This predisposes the data to various privacy issues that, should the data be released to a third party, compromise customers' trust. Poor data-control measures raise serious privacy and security issues in data-sharing [6], [14], costing patients both privacy and money. For instance, if they visit another health organisation they may need to repeat an earlier test due to its results being missing from their records.

C. GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a European Union law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA) [15]. It stipulates that a user has the right to request complete erasure of their data. Thus, it prohibits processing special-category data unless the affected parties have given their explicit consent or when specific conditions have been met [15].

D. PRIVACY IN HEALTHCARE SYSTEMS

Without a highly secure infrastructure, interaction among medical systems might heighten the risks to health information and leakages stemming from the electronic transmission of data, with serious legal and financial consequences [16].

Records involve major security requirements, such as non-repudiation, access control and authentication, and those associated with medical information and healthcare, such as confidentiality, integrity, and the availability of medical data [17]–[22]. Additional role-based privileges and security are necessary to protect the information and secure the records, since the information is being transferred from paper to a digital format. Because the medical records are to be stored on a database, access should be limited to authorised individuals, and this needs to be monitored and enforced. To decrease the risk of medical records being tampered with or copied it is vital to perform audits and strict access control [23].

In general, both special-category data and personal data are vulnerable to attack and misuse, meaning that they should not be trusted to intermediaries [24].

Privacy is a highly important feature in the analysis of personal data. Sensitive data storage facilities, such as medical and healthcare databases, are considered a valuable source of data for personalising services and conducting clinical research and statistical analyses [25]. Nevertheless, any leaks of their personal private information will be seen as inadmissible by the original owners of the data [26]. A possible solution that is currently employed to protect information privacy may lie in rendering it anonymous [27].

E. DATA-SHARING

Currently, centralised data-sharing struggles to fulfil the healthcare sector's requirements of accessibility, scalability, and security [10]. To enable patients to make efficient collaborative treatment and care decisions, it is essential to achieve scalable and secure data-sharing [2], [3], [4]. Patients visit multiple clinical institutions during their life, and healthcare organisations need to keep patients' conditions and data updated by exchanging such information in a timely and private manner [28]. Data related to patients' treatment and diagnosis or EMRs are considered critical, because they contain private and sensitive information [12]. It is evident that health data are managed mainly by the separate clinical institutions, each with its own strict regulations and policies on transferring such critical information. Therefore, data are scattered across institutions and the resulting lack of standardisation means low interoperability [29].

F. HEALTHCARE SYSTEMS IN THE KSA

The Government of Saudi Arabia is heavily involved in the provision of public health services. For example, the country's Ministry of Health (MoH) provides approximately 60% of all healthcare services for citizens. These comprise approximately 244 hospitals (33,277 beds), which the MoH directly controls and manages [30]. Non-profit government

institutions, such as referral hospitals and National Guard Health Affairs, and the private sector make up the remaining 40% [31]. The adoption of EMR systems in KSA's hospitals is currently poorly known; furthermore, its determinants are also as yet poorly known. Unlike countries in the West, Saudi Arabia has no data protection laws [31], and the anti-cyber crime law that was issued and approved in 2007 is considered to be general and unclear [32].

G. HEALTHCARE SYSTEM CHALLENGES IN THE KSA

In the KSA, medical information is one of the assets most targeted by hackers, even more so than personal data. A recent survey conducted by [33] found that a significant majority of consumers, 75%, had personally encountered a breach of their medical data, whereas only 32% claimed that this had happened to their personal information. This shows that breaches in Saudi Arabia are nearly three times more prevalent (35%) than that of other countries that were surveyed. The study found that such breaches typically arose in hospitals (43%), doctors' practices (25%), and pharmacies (24%).

Europe and North America have laws in place to ensure that personal data are secured and protected, yet Saudi Arabia has neither a law on data protection, nor guidelines on what to do in the event of a data security violation.

H. DATA-SHARING IN THE KSA

KSA's MoH regards improving healthcare delivery through embracing new technologies as a priority; however, the technological systems adopted in the past few years have been mainly administrative rather than patient-centred. It is projected that patient-focused technologies will improve the quality of care by minimising medication errors, reducing the cost of accessing healthcare, and improving overall organisational efficiency [34]. One of the most significant challenges in Saudi Arabia is managing patient records. Most KSA hospitals and health facilities find it difficult to update patient records regularly. Recent studies indicate that only 16% of hospitals have implemented EMR [35]. Most public hospitals still rely on paper-based systems to manage patient records, and the evidence suggests that their adoption of technology is quite rare [36].

Blockchain technology offers a secure environment for storage, access, and retrieval of data in hospitals and other healthcare facilities. Furthermore, it has numerous other advantages that make it easier to manage health records. Its features of decentralisation, encryption, interoperability, and immunity render systems more secure than KSA's existing health technologies [11]. In one scenario, a record is created and the data stored either on blockchain or off chain whenever a patient visits a hospital. For security purposes the data undergo asymmetric encryption and, in this scenario, the blockchain generates a uniform resource identifier to point to the off-chain storage of the related fine-grained medical dataset. In addition, to assure the data's integrity, a hashing summary of the actual clinical data is uploaded to the blockchain. For auditing purposes, at the same time it records the sharing list; that is, the list of those approved to access the data. Furthermore, as a countermeasure to the scalability issue, the encrypted clinical data may be stored off-chain and blockchain used only to store condensed information on how the data are to be accessed [8], [14], [37].

Public Key Infrastructure (PKI) methods enable asymmetric encryption to guarantee that medical data continue to be accessible only by authorised participants [38].

I. BLOCKCHAIN

Würst and Gervais, with their model, illustrate that blockchain may be used where multiple institutions need to communicate and exchange data yet neither trust each other nor want to involve a trusted third party (TTP) [39]. Blockchain may be described as a database that is immutable and shared among peers in a network, and where records of transactions or events are appended in chronological order [40].

The technology of blockchain is regarded as an efficient tool to enhance the verification of the identity and integrity of data, providing users with consistent and trustworthy data in the cloud environment [41]. In addition, it is a robust instrument that boosts governments' performance with resource information. This peer-to-peer (P2P) decentralised data-sharing system increases the efficiency of sharing and cuts the costs relating to data [42].

With the rapid development of Information and Communication Technology [43], attention to privacy issues is increasing. For instance, there is much interest in the personal privacy of medical information and monetary data, which must be kept from major losses [44].

With no third-party intervention required, blockchain offers low-cost data exchange with a monitored, trusted contract. It facilitates engagement, smart contracts, and agreements, at the same time making cyber security more robust [45]. Blockchain may be defined as timestamped blocks that can be chained together using hashing cryptography. These blocks are sealed in an immutable and secure manner [46], [47]. The chain constantly grows by appending new blocks to the end, each holding a reference to the content of the previous [48].

J. SECURITY IN BLOCKCHAIN

The technological environment continues to develop under constant threats to information security (IS) from hackers, viruses, criminals, and terrorists [49]. Blockchain technology has the potential to help the healthcare sector to overcome its challenges over data security, sharing, privacy, and storage [50]. One of the sector's most important requirements is interoperability, or the ability of multiple parties, machine or human, to exchange information or data consistently and efficiently [51]–[54].

The blockchain infrastructure ensures that data stored on the network are immutable and have an auditable history. This concept is vital in healthcare, because it preserves the integrity of patient data through ensuring that no other agency can access and alter them. All transactions involving the

specific set of data are traceable, facilitating the audit of transition processes on the network [55].

K. BLOCKCHAIN IN THE KSA

Blockchain is considered an emerging technology and, as far as we know, has not yet been adopted or applied in the KSA. Our search for blockchain usage in KSA found only a single result, a study that discusses value-added tax (VAT) in finance. In it the author proposes a system for VAT transactions with a transparent database, deducting the tax and storing it on a peer-to-peer network [56]; the solution has not yet been implemented in the real world.

III. HOW BLOCKCHAIN CAN ADDRESS A HEALTH SYSTEM'S CHALLENGES

To address the challenges of a health system using blockchain, first needed is an immutable and auditable history, as well as traceability, because the permissions required to access patient data shift from one actor to another on a regular basis.

Second, the use of a centralised institution, where a single entity is in control, increases the security risk and cost of trust [55]. Existing systems that depend on a single authority to store encrypted data are vulnerable, as hackers can concentrate their efforts on a single target to perpetrate Denial of Service (DoS) attacks, inject malicious data, or undertake extortion through theft or blackmail. The management of medical data in a safe and accurate way leads to good digital health [57]. Government entities can offer better healthcare services by properly maintaining patients' medical records, which can then be shared with other service organisations [58].

There are further advantages to implementing blockchain technology in healthcare institutions. One is the management of patients' EMRs. Currently, patient data are stored securely yet in multiple places, scattered across organisations, clinics, and insurance providers, so there is no full access to a shared database of patients [59].

Further benefits of applying blockchain technology in healthcare institutions are its immutability and verifiability for transactions; transparency; tamper-proofing; and the integrity of distributed sensitive health information. Basically, these can be achieved by using consensus protocol and cryptographic mechanisms such as digital signatures and hashing [60].

Blockchains are decentralised, meaning that they need the authority or trust of neither the individuals in the network, nor the group. The reason that the system does not require trust is that each node has a complete copy of all the available historic information; just by achieving majority consensus, more data are added to the chain of prior information. In this way, blockchain has the advantage over current security measures [61].

Blockchain methodology addresses many issues confronting current health IT models, including security, especially data integrity and privacy, and immutability, which assures identities thus creates a robust audit trail and subsequently improves healthcare-related security for both patients and organisations [62].

It is anticipated that blockchain technology will benefit patients who interact with healthcare systems, in that they can avoid routine registration processes and shorten their waiting time. Moreover, providing immutable and transparent personalised medical records that can be accessed anywhere (universal EMR) will decrease paperwork, costs, and overheads [63]. The potential of blockchain technology is to modify healthcare delivery, placing the patient at the centre of the healthcare ecosystem and making improvements in the security, interoperability, and privacy of medical data [63]. Finally, the research gap has been identified.

IV. RELATED WORK

This section critically reviews related works on healthcare systems that are based on blockchain.

Gem Health Network (GHN), based on blockchain technology, allows health providers to share health information and data. It was developed from Ethereum blockchain technology to create a secure infrastructure in which there is a shared ledger system where new transactions and records are maintained, thus removing the challenges arising from centralised storage. This system gives patients significant control over their data while allowing health providers access to all relevant information in real time [64].

In 2011, a collaboration between Guardtime and the country of Estonia used blockchain technology to set up a healthcare platform that now secures millions of records [65]. It shows that operating a complete public health infrastructure using blockchain technology is achievable [64]. In this system the patients both own and control the access to their healthcare data [66].

MedRec is a blockchain-based decentralised record management system to handle HER. It was designed to manage issues such as authentication, confidentiality, accountability, and data-sharing in managing healthcare records and patient data. The technology creates an immutable log of all transactions involving a patient's information, and is provided to the patient [67]. The MedRec system does not store patients' actual health records: it uses blockchain technology to store each record's signature. The signature provides assurance that each record's unaltered copy is obtained [67], [68].

Medshare was introduced by [69] to address the issues of sharing medical data. This system is built on blockchain technology, which is secure and safe for health data exchange between untrusted entities. The design uses smart contracts and a control mechanism to track data behaviour in an effective manner and repeal access to any entity upon detecting it violating its permissions. Healthbank offers users a platform to store and manage their medical information in a secure environment and, with financial compensation, to make it available for medical research. By using blockchain technology for transaction validation and verification, this company is working on empowering patients to have full control over their data.

Ancile is a framework built on Etherum blockchain, and it uses smart contracts for EHR management to give patients both ownership of and control over their EMRs. It securely controls access to documents and tracks how records are used, transfers records in a secure way, and restricts unauthorised parties' ability to obtain PHI. Another permissioned blockchain framework proposed by [60] is for sharing and managing cancer patients' medical records. To authenticate registered users the design employs a membership service with a username/password scheme. Each patient's identity is created from a combination of personal information, encrypted for security, including names, date of birth, social security number, and zip code. For medical data, a secure cloud server is used to upload information, with access managed by the logic of blockchain.

V. PROPOSED FRAMEWORK

The healthcare sector is significant because it uses special-category information (as explained later), which can have a direct effect on patients' lives. Using technology may improve patient outcomes, yet it raises challenges over security, patient privacy, and healthcare data exchange. The last challenge needs a solution that gives access to updated healthcare information and allows physicians and other healthcare professionals to make decisions quickly when emergencies arise, with ease of access to quality data in a secure information system.

The purpose of this study is to propose a framework to identify the factors found to support data-sharing using blockchain among healthcare organisations. As far as we know no previous studies in Saudi Arabia have attempted to solve this issue. The conjecture is that blockchain can be part of the solution for secure information sharing in KSA.

The following framework is based on a literature review, as elaborated in a previous research paper [70], and consists of the three main categories depicted in the first version of the Sharing Data between Healthcare Providers Framework (SDHPF) (Figure: Data-Sharing between Healthcare Organisations Framework V.1) [70].

A. FACTORS RELATING TO HEALTHCARE SYSTEMS

This category includes factors relating to healthcare systems to describe how the systems work and are accepted on the basis of decentralisation, cost, efficiency, risk policy, and ease of use.

Decentralisation: enables a distributed environment between nodes, so that the data can be recorded, stored, and updated without reliance on a central authority [13], [40], [65], [71]–[74].

Cost: through moving records between entities and reducing administrative costs by eliminating any third party, blockchain can reduce the costs that arise in current systems [13], [50], [63], [65], [71].

Efficiency: because these factors might delay a patient's treatment and increase its cost, the need to repeat a test through non-availability of data could present a risk to health. Moreover, sending data in traditional ways such as email

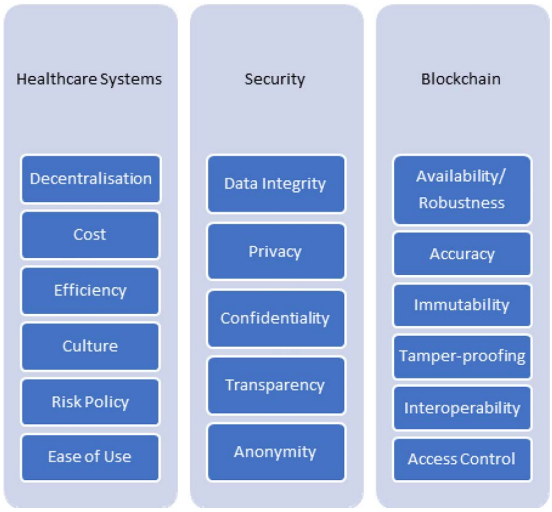

FIGURE 1. Framework V.1.

presents a security risk, unlike blockchain. Blockchain has great potential to reduce cost and perform repetitive registrations while improving treatment outcomes [50], [63], [65].

Culture: this can be considered a huge difficulty facing the adoption and acceptance of blockchain. Since most people in KSA prefer to contact the government using traditional methods, explaining the benefits of blockchain is essential [75]–[78].

Risk policy: making the policy on risk clear to patients and using smart contracts will help to make policy suitable for them, motivating them to become involved in blockchain technology [32], [71].

Ease of use: this involves demonstrating the system to motivate practitioners, such as doctors, to use technology rather than basic methods (paper), reducing the cost and waiting times and improving treatment outcomes [79], [80].

B. FACTORS RELATING TO SECURITY

This section encompasses all factors relating to security. System security is measured by data integrity, privacy, confidentiality, transparency, and anonymity.

Data integrity: the immutable property of blockchain guarantees the integrity of the data because, once the data are saved on blockchain, they cannot be altered, corrupted, or even deleted [50], [58], [63], [65], [73].

Privacy: blockchain is more secure, since all data are encrypted. Using symmetric encryption helps to keep patients' identity anonymous, protecting their privacy [40], [50], [65].

Confidentiality: because data are by default encrypted by the symmetric technique, patient confidentiality is assured, and this maintains anonymity and protects information against hacking. Using blockchain makes the data/records available, reducing the issues arising from storing patient data locally at each hospital, such as the need to repeat tests and basic paperwork [63], [73], [81].

Transparency: blockchain can improve communication and data transparency among clinics. The data are updated,

therefore become trusted and accessible from anywhere [13], [68], [71], [82].

Anonymity: eliminating any third party smooths communication and data transference among nodes, while the identities of individuals remain anonymous by virtue of data encryption, making the system secure and reliable. Furthermore, when it comes to sensitive information about patients, access is restricted to fully trusted nodes [13], [50], [74].

C. FACTORS RELATED TO BLOCKCHAIN

In this category are the factors relating to blockchain. These features result from applying blockchain to the healthcare sector.

Availability/robustness: blockchain enables the replication of data or records in multiple nodes, ensuring that records that have been stored on blockchain are available. This makes the system flexible against data hacking, data loss, or data corruption [7], [61], [74].

Accuracy: records are accurate in terms of the consensus of nodes in the blockchain, because it is almost impossible for the data in records added on blockchain to be changed, tampered with, or deleted [50], [65].

Immutability: one of the most important properties of blockchain is that, after the nodes majority consensus, the records are preserved forever and it becomes very difficult for anyone to tamper with or modify them [13], [40], [50], [61], [63], [65].

Tamper-proofing: after data are added to the blockchain, due to the encryption and digital signature they cannot be changed. If any are modified or removed it is easy to detect [83].

Interoperability: one of the benefits of blockchain most needed by healthcare systems is to exchange patient data freely in a secure manner to ensure decreased costs and enhanced efficiency and privacy [13], [65], [71].

Access control: this provides the ability to track any action that has been carried out in the system, and by whom, thus limiting access to critical information to completely trusted nodes [20], [65].

D. DISADVANTAGES OF BLOCKCHAIN

Scalability: as the system's users store and add data the blockchain grows, storing appended data and all associated hashes, thus increasing the computational power and storage demands [62]. Since only those blockchain users able to participate as miners of full nodes have sufficient computational power and storage space [4], its scalability may be compromised.

In response, blockchain supports three types of nodes: full nodes; light nodes; and archive nodes [84]. Full nodes process each transaction and store each block in the blockchain. Light nodes store only block headers containing the hash of the previous block, the hash of the Merkle Root and the nonce value, hence without using large portions of memory can verify that certain transactions are unaltered, moreover they can access the data that they desire. Archive nodes store all transactions and blocks in exactly the same way as full nodes; in addition, they store receipts of transactions, thus can help the network to retrieve the necessary data [85], [86]. Nodes' versatility increases the scalability of the Ethereum blockchain; for instance individuals and large institutions can interact with blockchain for their own purposes using their available resources [4].

Storing medical data on blockchain is expensive, so we suggest an off-chain secure data management mechanism. This can be arranged in two ways. The first is to identify a legal institution, for instance a government authority, to take responsibility for hosting the medical records and providing storage facilities. The second is to manage the medical data as presented, for storage at the individual institutions in which patients register their information. In both arrangements the blockchain operates a uniform resource identifier to point to off-chain storage of related fine-grained medical datasets. To assure the data's integrity, a hashing summary of the actual clinical data is uploaded to the blockchain while, for auditing purposes, the sharing list is recorded on the blockchain; that is, the list of whoever is approved to access to the data. For security purposes, the off-chain EMR data are encrypted using asymmetric encryption [38].

Furthermore, to counter the issue of scalability, encrypted clinical data may be stored off-chain; the blockchain itself may only store how the data may be accessed, using condensed information [8], [14], [37]. This deals with the GDPR issue, the 'right to be forgotten', because, even if the pointer to the data cannot be permanently deleted, the actual medical data can [40]. Reasonable solutions include using blockchain as an index of medical data rather than as records storage [82] and making sure that only the verified and ongoing transactions are stored, not the whole history [87].

Standardisation: because the technology is still in its infancy, there are bound to be challenges to its application to the health sector. It lacks any standardisation structures. There is a need for properly authenticated and certified standards that meet international requirements for systems in the health sector around the world, including the nature of the data shared on the network, an evaluation of size and the appropriate format for exchange over the blockchain network. The standards would serve as precautionary safety measure for network storage and sharing of data [88].

51% attack: blockchain's infrastructure makes it impossible for any centralised entity to use the network for its own advantage. Inasmuch as the technology offers a secure platform for managing data, however, there is a risk that a single entity on the network gains control over the majority of the hash rate and is thus in a position to effect amendments to data. For this to happen, the central entity would need huge power to modify or exclude certain transactions from the original order.

In the event of a 51% attack, the successful majority would be able to prevent some or all network transactions from being confirmed, yet it could not reverse any transactions by other users on the network. Neither could it prevent other users

from continuing to create new content and broadcast it over the network [88]–[91].

Speed: it is impractical for a hospital to use proof-of-work (PoW), since it is a computationally demanding algorithm and, even to mine just the transactions, it would need to establish large computer centres. For all these mentioned reasons, unlike like proof-of-authority or proof-of-stake, PoW does not suit the limitations. In the healthcare environment Transaction speed can be vital, and PoW is a slow consensus algorithm. Furthermore, it can be used with neither a consortium nor a private blockchain, in which transaction speed is faster and trust is easier to establish [74].

VI. RESEARCH METHODOLOGY

Both quantitative and qualitative methods are commonly used by scholars to confirm the findings of their investigations. Recently, to gain a deep understating of the research problem, there has been increased use of a combination of both in a single study, instead of just one. Quantitative, qualitative, and mixed-method approaches are examined in the first section, then the focus turns to explaining the triangulation technique employed in the confirmation study, with an in-depth explanation of the further research methods used: the interviews with experts; and the survey.

Qualitative methods are usually employed to analyse and explain non-numeric data to clarify and understand certain phenomena. They let scholars investigate and question areas of research, and they help them to explore new important variables. They involve gathering and analysing data, interpreting them to understand the situation or the field, for instance individuals' experiences, values, and behaviours [92]. Under the qualitative research banner are several possible techniques, such as observations, interviews, discussions, and documents, all of which make the data that are gathered rich and holistic [92].

Quantitative methods are typically used when the factors that impact on results need to be identified, the feasibility of an intervention determined, or the results predicted. In addition, they are used to collect, analyse, and interpret numeric data produced by surveys or questionnaires, and help to define certain phenomena [92].

Since the nature of this research is exploratory, and because this study is based on mixed-methods research [93], both quantitative and qualitative approaches were adopted. To ascertain the study's aims a methodical triangulation research technique in a sequential approach was adopted [94]. This technique helps researchers to paint a comprehensive picture of the topic and increases the possibility of validating and confirming the results. The research technique in Table 1 comprises the literature review, expert review, and survey.

For this study, to produce significant results an adequate number of experts had to be interviewed. At this stage it is essential to establish the minimum sample so that reliable results can be acquired [95].

Scholars are not in agreement over how many experts should be interviewed, yet most recommend between three and 20 [96], [97]. One suggestion is to aim for saturation [98], at which point no new data can be produced [99]. It is suggested by [100] that this point is normally achieved when 12 respondents have been interviewed. As a consequence, the present study interviewed 16 blockchain and healthcare IT experts.

TABLE 1. Summary of interviewees.

Expert	Job discretion	Years of experience
1	Network Administrator	16
2	Security Engineer	5
3	Medical System Specialist	12
4	Software Engineer (Blockchain Expert)	5
5	Network Administrator	6
6	System Engineer	12
7	Network Security	10
8	Database Administrator	11
9	Software Engineer	5
10	Application Support	7
11	Information Security Engineer	5
12	Network Administrator	8
13	System Technician	17
14	Cyber Security	15
15	Assistant Professor (Blockchain Expert)	3
16	Chief Technology Officer (Blockchain Expert)	4

After the expert interviews and review, the framework was revised according to the experts' suggestions.

Next, a questionnaire was distributed to healthcare IT specialists and blockchain experts. The aim was to confirm the framework reviewed by the experts, and a questionnaire was considered to be the best way to do so. According to .Recker [101], questionnaires have the ability to confirm and quantify the results of quantitative studies. In fact, many scholars choose this method because it is effective in collecting data that cannot be observed, such as respondents' opinions. It can also gather data relating to a wide population that cannot be directly observed, and participants have the freedom to give their answers when they feel most ready [102].

To confirm the framework, a self-administered questionnaire was employed in this study, and was uploaded to the internet to distribute it to various practitioners experienced in the field of blockchain. Each respondent has a minimum of two years' experience in this field. In total, 45 practitioners took part in the web-based survey.

Mostly, the calculation of random sample sizes for a questionnaire is performed mathematically, according to set guidelines [100]. In establishing the minimum sample size, two types of errors need to be considered [95]: the first is the type 1 or α error, which occurs when a true null hypothesis is rejected. The second is the type 2 or β error, which arises where a false null hypothesis is accepted. By convention, α is normally 0.05 and (1- β) is 0.95 [95]. A further parameter must be considered, namely effect size. This indicates the strength of the link between the predictor and the outcome variables. According to [103], there are three effect sizes: small (d = 0.2); medium (d = 0.5); and large (d=0.8). Studies that are exploratory in nature often employ a large effect size. To calculate the minimum sample size, this study used

TABLE 2. Sample size.

Statistical test	Mean: Difference from constant o-sample test)	
Tails	Two	Input
Effect size (d)	0.8	
Error probability (α)	0.05	
Power (1– β error probability)	0.95	
Minimum sample size	23	Output

G∗ Power software [104]. The t-test was essential in this calculation; in fact, it made it possible to distinguish between the means. The calculation can be seen Table 2. As shown, it was first decided to set the minimum sample size at 23.

Nonetheless, some statisticians maintain that, when applied to a survey, only a larger sample size of 30 participants can be regarded as sufficient, considering the Central Limit Theorem [105]. For this reason, the decision was taken to set the minimum sample size to 30 blockchain experts and healthcare IT specialists.

VII. EXPERT REVIEW FINDINGS

The goal of the analysis was to present and examine the findings of the interviews with experts specialising in blockchain and healthcare IT. The data were from semi-structured interviews with a total of 16 experts from various countries. The reason for conducting these interviews was to examine the factors supporting data-sharing using blockchain among healthcare organisations, as identified by the expert review. The interviews made it possible to explore potential additional factors.

A. HEALTHCARE SYSTEM CATEGORY

Once the participants had answered the closed-ended questions, they were asked to give their thoughts on factors relating to healthcare systems. The results were clear; all agreed that the healthcare system factors are highly important or important in the context of using blockchain for data-sharing. Of the experts interviewed, most agreed on the importance of decentralisation. Additionally, every expert agreed that efficiency is vital to the use of blockchain to share data in the healthcare sector and that a consideration of culture is vital. Interviewees were mostly in agreement on the importance of taking into account the factor of risk policy in the healthcare sector. Similarly, all stated that it is very important to consider the factor of ease of use when attempting to share data using blockchain in the healthcare sector. Table 3 presents the most notable findings in this regard.

B. SECURITY CATEGORY

As clearly shown by the findings from the expert interviews, security factors are viewed as very important or important to achieving data-sharing. It was fairly clear that there was consensus among respondents on the importance of data integrity to achieving data-sharing. Moreover, all agreed that, if data-sharing is to be achieved by healthcare institutions,

TABLE 3. Healthcare findings.

Code	Theme	Expert
Decentralisation	"It is very important because data will be safe and the risk of losing it will be lower as the data exists in many nodes."	8
	"It quite important because it will help to keep the data safe, authenticated, and remove forged data."	9
	"It is so important because it keeps data available, updated, and safe."	10
	"It is quite important because it will make the data safer, shared and not exclusive to a certain entity."	13
	"It is important especially for the healthcare sector because it will eliminate the dependence on the centralized authority."	14
Cost	"It is important because it will reduce the cost for the patients in the long-term, where the patient doesn't have to carry the tests in CD or hard copies."	6
	"It will help to reduce the cost for both patients and the organisations by not duplicating the tests which makes it very important."	7
	"It is important to save time and the cost for both hospitals and patients by not doing the paperwork and tests again."	11
	"Lower the cost of the patient and get a more accurate diagnosis in less visits."	12
	"It is important to reduce the cost for the patients such as the registration cost and other medical tests."	16
Efficiency	"It will improve the level service that hospital gives otherwise it will take and waste critical time by running the same test and same diagnosis again"	1
	"The efficiency will be better since the data will be accessible from anywhere"	2
	"It's very important and by using blockchain it will increase the efficiency and will be faster."	3
	"The current system is not perfect and blockchain is very important to increase the efficiency of the healthcare system."	5
	"It is very important and blockchain can help to increase the efficiency of the system."	7
Culture	"It is human nature to resist change, and it might take time especially for older people."	1
	"At first, it will be difficult since people are conservatives and concern regarding their sensitive data. Yet, it would be easier to be accepted by society if it was by the government"	2
	"Culture is important and it is human nature to resist anything new, showing the benefits by the government will help people to accept the technology."	6
	"Since it is a new technology there will be resistance that will be decreased within time if it was sponsored by the ministry of health."	12
	"People are more accepting to the technology when they see the benefits of it and culture can make a big difference thus the implementer needs to understand the culture."	16
Risk Policy	"I don't think that the patients have any knowledge or awareness regarding the risk	2

TABLE 3. *(Continued.)* **Healthcare findings.**

	policy and should be clear and understandable by them thus will increase the acceptance of the new technology"	
	"This factor is important because the level of the patients' awareness is low and could be better."	3
	"Patients are not aware of the risk policy and it is important to know and be educated about it."	6
	"It very important, because it is not clear to patients and social media can be used to increase the awareness of the patients."	7
	"The patient should know about the policy and to increase the awareness different methods can be used such as SMS, brochures and hospital websites."	10
Ease of Use	"It is important factor and should be there to decrease the resistance by the employees."	3
	"It is very important and the employees usually resist the new system if it was not easy or take more steps to do a certain job."	5
	"It is very important otherwise people will stop using the system it should be user-friendly to be used and accepted."	6
	"To make the system easy enough for the employees to use will help to bypass most of the barriers that might stop using or adopting the technology."	9
	"Showing the easiness of the system and what the benefits that would result for the employees will help to make it more acceptable."	12

data privacy should be in place. Many pointed to the importance of confidentiality to an organisation's goal of data-sharing. All agreed on the importance of transparency to sharing data. The notable statements are presented in Table 4.

C. BLOCKCHAIN CATEGORY

Following the interviews, it was clear that blockchain factors are seen as either very important or important in using blockchain to share data in the healthcare sector. There was clear agreement among expert respondents on the importance of the factor of availability in the healthcare sector. Additionally, there was a firm belief among all interviewees that accuracy is vital to the use of blockchain to share data in the healthcare sector. Moreover, all stated that immutability is vital and all agreed on the importance of tamper-proofing to the use of blockchain to share data in the healthcare sector. Furthermore, all stated that that interoperability is vital and agreed over the importance of taking into account the factor of access control to the use of blockchain to share data in the healthcare sector. Table 5 below presents the most notable findings in this regard.

VIII. RESULTS OF THE QUESTIONNAIRE

This section presents the findings yielded by the survey. The questionnaire was distributed to 80 experts, yet only 56 responded. All had jobs in various organisations. The final sample comprised 45 participants. The reason for conducting the survey was to confirm the updated framework, already revised on the basis of the expert review.

TABLE 4. **Security findings.**

Data Integrity	"It is very important in order to protect the patients from any risks that could result from errors, it's low in the current system and blockchain will increase it."	3
	"It is very important and it is one of the features that blockchain can offer for healthcare and it won't be affected if one the nodes go down."	5
	"Blockchain can preserve data integrity because data cannot be modified therefore it is very important."	6
	"It is very important because it will affect the patient safety and may lead to his death and blockchain can help to improve that."	7
	"Human errors are there and data entry mistakes can cost lives, blockchain could help to remove errors after data authenticated as well as data cannot be changed."	13
Privacy	"This kind of information and the details must be kept private and blockchain can improve the privacy of the patients".	2
	"It is very important in order to protect the data of the patient unless it was the authorized person and limit the access to the right person."	5
	"It is very critical in the medical institution to protect the information of the patient and keep the privacy of it."	7
	"As a patient, I want my data to be saved and private away from unauthorized people and from selling it to a different party which makes it very important."	9
	"The privacy of the patient is very important and rationing the access control will help to maintain the privacy."	12
Confidentiality	"It's important to keep the patients' data confidential as well as for the employees in some cases"	2
	"Currently, we don't have any clear rules for information regarding confidentiality, it is important to keep the patient information confidential, and blockchain helps to do that."	6
	"It is the right of the patient to keep this information confidential between him and the doctor so it is important."	7
	"It is important to make sure that only the right and authorized specialist can access and take look at the information."	9
	"It is very important so people can trust the system because some diseases have a bad stigma such as HIV and should be kept confidential and blockchain can raise the level of confidentiality."	16
Transparency	"Transparency is there in the current system and blockchain can increase it."	3
	"It is very important and required in the healthcare system to give good care to the patients and blockchain can boost the transparency of the data."	7
	"It is important and blockchain can make the data more transparent and stop it from being exclusive and locked in the organization."	9
	"The level of the transparency currently is low because the data is locally locked and hidden and blockchain can elevate the level of transparency."	10
	"Blockchain can contribute to making data more	14

TABLE 4. *(Continued.)* **Security findings.**

	transparent between departments and become clear and in motion instead of being stuck in the organization."	
Anonymity	"It important and good idea to protect patient with critical condition and don't reveal his identity."	6
	"It is essential in the healthcare environment in order to protect patient information especially in critical conditions thus it is very important."	7
	"It is important to protect the patient identity and when sharing data it will help to prevent impersonation and counterfeit the data."	9
	"Anonymity is important but not necessarily needed for security and in blockchain by default is better than in centralized system."	15
	"I don't this factor will be important because sometimes it is needed for patients to be known."	16

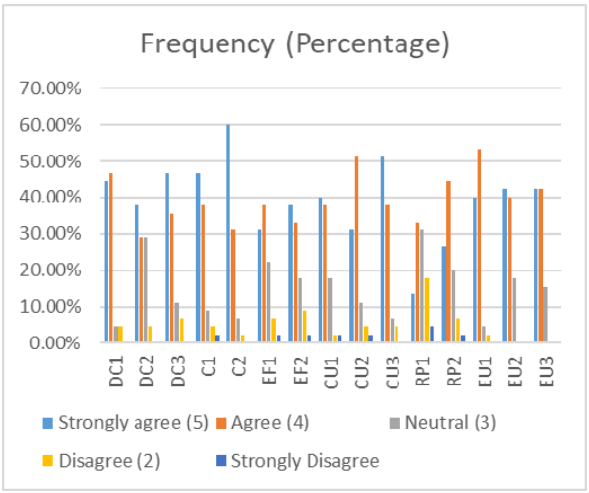

FIGURE 2. Frequency of responses to healthcare system factors.

The survey analysis consists of three sections. The first is participants' demographic information, followed by sections describing and then giving the frequency of the responses.

A. DESCRIPTIVE AND FREQUENCY ANALYSES OF THE FACTORS IN HEALTHCARE SYSTEMS

The 45 participants were asked a total of 15 questions on the healthcare systems section of the framework. Participants were encouraged to rank the importance of factors affecting the use of blockchain to share data in the healthcare sector. Figure 2 presents the frequency of the responses.

B. DESCRIPTIVE AND FREQUENCY ANALYSES OF SECURITY FACTORS

The 45 participants were asked 10 questions on the security factors and encouraged to rank their importance to using blockchain in the healthcare sector. Figure 3 shows the frequency of the responses clearly.

C. DESCRIPTIVE AND FREQUENCY ANALYSES OF THE BLOCKCHAIN FACTORS

The 45 participants were asked 10 questions on blockchain factors and encouraged to rank their importance to the use

TABLE 5. Blockchain findings.

Availability	"It is very important because that data will be available all the time and helps a lot in healthcare especially when a critical case occurs to the patient."	8
	"The availability of data using blockchain is assured all the time which is very important in the healthcare."	9
	"Lack of access to the data is an issue and critical in hospitals, and blockchain can make sure that data are available all the time which is very important."	10
	"Blockchain will help to keep the data available all the time which is important to give better healthcare services."	11
	"System failure can cause the absence of data which could affect the patient but blockchain can help to makes it available all the time."	12
Accuracy	"In the current system, there are human errors, that can affect the patient safety, therefore, the accuracy of the data is very important, and blockchain can improve it."	5
	"It is very important because data accuracy can help to give the proper treatment to the patient and blockchain can improve the data accuracy."	6
	"In the centralized system, it is possible to have error either by the system or human and blockchain can improve the accuracy of data and reduce the errors."	9
	"This factor is essential and could make a difference in the such environment"	11
	"Any mistakes of the information could affect the patient's life therefore it is very important."	13
Immutability	"There are some possibilities for manipulating that data in the database in the current system and need to be controlled and this factor that's provided by blockchain is very important regarding the sensitivity of the data."	2
	"It is very important in healthcare systems, where you know what happened and when and in case of changing or adding information it will show who did it or which system did it to figure out if something goes wrong."	4
	"Modifying the data currently is possible thus it is very essential because blockchain cannot tolerate data tampering."	7
	"Changing data currently is doable which is critical and might affect the patient safety and blockchain can stop that and see any activities that have been made."	9
	"It a fundamental feature of blockchain and it is very important to keep the data protected, see the history of patients and trace back bad actors on the systems such as hackers or someone entering bad information and distrust it."	16
Tamper-proofing	"This factor considers very important because data tampering is possible and can be tracked but with difficulty and the lost data can be brought back based on the backup solution, but not necessarily all data."	2

TABLE 5. *(Continued.)* **Blockchain findings.**

	"Currently, we cannot track the modified data in the database unlike blockchain which make this factor very important."	3
	"Very important because IT experts try to do things manually in systems to make them tamper-proof and cost a lot of money but blockchain is more fundamental and helps to get rid of hackers, stops them from doing bad things and, does it for free."	4
	"Blockchain is way better and can help to keep tracking any changes and actions by unauthorized persons or intruders by access control."	14
	"If you have immutability then it can boost tamper-proofing, because you can't alter data or falsify data once it is in the system which makes it very important."	15
Interoperability	"It is one of the big benefits of the blockchain and it is very hard to share data without the technologies and cost a lot of money to exchange information and connect systems together but blockchain does that and it is fundamental in the technology thus, it is very important. Blockchain helps a lot with data sharing and does it in a much cheaper, easier and more reliable way than all technologies."	4
	"There is no exchange of data between hospitals because it will help to reduce the effort of the patients and the cost, therefore, it is very important and blockchain can offer it to solve this problem."	7
	"There are no data sharing between hospitals and it is needed because it helps the patients to get different diagnoses by multiple doctors and get better treatment."	9
	"In the current time, there is no data exchange between hospitals and the patient that comes from another hospital is treated as a new patient and has to do the registration and often performs medical exams all over again."	10
	"Blockchain has some advantage because it is provided interoperability by default, unlike the centralized system which is very important."	15
Access Control	"Healthcare has access control everywhere and for everything whether for physical cards to get into buildings, or to control access to the systems. Blockchain can do that and can copy healthcare access control features using permissioned blockchain which uses the same creational and access control and let that applied in the blockchain. It is very important to control who can access data and give different access control to different persons."	4
	"It is very important to know who is accessing data and give access authorizations to who can access certain data and who cannot."	6
	"It is very important to protect the data from any unauthorized access."	8
	"It is very important to put limits of data accessing and decrease illegal activities in the system."	9
	"Controlling access control and give different levels of it can help to keep the data safe and preserve patient privacy."	13

of blockchain in the healthcare sector. Figure 4 shows the frequency of responses to the blockchain factors clearly.

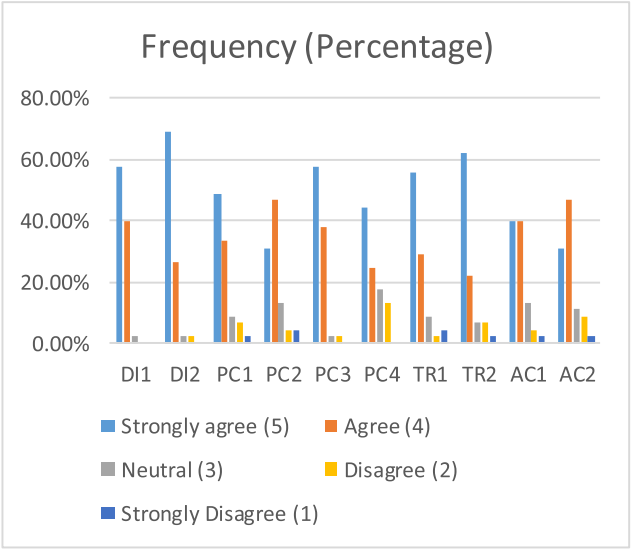

FIGURE 3. Frequency of responses to the security factors.

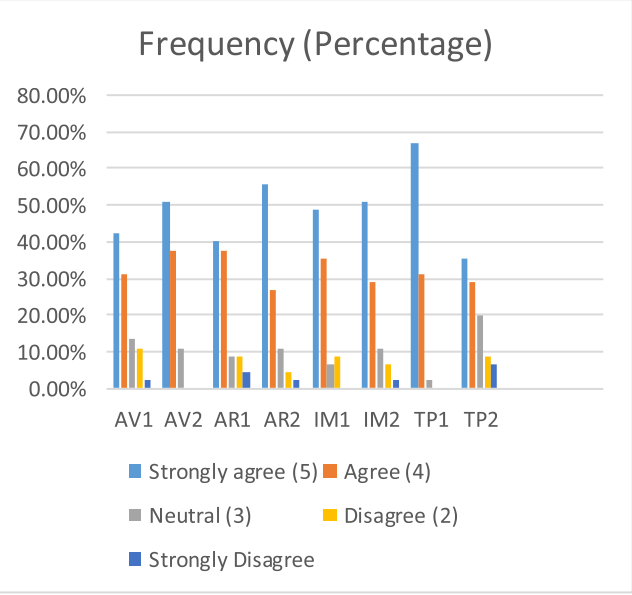

FIGURE 4. Frequency of responses to blockchain factors.

IX. DISCUSSION

As this study's analysis took place in stages, each informed by the findings of the previous, it can be said to adopt a multi-phase mixed sequential methods approach. Thus, after the literature review, the framework was confirmed by the expert review and questionnaire: the names of three factors were modified and one factor was removed.

A. EXPERT REVIEW FINDINGS

The experts suggested that the framework should be re-categorised, moving the factor of access control from the blockchain to the security category. In addition, they felt that the anonymity factor was unimportant and should be omitted as it could create confusion, even though, as mentioned in the literature review, according to [27] it is a possible means of protecting information privacy. It was duly

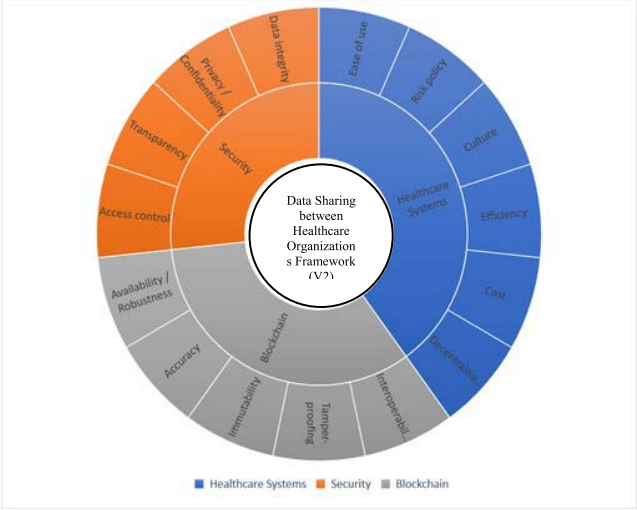

FIGURE 5. Framework V2.

removed. Furthermore, one expert suggested adding identity and another adding identity authentication to the proposed framework; however, as patients' identity can be established from their unique ID number, this was not considered a problem so it was not added. The experts were asked if, in addition to those already discussed, there were further factors that should be added or modified to make the framework more robust and reliable. They suggested that two factors should be merged, namely privacy and confidentiality.

B. DISCUSSION OF QUESTIONNAIRE RESULTS

The questionnaire was used to confirm the reviewed framework and establish whether the identified factors are statically significant. Below, the discussion focuses on the healthcare system, security, and blockchain factors.

Regarding the statistical results for the healthcare systems factors, after studying the questionnaire findings it was concluded that all items were statistically significant apart from RP1, which was duly removed. In brief, respondents agreed that all healthcare systems factors are vital and should be taken into account when using blockchain in the healthcare sector.

In relation to the security factors, all were seen as vital by the questionnaire's respondents. The statistical test results clearly proved that they are all statistically significant. The participants were confident that every security factor is vital and should be taken into account when using blockchain in the healthcare sector.

Analysis of the questionnaire findings proved that every blockchain factor is statistically significant. Respondents were in agreement that all are vital and must be taken into account when using blockchain in the healthcare sector.

The initial framework was thus modified after assessing the findings of the interviews with experts, and this revised framework was confirmed by the survey. As a result, one of the original factors was discarded, two were merged, and one was re-categorised, as seen in the second version in Figure 5.

X. CONCLUSION

In summary, the primary objective of this research was to give an overview of blockchain technology's potential in the healthcare sector. The study analysed blockchain technology from several perspectives, including that of storing medical records in blockchains and patient data ownership. The use of technology in providing healthcare services involves many considerations that must be analysed comprehensively to render it effective. New healthcare information technologies focus on providing an avenue along which the health sector can keep growing and improving, while maintaining quality through minimising the cost of accessing healthcare and simultaneously improving patients' experience of healthcare facilities. Although numerous technologies have improved data management in the health sector, challenges persist. For example, current technologies have not been successful in improving health facilities' maintenance of data and records.

The healthcare sector has suffered from inefficiencies in its handling of data. Many patients and healthcare organisations face numerous hurdles to obtaining current real-time patient information. Patients are frustrated when scheduling appointments with healthcare organisations that have outdated contact information. Significant time is wasted by staff in coordinating patients' care and updating other healthcare organisations. This is evident when a patient has been hospitalised for an extended time: their primary provider is unaware of their condition until they have been discharged.

Following the literature review, it became clear that it is essential to explore blockchain's effects on the healthcare sector. This study aimed to investigate the factors that support data-sharing using blockchain among healthcare organisations. The research has proposed and confirmed a framework that promotes such data-sharing.

ACKNOWLEDGMENT

The authors acknowledge with thanks DSR for technical support.

REFERENCES

[1] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019.

[2] L. Cardoso, F. Marins, F. Portela, M. Santos, A. Abelha, and J. Machado, "The next generation of interoperability agents in healthcare," *Int. J. Environ. Res. Public Health*, vol. 11, no. 5, pp. 5349–5371, May 2014.

[3] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," 2017, *arXiv:1706.03700*.

[4] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[5] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[6] C. S. E. McIntyre and M. Cornish. (2016). *Members and Patient Privacy: Be Aware and Beware! Counsel of Nurses, Ontario Nurses Association*. [Online]. Available: https://www.ona.org/wp-content/uploads/ona_flfeature_patientprivacy_201601.pdf

[7] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus database: A critical analysis," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1348–1353, doi: 10.1109/TrustCom/BigDataSE.2018.00186.

[8] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.
[9] R. Ribitzky, J. S. Clair, D. I. Houlding, C. T. McFarlane, B. Ahier, M. Gould, H. L. Flannery, E. Pupo, and K. A. Clauson, "Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: Paving the future for healthcare," *Blockchain Healthcare Today*, vol. 1, 2018.
[10] M. A. Cyran, "Blockchain as a foundation for sharing healthcare data," *Blockchain in Healthcare Today*, vol. 1, 2018.
[11] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, p. 5, Jan. 2019.
[12] H. M. Hussen, "A blockchain-based service provider validation and verification framework for healthcare virtual organization," *UHD J. Sci. Technol.*, vol. 2, no. 2, pp. 24–31, Aug. 2018, doi: 10.21928/uhdjst.v2n2y2018.pp24-31.
[13] E. W. Mwashuma, "Towards universal healthcare coverage through adoption of blockchain technology: A literature review," *J. Health Informat. Afr.*, vol. 5, no. 2, pp. 46–51, 2018.
[14] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.
[15] M. Goddard, "The EU general data protection regulation (GDPR): European regulation that has a global impact," *Int. J. Market Res.*, vol. 59, no. 6, pp. 703–705, Nov. 2017.
[16] A. S. Downey and S. Olson, *Sharing Clinical Research Data: Workshop Summary*. Washington, DC, USA: National Academies Press, 2013.
[17] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
[18] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," *J. Comput. Syst. Sci.*, vol. 90, pp. 46–62, Dec. 2017.
[19] B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Future Gener. Comput. Syst.*, vol. 68, pp. 1–13, Mar. 2017.
[20] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Proc. Comput. Sci.*, vol. 113, pp. 73–80, Jan. 2017.
[21] A. Small and D. Wainwright, "Privacy and security of electronic patient records—Tailoring multimethodology to explore the socio-political problems associated with role based access control systems," *Eur. J. Oper. Res.*, vol. 265, no. 1, pp. 344–360, 2018.
[22] S. I. Khan and A. S. Latiful Hoque, "Privacy and security problems of national health data warehouse: A convenient solution for developing countries," in *Proc. Int. Conf. Netw. Syst. Secur. (NSysS)*, Jan. 2016, pp. 1–6.
[23] S. Suzuki and J. Murai, "Blockchain as an audit-able communication channel," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2017, pp. 516–522.
[24] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[25] N. R. Adam and J. C. Worthmann, "Security-control methods for statistical databases: A comparative study," *ACM Comput. Surv.*, vol. 21, no. 4, pp. 515–556, Dec. 1989.
[26] G. Duncan and D. Lambert, "The risk of disclosure for microdata," *J. Bus. Econ. Statist.*, vol. 7, no. 2, pp. 207–217, 1989.
[27] C. C. Aggarwal and S. Y. Philip, *Privacy-Preserving Data Mining: Models and Algorithms*. Springer, 2008.
[28] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jul. 2018.
[29] L. X. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.
[30] M. Almalki, G. FitzGerald, and M. Clark, "Health care system in Saudi Arabia: An overview," *Eastern Medit. Health J.*, vol. 17, no. 10, pp. 784–793, 2011.
[31] B. Aldosari, "Rates, levels, and determinants of electronic health record system adoption: A study of hospitals in riyadh, Saudi Arabia," *Int. J. Med. Informat.*, vol. 83, no. 5, pp. 330–342, May 2014.
[32] C. A. I. T. Commission. (2017). *Anti-Cyber Crime Law*. [Online]. Available: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx
[33] Accenture. (2017). *The Impact of Healthcare Cybersecurity on SAUDI ARABIAN Consumers*. [Online]. Available: https://www.accenture.com/_acnmedia/pdf-59/accenture-health-consumer-survey-cybersecurity-ksa.pdf
[34] M. Altuwaijri, "Health information technology strategic planning alignment in Saudi hospitals: A historical perspective," *J. Health Inform. Developing Countries*, vol. 5, no. 2, pp. 338–355, 2012.
[35] S. Bah, H. Alharthi, A. A. El Mahalli, A. Jabali, M. Al-Qahtani, and N. Al-kahtani, "ÖAnnual survey on the level and extent of usage of electronic health records in government-related hospitals in Eastern Province, Saudi Arabia," *Perspect. Health Inf. Manage./AHIMA, Amer. Health Inf. Manage. Assoc.*, vol. 8, 2011.
[36] A. Aljarullah, R. Crowder, and G. Wills, "A framework for the adoption of EHRs by primary healthcare physicians in the kingdom of Saudi Arabia," in *Proc. Int. Conf. Inf. Soc. (i-Society)*, Jul. 2017, pp. 49–54.
[37] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, 2018.
[38] Z. Xiao, Z. Li, Y. Liu, L. Feng, W. Zhang, T. Lertwuthikarn, and R. S. Mong Goh, "EMRShare: A cross-organizational medical data sharing and management framework using permissioned blockchain," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 998–1003.
[39] K. Wust and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54.
[40] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019.
[41] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.
[42] L. Wang, W. Liu, and X. Han, "Blockchain-based government information resource sharing," in *Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2017, pp. 804–809.
[43] A. F. Hussein, N. Arunkumar, G. Ramírez-González, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cogn. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018.
[44] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019.
[45] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON)*, Jun. 2017, pp. 137–141.
[46] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, Jan. 2017.
[47] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017.
[48] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin message: Data insertion on a proof-of-work cryptocurrency system," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2015, pp. 332–336.
[49] ITGI, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, ISACA, Schaumburg, IL, USA, 2006.
[50] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technol. Innov. Manage. Rev.*, vol. 7, no. 10, pp. 22–34, Oct. 2017.
[51] C. N. Mead, "Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. Do we really need a better mousetrap?" *J. Healthcare Inf. Manage.*, vol. 20, no. 1, p. 71, 2006.
[52] O. Iroju, A. Soriyan, I. Gambo, and J. Olaleke, "Interoperability in healthcare: Benefits, challenges and resolutions," *Int. J. Innov. Appl. Stud.*, vol. 3, no. 1, pp. 262–270, 2013.
[53] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Al Ridhawi, and Y. Jararweh, "A collaborative mobile edge computing and user solution for service composition in 5G systems," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 11, p. e3446, Nov. 2018.
[54] I. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh, and H. T. Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities," *Comput. Netw.*, vol. 145, pp. 207–218, Nov. 2018.
[55] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706.

[56] A. Alkhodre, S. Jan, S. Khusro, T. Ali, Y. Alsaawy, and M. Yasar, "A blockchain-based value added tax (VAT) system: Saudi Arabia as a use-case," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 708–716, 2019.

[57] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR mHealth uHealth*, vol. 5, no. 7, p. e111, 2017.

[58] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *Proc. 15th Learn. Technol. Conf. (L&T)*, Feb. 2018, pp. 112–119.

[59] E. D. J. Skiba, "The potential of blockchain in education and health care," *Nursing Educ. Perspect.*, vol. 38, no. 4, pp. 220–221, 2017.

[60] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.*, 2017, p. 650.

[61] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.

[62] C. Brodersen, B. Kalis, C. Leong, and E. Mitchell, *Blockchain: Securing a New Health Interoperability Experience*. Palo Alto, CA, USA: Accenture LLP, 2016, pp. 1–10.

[63] K. Rabah, "Challenges & opportunities for blockchain powered healthcare systems: A review," *Mara Res. J. Med. Health Sci.*, vol. 1, no. 1, pp. 45–52, 2017.

[64] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[65] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *J. Med. Internet Res.*, vol. 21, no. 2, Feb. 2019, Art. no. e12439, doi: 10.2196/12439.

[66] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[67] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, Aug. 2016, p. 13.

[68] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[69] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[70] A. G. M. Alzahrani, A. Alenezi, A. Mershed, H. Atlam, F. Mousa, and G. Wills, "A framework for data sharing between healthcare providers using blockchain," in *Proc. 5th Int. Conf. Internet Things, Big Data Secur.(IOTBDS)*, vol. 1, 2020, pp. 349–358.

[71] S. Khezr, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.

[72] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018.

[73] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–4, doi: 10.1109/ICECTA.2017.8252043.

[74] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

[75] M.-S. Hwang, C.-T. Li, J.-J. Shen, and Y.-P. Chu, "Challenges in e-government and security of information," *Inf. Secur.*, vol. 15, no. 1, pp. 9–20, 2004.

[76] R. M. Schneider, "A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques," in *Proc. Inf. Secur. Curriculum Develop. Conf. (InfoSecCD)*, 2010, pp. 107–116.

[77] N. R. Al Khater, "A model of a private sector organisation's intention to adopt cloud computing in the Kingdom of Saudi Arabia," Ph.D. dissertation, Univ. Southampton, 2017.

[78] A. Abdullah, S. Rogerson, N. B. Fairweather, and M. Prior, "The motivations for change towards e-government adoption: Case studies from Saudi Arabia," in *Proc. E-government Workshop*, 2006, vol. 6, no. 1, pp. 1–21.

[79] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, Feb. 2000.

[80] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," *Manage. Sci.*, vol. 35, no. 8, pp. 982–1003, Aug. 1989.

[81] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.

[82] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *Proc. ONC/NIST Blockchain Healthcare Res. Workshop* Gaithersburg, MD, USA, 2016, pp. 1–10.

[83] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *Proc. 4th Int. Conf. Syst. Informat. (ICSAI)*, Nov. 2017, pp. 975–979, doi: 10.1109/ICSAI.2017.8248427.

[84] G. Ethereum. (2017). *Official go Implementation of the Ethereum Protocol*. Accessed: Jan. 25, 2019. [Online]. Available: https://geth.ethereum.org

[85] V. Buterin, "On public and private blockchains," *Ethereum Blog*, Aug. 7, 2015.

[86] V. Buterin, "State tree pruning," *Ethereum Blog*, to be published.

[87] S. Attili, S. Ladwa, U. Sharma, and A. Trenkle, "Blockchain: The chain of trust and its potential to transform healthcare-our point of view," in *Proc. ONC/NIST Blockchain Healthcare Res. Workshop*, Gaithersburg, MD, USA, 2016, pp. 1–9.

[88] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, Jan. 2019.

[89] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[90] A. Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*. Cambridge, MA, USA: MIT Press, 2016.

[91] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[92] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Newbury Park, CA, USA: Sage, 2017.

[93] J. W. Creswell and V. L. P. Clark, *Designing and Conducting Mixed Methods Research*. Newbury Park, CA, USA: Sage, 2017.

[94] L. Cohen, L. Manion, and K. Morrison, *Research Methods in Education*. Hoboken, NJ, USA: Taylor & francis, 2013.

[95] A. Banerjee, U. Chitnis, S. Jadhav, J. Bhawalkar, and S. Chaudhury, "Hypothesis testing, type I and type II errors," *Ind. Psychiatry J.*, vol. 18, no. 2, p. 127, 2009.

[96] J. S. Grant and L. L. Davis, "Selection and use of content experts for instrument development," *Res. Nursing Health*, vol. 20, no. 3, pp. 269–274, Jun. 1997.

[97] M. R. Lynn, "Determination and quantification of content validity," *Nursing Res.*, vol. 35, no. 6, pp. 382–386, Nov. 1986.

[98] B. Marshall, P. Cardon, A. Poddar, and R. Fontenot, "Does sample size matter in qualitative research?: A review of qualitative interviews in is research," *J. Comput. Inf. Syst.*, vol. 54, no. 1, pp. 11–22, Sep. 2013.

[99] G. A. Bowen, "Naturalistic inquiry and the saturation concept: A research note," *Qualitative Res.*, vol. 8, no. 1, pp. 137–152, 2008.

[100] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," *Field Methods*, vol. 18, no. 1, pp. 59–82, 2006.

[101] J. Recker, *Scientific Research in Information Systems: A Beginner's Guide*. Berlin, Germany: Springer, 2012.

[102] A. Bhattacherjee. 2012. *Social Science Research: Principles, Methods, and Practices*. Univ. South Florida.

[103] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. Abingdon, U.K.: Routledge, 1988.

[104] F. Faul, E. Erdfelder, A. Buchner, and A. G. Lang, "Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses," *Behav. Res. Methods*, vol. 41, no. 4, pp. 1149–1160, 2009.

[105] A. Field, *Discovering Statistics Using IBM SPSS Statistics*. Newbury Park, CA, USA: Sage, 2013.