INFORMATICA, 2022, Vol. 33, No. 2, 365–397

DOI: https://doi.org/10.15388/22-INFOR486

Ontological Representation of Healthcare Application Security Using Blockchain Technology

Raimundas MATULEVIČIUS[1,*], Mubashar IQBAL[1,*], Emna AMMAR ELHADJAMOR[2], Sonia Ayachi GHANNOUCHI[2], Mariia BAKHTINA[1], Slaheddine GHANNOUCHI[3]

[1] *Institute of Computer Science, University of Tartu, Narva mnt 18, 51009 Tartu, Estonia*
[2] *RIADI Laboratory-ENSI, Manouba University, Tunisia ISG Sousse, Sousse University, Tunisia*
[3] *Farhat Hached University Hospital of Sousse, Ibn El Jazzar Medical Faculty of Sousse, University of Sousse, Tunisia*
e-mail: rma@ut.ee, mubashar.iqbal@ut.ee, emnahouda@yahoo.fr, sonia.ayachi.ghannouchi@gmail.com, mariia.bakhtina@ut.ee, slaheddine.ghannouchi@gmail.com

Received: December 2021; accepted: May 2022

Abstract. Blockchain is gaining traction for improving the security of healthcare applications, however, it does not become a silver bullet as various security threats are observed in blockchain-based applications. Moreover, when performing the security risk management (SRM) of blockchain-based applications, there are conceptual ambiguities and semantic gaps that hinder from treating the security threats effectively. To address these issues, we present a blockchain-based healthcare security ontology (HealthOnt) that offers coherent and formal information models to treat security threats of traditional and blockchain-based applications. We evaluate the ontology by performing the SRM of a back-pain patient's healthcare application case. The results show that HealthOnt can support the iterative process of SRM and can be continually updated when new security threats, vulnerabilities, or countermeasures emerge. In addition, the HealthOnt may assist in the modelling and analysis of real-world situations while addressing important security concerns from the perspective of stakeholders. This work can help blockchain developers, practitioners, and other associated stakeholders to develop secure blockchain-based healthcare applications in the early stages.

Key words: blockchain, healthcare, security threats, healthcare security ontology.

1. Introduction

Digitization in healthcare means generating massive electronic health records (EHRs), empowering patients as well as the whole healthcare sector (Narikimilli *et al.*, 2020). Furthermore, healthcare organizations connect the internet of things (IoT) and smart devices with healthcare applications to allow real-time monitoring of patients' health and decrease

*Corresponding authors.

hospital visits for routine checks (Yaqoob *et al.*, 2021). Using IoT and smart devices in healthcare also results in large amounts of data generation. Such advancements bring opportunities for making immediate and informed decisions by dint of having access to the extensive patient data (Yaqoob *et al.*, 2021; Narikimilli *et al.*, 2020).

EHR combines the health-related information of patients (e.g. medical conditions, diseases, health monitoring data), prescription, medication, medical analysis, personal information (e.g. name, age, gender, address), and financial information (e.g. insurance, billing details). Such medical data is confidential and indispensable, as well as plays an essential role in patients' health diagnoses and treatments to reduce medical mistakes (Chen *et al.*, 2019). The growing medical data heightens the concerns of securing it against various security threats, for example, data tampering, data theft, and counterfeit drugs (Radhakrishnan *et al.*, 2019; Dagher *et al.*, 2018). Blockchain technology is emerging in healthcare to address such security challenges, improve data integrity, and restructure the transaction process to be decentralized, transparent, and irreversible. For example, Saha *et al.* (2019) present the blockchain-based healthcare application (BBHA) along with cloud computing to protect medical data from tampering, theft, and unauthorized use.

Blockchain is a decentralized computing architecture that operates over a peer-to-peer (P2P) network and maintains transactions in the immutable ledger (Chen *et al.*, 2018). The ledger contains a certain and verifiable record of every single transaction ever made (Saha *et al.*, 2019). While blockchain technology is making inroads to such domains as finance, supply chain, and digital identities, the healthcare sector is leading the way (Narikimilli *et al.*, 2020). The success of blockchain-based applications is contingent on accurate, verifiable, and untampered medical data.

1.1. *Motivation*

EHRs are one of the most valuable assets in healthcare applications. The current healthcare applications follow the traditional technology infrastructure where a centralized individual is responsible for maintaining the EHRs (Dagher *et al.*, 2018). Therefore, the traditional healthcare applications (THAs) suffer from diverse security threats (Xu *et al.*, 2019) that could negate the confidentiality, integrity, and availability of EHRs. Consequently, the tampered medical data can cause major issues during the patient's treatment. Besides that, there are risks of unauthorized access, information disclosure, and various internal and external threats. Mansfield-Devine (2016), Dagher *et al.* (2018) investigated the security of THAs, and findings show that organizations do not adhere to best practices when designing and developing healthcare applications. Moreover, the technology infrastructure is incompatible and does not provide security measures by design.

Security is critical in the acceptability of healthcare applications. The first motivation of our research is to identify the security threats of THAs and present blockchain as a countermeasure solution to mitigate them. The second motivation is to uncover potential security threats in BBHAs. Moreover, we aim to reveal what countermeasures are

available to mitigate these threats to secure BBHAs. The advent of blockchain technology has opened several research areas to preserve medical data, ensure data integrity, patient ownership of their data, easy exchange of medical data, and seamless medical insurance claims. However, there is conceptual ambiguity and semantic gaps because of varied interchangeable security concepts. Such a gap brings confusion about how to treat security threats effectively (Saha *et al.*, 2019; Linn and Koo, 2016) in healthcare applications. This constraint inspired us to build an ontological representation of healthcare information security. The ontological representation can be a helpful tool for assessing and communicating the security aspects of healthcare applications, allowing for timely decisions to fix them.

1.2. *Contributions*

This work builds on the work presented in Iqbal and Matulevičius (2021b), in which we present blockchain-based healthcare security ontology (HealthOnt). HealthOnt demonstrates blockchain as a countermeasure solution to alleviate security threats of THAs. However, BBHAs do not become a silver bullet, and various security threats can appear (Iqbal and Matulevičius, 2019). Thus, we extended the HealthOnt with knowledge of BBHAs security threats. This work makes the following contributions:

- A framework that explains the security threats that can appear in BBHAs;
- Extension of HealthOnt by encoding the knowledge of BBHAs security threats.

Similar to our previous work, the above contributions rely on the security risk management (SRM) domain model (Dubois *et al.*, 2010; Matulevičius, 2017). The domain model assists us in developing a framework for the security threats of BBHAs that contributed to the extension of HealthOnt. The HealthOnt can support the selection of blockchain when designing healthcare applications. There exist some comparable security models that address securing blockchain-based solutions (Arunkumar and Muppidi, 2019). However, such security models are either platform-specific or can not be updated upon appearing of new security threats. In contrast, HealthOnt encodes THAs' and BBHAs' information security into a dynamic ontology-based knowledge that can be extended, reused, and integrated with other security ontology representations.

1.3. *Paper Roadmap*

The remainder of the paper is structured as follows: Section 2 overviews the blockchain, discusses the research method, related work, and back-pain patients' healthcare application case. Section 3 presents the security threats that are mitigated in THAs through blockchain, and Section 4 discusses the security threats that can appear in BBHAs. Section 5 gives an overview of ontology development. Section 6 validates ontology, and Section 7 describes the emerging challenges in BBHAs. Section 8 concludes the paper.

2. Background

2.1. *Blockchain*

Blockchain is a decentralized, distributed, and immutable ledger technology (Ali *et al.*, 2020). Blockchain creates a chain of blocks where a unique cryptographic hash links each block to the previous block. Blockchain eliminates trusted intermediaries from the transaction process, allowing for the development of transparent, yet secure applications (Rahmadika and Rhee, 2018) where network participants are managing the ledger blocks by themselves collaboratively. Blockchain networks can be classified as permissionless (e.g. Ethereum) or permissioned (e.g. Hyperledger Fabric (HLF)). A permissionless blockchain is fully decentralized and accessible to anyone who can join the network and participate in the consensus process (Junejo *et al.*, 2020). Contrarily, a permissioned blockchain is partially decentralized with restrictions on who can join and access the operations. The designated authority establishes the structure of the blockchain network, as well as keeps control of various operations and processes (Jin *et al.*, 2019).

Blockchain relies on the consensus mechanisms (e.g. Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT)) to maintain the ledger state (Zhang and Lin, 2018). For example, Ethereum employs PoW, and HLF uses PBFT consensus. A smart contract in the blockchain is a piece of code that executes autonomously when certain conditions are met (Griggs *et al.*, 2018). Smart contract eliminates trusted intermediaries, requires less human intervention, and reduces enforcement costs. Additionally, a smart contract prevents malicious or unintentional security threats (Jin *et al.*, 2019) and enables decentralized distributed access control for resource authorization. Blockchain also provides provenance (Singh *et al.*, 2021) to verify the record's authenticity, while the ledger's characteristic of tamper-evidence (Chukwu and Garg, 2020) allows to detect any interference or tampering with the content. Finally, blockchain provides pseudonymous characteristics (Iqbal and Matulevičius, 2021b). Such blockchain characteristics make blockchain an enticing technology in various application domains. These features support transparency, trust, and tamper resistance, which are key components in making business and transactional operations more secure, efficient, and effective.

2.2. *Research Method*

We utilize the systematic literature review (SLR) since it allows the systematic analysis to identify relevant literature and synthesize the results. We follow the SLR guidelines of Kitchenham and Charters (2007) and define five research questions, each covering a different aspect of the SRM domain model.

RQ1: *What are the assets to protect in healthcare applications?*
RQ2: *What are the security threats of THAs?*
RQ3: *What are blockchain-based countermeasures to mitigate security threats of THAs?*
RQ4: *What are the security threats that can appear in BBHAs?*
RQ5: *What are the countermeasures to mitigate security threats of BBHAs?*

Table 1
Inclusion and exclusion criteria.

Inclusion criteria	
IC1	Papers discuss security threats of THAs
IC2	Papers discuss blockchain-based countermeasures to mitigate security threats of THAs
IC3	Papers present security threats of BBHAs
IC4	Papers discuss countermeasures to mitigate security threats of BBHAs
Exclusion criteria	
EC1	Papers published before 2008 and not available freely
EC2	Papers shorter than five pages and not written in English

In this SLR, we use the primary search, backward and forward tracing techniques (Okoli, 2015; Fink, 2019) to collect the relevant studies. First, we performed a primary search based on search strings to identify an initial set of papers. Second, a secondary search was performed employing backward and forward tracing. We defined the search strings to gather literature studies that discuss the BBHAs and their security aspects.

Search string: *((“blockchain” OR “blockchain-based” OR “decentralized”) AND (“healthcare application” OR “eHealth” OR “healthcare services”)) AND (“security” OR “security threats” OR “security risks” OR “security risk assessment”))*

We run these search strings on *ACM Digital Library*, *IEEE Xplore*, *SpringerLink*, *ScienceDirect*, *Scopus*, and *Web of Science*. We also included other non-academic research (e.g. gray literature). We applied *exclusion* (*EC*) and *inclusion* (*IC*) criteria to identify only the relevant papers (Table 1). For example, the papers that were duplicates, not in English, shorter than five pages, inaccessible (via university subscriptions or internet search), or published before 2008, were excluded (*EC1 & EC2*). We included the papers within the domain of blockchain and covering the security aspects of healthcare applications with blockchain (*IC1*), and providing blockchain-based countermeasures (*IC2*). To identify the security threats of BBHAs, we search for papers that discuss security threats of BBHAs (*IC3*) and countermeasures to mitigate them (*IC4*). The search resulted in approximately 1900 research papers from all the sources. First, we removed the duplicates and then performed several filtering iterations by considering the exclusion and inclusion criteria. A total of 90 papers remained that were subjected to full-text examination. After the full-text examination, a *total of 39 studies* remained that we used to conduct our research.

We utilize the *SRM domain model* (Dubois *et al.*, 2010; Matulevičius, 2017) that helps to structure the security risk analysis of healthcare applications (Tables 3 and 4) that contributed in HealthOnt. Among other SRM approaches (Ganji *et al.*, 2019), the SRM domain model fulfills the criteria of ISO/IEC 27001 standard and explores three aspects (*e.g. assets-, risk-, and risk treatment-related*) during the early phases of information system development. Based on the SRM domain model, the asset can be categorized as a system or business asset. The business asset has value, and the system asset supports it. Security criteria (confidentiality – C, integrity – I, and availability – A) distinguish business assets' security needs and constraints. The risk constitutes the threat and one or more vulnerabilities. The threat targets the system asset and exploits the vulnerability. The vulnerability

Table 2
Comparison of traditional healthcare applications.

Paper reference	Domain	Findings and addressed topics					
		Threats/Risks in healthcare	Counter-measures	Blockchain as counter-measure	Business/ System Assets	Vulnerabilities in healthcare	Use of SRM model
Fatima and Colomo-Palacios (2018)	Healthcare; Security	◉	◉	○	○ / ○	○	○
Ahmadi et al. (2019)	Healthcare; Security	○	◎	○	○ / ◎	○	○
Iwaya et al. (2020)	mHealth and uHealth; Security & Privacy	○	◎	◎	○ / ○	○	○
Sardi et al. (2020)	Healthcare; Security	◉	○	○	◎ / ○	○	○
Wani et al. (2020)	Healthcare; Security	◉	◉	○	○ / ○	◎	○
Semantha et al. (2020)	Healthcare; Privacy	◉	◉	◎	◉ / ○	○	○
Aljedaani and Babar (2021)	mHealth; Security	◎	◎	○	○ / ○	○	○
Yeng et al. (2021)	Healthcare; Security	◎	◎	○	◎ / ○	◎	○
Iqbal and Matulevičius (2021)	Healthcare; Security	◉	◉	◉	◉ / ◉	◉	◉

◉ - detailed discussion; ◎ - limited discussion; ○ - not addressed

is connected to the system assets and depicts their weaknesses. Impact harms the business asset and negates the security criteria. The risk treatment implements the security requirements as countermeasures to improve the system security. Furthermore, we evaluate the ontology by performing the SRM of a back-pain patient's healthcare application case.

2.3. *Related Work*

While healthcare applications are getting ubiquitous, researchers are working to improve the security and privacy of these applications to an acceptable level. However, a number of surveys and literature studies have only focused on the technical perspective of security threats in healthcare applications (Table 2). The studies neglected the business context and the impact of security threats on business assets, also not following the SRM domain model to describe the relationships of security threats with the system. Moreover, the THAs are not fully leveraging the benefits of emerging technology (e.g. blockchain).

For instance, Fatima and Colomo-Palacios (2018), Aljedaani and Babar (2021) review the common security threats and corresponding countermeasures considering only the technical side of the healthcare systems components. Similarly, Wani *et al.* (2020) investigated a few notable vulnerabilities in the hospitals connected to bring-your-own-device usage, the study reviewed the countermeasures to mitigate them. Still, they do not explicitly pinpoint the assets in the healthcare system targeted by the security threat and what business assets to protect. Sardi *et al.* (2020) explore the variety of existing security threats in healthcare facilities solely and briefly mention key assets. Still, they highlight the lack of risk assessment based on the specific needs of healthcare facilities and processes.

Some studies focus on controls to secure complex mobile, ubiquitous, and connected IoT healthcare systems. For example, Ahmadi *et al.* (2019), Iwaya *et al.* (2020) classified various countermeasures. However, they do not consider the context of such measures and do not describe how they can contribute to EHRs protection. At the same time, Yeng *et al.* (2021) present relatively complex security and privacy analysis of healthcare systems

by investigating what assets to protect in healthcare, their vulnerabilities, and countermeasures. Table 2 illustrates that most of the literature reviews similar to our previous work (Iqbal and Matulevičius, 2021b) present a rather limited scope of analysis. Also, it is noteworthy that only a few studies mention blockchain technology as a countermeasure to THAs' security threats. However, various organizations started working on BBHAs, for example, IBM-Blockchain (2022) is integrating blockchain in healthcare for better data sharing between healthcare providers without compromising data security, to overcome the drug counterfeiting (Martino *et al.*, 2019), and so on.

In recent years, ***blockchain technology*** has gained interest in the healthcare domain and researchers presented blockchain as a countermeasure solution to mitigate security threats of THAs. For example, Saha *et al.* (2019) present a comparative analysis of healthcare applications that use blockchain-based healthcare solutions to protect against data tampering and data leakage. The survey of Hathaliya and Tanwar (2020) addresses the security and privacy concerns in healthcare. The authors explore the timeline of security attacks on medical data and various traditional security algorithms to defend against them. The traditional security algorithms are shown to be ineffective, and blockchain is used as an advanced architecture for the safe and secure execution of medical transactions and to maintain the security and privacy of digital medical records.

Linn and Koo (2016) describe the fundamental principles of blockchain to address the security and privacy issues of THAs. The study also discusses the technical advantages of blockchain in healthcare (e.g. faster and easier interoperability). Randall *et al.* (2017) present the different use cases to address the security and interoperability challenges of THAs. Chukwu and Garg (2020) perform the SLR to explore the trust, security, and privacy constraints of traditional EHRs and how blockchain plays a role in overcoming them. The SLR of Agbo *et al.* (2019) investigates the security challenges, including how blockchain can protect medical data from potential data loss, corruption, or intentional security attacks. Jin *et al.* (2019) present blockchain in healthcare for secure and privacy-preserving medical data sharing. The study argues that blockchain's tamper-evidence and decentralization features could help build a secure medical data-sharing network.

The related works explore various security aspects without addressing vulnerabilities, what assets to protect, blockchain characteristics, and not adhering to any SRM domain model. Furthermore, the related works do not address the security threats and vulnerabilities that may arise in BBHAs. In contrast, we use the SRM domain model to analyse and compile the security threats of THAs and BBHAs. We also investigated the countermeasures to minimize them. To ease the SRM of healthcare applications, we provide an SRM domain model-based ontological framework (HealthOnt) that offers a dynamic knowledge base of security threats of THAs and BBHAs, vulnerabilities, assets to protect, and countermeasures to mitigate the security threats of both THAs and BBHAs.

2.4. *Back-Pain Patients' Healthcare Application Case*

In this section, we discuss a case of the back-pain patients' healthcare application that we used to evaluate the ontology. This application is operating at *Farhat Hached University Hospital in Sousse, Tunisia* to illustrate our proposal. The case scenario is shown in

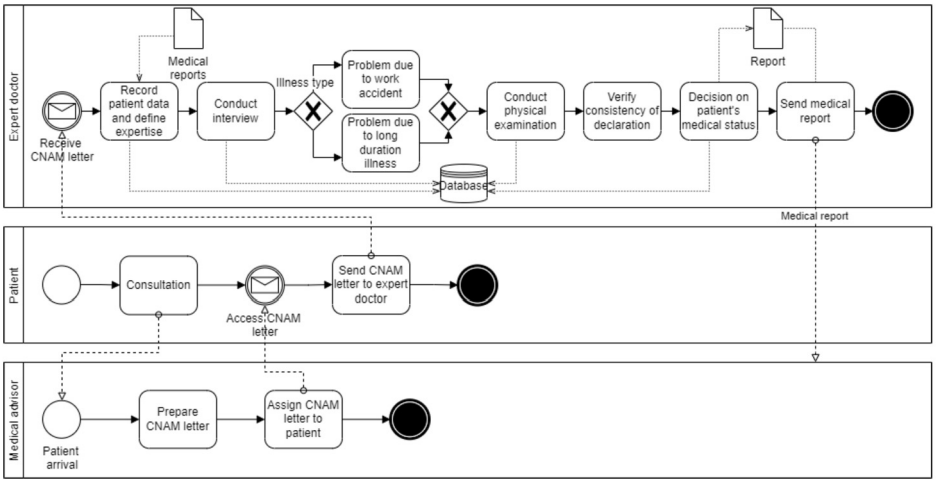

Fig. 1. Case of back-pain patients' healthcare application.

Fig. 1, where the main stakeholders are the medical advisor, patient, and expert doctor. The scenario starts when the patient contacts the medical advisor for consultation. After the appointment, the medical advisor prepares the CNAM letter[1] (including questions to the expert doctor) and attaches the necessary medical reports. The patient is then in charge of delivering the CNAM letter and the medical reports to the expert doctor. The expert doctor registers the patient's data and collects additional information during the interview in order to define illness type (e.g. work accident or long-duration illness). For example, during the interview, the expert doctor collects whether the patient suffers from low back-pain, the type of sciatica, whether the patient is diabetic, and also asks for the personal information (e.g. marital status, number of children, and the last job type). Thereafter, the expert doctor identifies the illness and studies the necessary documents related to either the work accident or the long-term illness.

Next, the expert doctor performs the patient's physical examination and records results (e.g. weight, height, build, limp, and gait). During the physical examination, the expert doctor can check and verify the consistency of the claim. Then, the expert doctor writes a conclusion based on the gathered data (e.g. on the patient's details, interview, and the physical examination outcomes). The expert doctor writes a medical report and sends it to the medical advisor. This report includes the conclusion about the patient's medical status and guides the medical advisor regarding the decision (e.g. whether the medical leave is needed, what is the duration of the medical leave, and when the patient could return to work). We will consider this back-pain patients' healthcare application case to illustrate the security threats and how they can be mitigated using blockchain technology.

[1] Caisse Nationale d'Assurance Maladie (*French*) – National Health Insurance Fund.

3. Security Threats Mitigated

In our previous work (Iqbal and Matulevičius, 2021b), we examine the literature studies that describe how blockchain can alleviate the security threats of THAs. We developed a framework (Table 3) using the SRM domain model and discussed the five security threats (*e.g. data tampering, data theft, medical records mishandling, counterfeit drugs, and man in the middle*) of THAs in detail. In this work, we provide the summary of those threats and other threats (*e.g. single-point failure, repudiation, insurance fraud, clinical trial fraud, tampering device settings, social engineering*) we discuss in detail. The framework describes THAs' security threats, vulnerabilities, assets to protect, blockchain-based countermeasures, and blockchain features that correspond to each countermeasure.

3.1. *Data Tampering*

THAs lack control over patients' data security (Xu *et al.*, 2019), which is a major concern for healthcare organizations. Blockchain provides various controls by design that can mitigate this threat. For example, smart contract-based distributed access control (Maesa *et al.*, 2017) regulates the users' access to stored medical data. Strong cryptographic primitives (Esposito *et al.*, 2018) help to build fine-grained access control. In a blockchain, the records are difficult to modify and delete due to the ledger redundancy and append-only structure (Dagher *et al.*, 2018). PoW consensus verifies transaction and data validation without a third party (Hussein *et al.*, 2018). Also, using the SHA-256 hashing, blockchain computes a unique hash id of original data to verify the authenticity of data (Han *et al.*, 2018). HLF uses trusted authorized nodes to verify and validate the authenticity of data (Chen *et al.*, 2018). Blockchain is tamper-evident (Han *et al.*, 2018) and thus detects any unauthorized modifications. Blockchain builds robust audit trails in an immutable ledger by keeping a record of each performed action (Bhuiyan *et al.*, 2018).

3.2. *Data Theft*

EHRs include confidential information that is attractive to cybercriminals that exploit various vulnerabilities in THAs to steal EHRs. In contrast, BBHAs are resistant to data theft. Blockchain works over a P2P network where nodes behave both as a server and client to send and receive data directly. This mechanism helps to protect the data leakage to unauthorized users (Chen *et al.*, 2018). Dagher *et al.* (2018) used the voting process (e.g. QuorumChain algorithm) to determine which nodes are allowed to access certain types of data. The permissioned blockchains define permission settings to restrict unauthorized data access (Han *et al.*, 2018). The strong cryptographic primitives (Esposito *et al.*, 2018) and smart contract-based distributed access control (Hussein *et al.*, 2018) allow only authorized users to access medical data. The ancile framework (Dagher *et al.*, 2018) uses the proxy re-encryption to store hashes of data on-chain and off-chain. In addition, Esposito *et al.* (2018) suggests data obfuscation to protect data on-chain and off-chain.

Table 3
Framework that presents security risk analysis of traditional healthcare applications.

Risk-related concept		Asset-related concept		Risk treatment concept	
Threat	Vulnerability	System asset	Business asset	Countermeasure	BC feature
Data tampering	Weak centralized access control mechanism	Healthcare database, Access control	Medical records (1), Patient data (C)	Distributed access control mechanism	Access control
				Access control with cryptographic primitives (e.g. attribute-based encryption)	
	No mechanism to verify and validate the authenticity of data	Healthcare database, Medical transactions	Medical records (1), Patient data (C), Data validation (1, A)	Distributed (shared) and append-only ledger	Distributed
				Proof of work-based consensus mechanism	Consensus
				Data validation without requiring third party	
				Unique hash id of original data	Cryptography
				HLF-based trusted authorized nodes	Permissioning
				Decentralized and tamper-resistant	Decentralized & Tamper-evident
				Immutable logging and data provenance	Provenance
Data theft	Improper security controls for centralized database	Healthcare system, Data access right	Healthcare database (1), Medical records (C)	Blockchain-based P2P network	Distributed
				Voting process to determine data access	Consensus
				Permissioned settings to restrict data access	Permissioning
				Access control with cryptographic primitives	Access control
	Weak centralized access control mechanism	Access control	Medical records (C)	Distributed access control mechanism to control data leak	
	No proper cryptographic controls	Healthcare system	Medical records (C)	Encrypts data and store on/off chain	Cryptography
				Store the encrypted and obfuscated data	
Medical records mishandling	Patients have weak control over their medical records	Data access right	Medical records (1, C)	Blockchain enables patients to control the access to their data	Permissioning
	Relying on a third-party	Healthcare database	Medical records (C)	Data validation without requiring third party	Decentralized
	No guarantee of electronic medical records authenticity			Decentralized and tamper-resistant	Decentralized & Tamper-evident
				Consensus mechanism	Consensus
Counterfeit drugs	Weak traceability controls in pharmaceutical supply chain	Drugs details, Supply chain	Drug traceability (1)	Immutable and traceable drug trails	Provenance & Immutability

(*continued on next page*)

Table 3
(*continued*)

Risk-related concept		Asset-related concept		Risk treatment concept	
Threat	Vulnerability	System asset	Business asset	Countermeasure	BC feature
Man in the middle attack	Weak controls to secure communication	Network, Data exchange	Communication (1)	Distributed IPFS for storage P2P-based encrypted communcation	Distributed & Cryptography
	Lack of anonymization of patient medical records	Healthcare system	Medical records (1, C)	Blockchain anonymize the data	Pseudo-anonymous
Single point failure	Relying on centralized server Weak implementation to handle large number of requests	Healthcare database and system	Server (A), Services (A)	Decentralized distributed P2P network	Decentralized & Distributed
Repudiation	Weak controls to prove illegal data changes by authorized users	Healthcare system	Medical records (1)	Blockchain-based versioning scheme to track each performed operation	Provenance & Immutability
	Lack of immutable logs	Action logs	Medical records (1)	Immutable log of all performed activities	
Insurance fraud	No proper authenticity to verify the insurance claim	Medical bills, Insurance data	Insurance claim (1)	Decentralized verification of insurers Verified records are distributed among nodes	Permissioning Distributed
Clinical trial fraud	Inadequate clinical trials data Improper patient recruitment and lack of data access	Clinical trial data, Data access right	Data processing (1, C)	Distributed nature and use of cryptography Blockchain provides data ownership Data saved on blockchain cannot be altered	Cryptography Permissioning Immutability
Tampering device settings	Weak controls on settings of medical devices	IoT devices	Device settings (1, A)	Storing devices settings in distributed immutable ledger	Immutability
Social engineering	Possible to manipulate employess to get data access	Employees, Stakeholders	Medical records (1)	Only relevant employees have access to particular information or part of information	Permissioning

3.3. *Medical Record Mishandling*

Healthcare institutions must guarantee that medical records are kept confidential and secure. In THAs, the medical institutions control and manage the patient's medical data where the non-relevant individuals can access it. BBHAs enable permission settings and distributed access control to handle patients' medical data (Yaqoob *et al.*, 2021). Also, blockchain performs data validation before saving on the ledger during the consensus

process. For example, blockchain defines data validation rules which are agreed upon by other network nodes (Dexter, 2018). Thus, all the nodes follow those rules to validate the data and discard all the unauthorized changes (Shi *et al.*, 2020).

3.4. *Counterfeit Drugs (Fake Medicine)*

The creation and distribution of counterfeit pharmaceuticals is a global problem with significant health and economic consequences, primarily for consumers (Martino *et al.*, 2019). According to Yaqoob *et al.* (2021), 10–30% (worth $200 billion) of drugs sold worldwide each year are counterfeit, posing significant health risks. Blockchain offers a solution to enable pharmaceutical traceability, real-time access to data, and supply chain validation by creating a log to track each step (Narikimilli *et al.*, 2020; Yaqoob *et al.*, 2021; Martino *et al.*, 2019). For example, IBM Research uses blockchain to reduce or eliminate the drug counterfeiting problems in Kenya (Martino *et al.*, 2019) by using immutable and traceable logs at each stage of the pharmaceutical supply chain.

3.5. *Man in the Middle (MitM) Attack*

According to SpecOpsSoft (2020), MitM attacks are rising in healthcare applications to gain or manipulate sensitive information. Xu *et al.* (2019) introduce the blockchain-based distributed interplanetary file system (IPFS) for storage to establish a secure communication channel. Blockchain works on a P2P network that makes it hard for an attacker to intercept the communication, data analysis, or sniffing (Chen *et al.*, 2018). Blockchain maintains pseudo-anonymity, for example, the patients and their medical data are linked with a cryptographic hash. Also, the data processing in a blockchain is anonymous (Yaqoob *et al.*, 2021) that hides the actual identity from patients' medical data (Ali *et al.*, 2020).

3.6. *Single Point Failure*

Like any other system, the attacker can find faults in the system's design, implementation, or centralized dependency components to disrupt the healthcare services.

Vulnerabilities: Currently, the healthcare system uses a *centralized server model* (Xu *et al.*, 2019) that can pose a threat of single-point failure and performance bottleneck. The *weak mechanism to handle large numbers of requests* (Shi *et al.*, 2020) allows the attacker to target the server and services of the system to halt them for legit users.

Countermeasures: Blockchain is resilient to this threat with the advantage of a decentralized distributed P2P network (Narikimilli *et al.*, 2020). Moreover, blockchains do not rely on a single or central point server (Xu *et al.*, 2019; Shi *et al.*, 2020).

3.7. *Repudiation*

The patient's medical data is sensitive and life-critical. The healthcare system should trace all actions performed (intentionally or unintentionally) by the authorized users on a patient's medical data and easily identify how it was performed.

Vulnerabilities: In THAs, there are *weak controls to prove illegal data changes by authorized users* (Kleinaki *et al.*, 2018). For example, almost every stakeholder within a medical institution has access to the patient's medical data that can be viewed, modified, or deleted. Moreover, unintentional data changes can happen that later are not traceable during data processing. The THAs manage *centralized and mutable logs* (Griggs *et al.*, 2018) that are handled (or have access) by a system administrator or other IT staff. Also, if the system is compromised, the attacker can easily remove the actions he performed from logs. Therefore, the authenticity of logs can not be proved on centralized systems.

Countermeasures: Blockchain keeps immutable logs (Griggs *et al.*, 2018) to track who and when the particular operation was performed. Also, Kleinaki *et al.* (2018) use the blockchain-based versioning scheme to track each performed operation over time.

3.8. *Insurance Fraud*

Healthcare insurance frauds are increasing, which involves the filing of dishonest healthcare claims. For example, the value of challenged healthcare claims surged from $11 billion to $54 billion annually (Narikimilli *et al.*, 2020).

Vulnerabilities: In THAs, there is a *lack of proper authenticity* (Martino *et al.*, 2019) to verify the insurance claim because of complex information systems, administrative burdens, expensive & manual validation and verification of provider directories, and record-keeping mistakes that attracts the attackers.

Countermeasures: The blockchain enables the decentralized verification of insurers based on the predefined set of rules (Martino *et al.*, 2019) before registering on the ledger. Once the insurer is verified and registered, the records are distributed among other nodes to keep track of valid and invalid insurers in the system.

3.9. *Clinical Trial Fraud*

Reproducible data is the lifeblood of advanced research across the globe. Currently, the healthcare institutions and research groups suffering from clinical trial frauds (George and Buyse, 2015) and medical decisions made by researchers on the premise of fraudulent data could leave patients at risk.

Vulnerabilities: The data frauds in clinical trials include deliberate fabrication, falsification, or plagiarism in proposing, performing, or reviewing research and research results (George and Buyse, 2015). The *inadequate clinical trial data* (Martino *et al.*, 2019) emerge due to a lack of data integrity and provenance. Also, the current infrastructure has *inefficiencies in patient recruitment and access to medical data* (Narikimilli *et al.*, 2020).

Countermeasures: The distributed nature and use of cryptography ensure data is authentic (Martino *et al.*, 2019). Also, blockchain provides data ownership to patients (Dagher *et al.*, 2018) to control the access of their data and once data is saved on the blockchain, it cannot be altered. Thus, eliminating the threat of clinical trial fraud.

3.10. *Tampering Device Settings*

Medical devices connected to the internet and the internet of things (IoT) enable healthcare professionals to be more watchful and connected with the patients. Progressively, IoTs are becoming the heart of digital healthcare, but new security challenges are appearing.

Vulnerabilities: In healthcare, the *medical devices are subject to heedless settings* (McGhin *et al.*, 2019) (e.g. lack of network segmentation, insufficient access control, and reliance on legacy systems). The intentional changes in device settings (e.g. from the attacker) or unintentional changes (e.g. from the authorized user) can lead to false readings that put the patient's life in danger.

Countermeasures: Blockchain follows the append-only structure to save data. Thus, device settings stored in blockchain are distributed and immutable (McGhin *et al.*, 2019).

3.11. *Social Engineering*

According to HelpNetSecurity (2019), only 1% of cyber-attacks in the year 2019 were exploited due to hardware or software vulnerabilities, and 99% of cyber-attacks utilized some form of human intervention (e.g. phishing, fake identity, honey trap, etc).

Vulnerabilities: In healthcare, the healthcare staff is one of the weakest points and the attackers use *social engineering techniques* (Ali *et al.*, 2020) to target them to get patients' medical data. Healthcare staff is vulnerable to social engineers because they naturally trust others, do not want to be rude, have a desire to be helpful, and find it difficult to remember everyone in a large healthcare environment (SecurityMetrics, 2015).

Countermeasures: Maesa *et al.* (2017); Dagher *et al.* (2018) implement smart contract-based distributed access control that ensures only relevant users have access to particular information or part of the information. Thus, protecting medical data against unauthorized user access. However, the threat of social engineering can not be eliminated through new technology or a more secure password, but it can be restricted to an acceptable level by proper training of employees (SecurityMetrics, 2015).

The security risk analysis of traditional healthcare applications shows that blockchain can help the healthcare sector to overcome the security threats of traditional technology infrastructure for preserving the medical data, data integrity, and patient ownership of their data. We use the constructs of the SRM domain model that fulfills the criteria of ISO/IEC 27001 standard (Ganji *et al.*, 2019) for defining the scope of our work and to assist in building a framework for structuring the security risk analysis of traditional and blockchain-based healthcare applications. This framework (Table 3) presents blockchain as a countermeasure solution for mitigating the security threats of THAs. Blockchain provides technology infrastructure with unique characteristics for building healthcare applications. For example, blockchain operates over a P2P network, uses consensus mechanism and cryptography, is immutable, decentralized, tamper-evident, and provides permission settings, provenance, and pseudo-anonymity. However, we cannot deny the security aspects of BBHAs because in recent years various security threats have appeared in blockchain-based solutions. Hence, we discuss such security threats in the next section.

4. Security Threats Appeared

We analyse the literature studies that describe security threats to BBHAs. We identify those security threats and categorize them using the SRM domain model and develop a framework (Table 4). The framework illustrates the BBHAs' security threats, vulnerabilities, assets to protect, countermeasures, and corresponding countermeasure strategies. In this section, we discuss the security threats in detail.

4.1. *Sybil Attack*

Sybil attack is a P2P network attack (Douceur, 2002) where the attacker creates numerous fake identities and connects with victim nodes to isolate them from other honest nodes.

Vulnerabilities: Blockchain systems run over the P2P network, and therefore they are susceptible to Sybil attack. The attacker can control several nodes on BBHAs by *creating fake identities* (Iqbal and Matulevičius, 2021a; Rahmadika and Rhee, 2018) to gain disproportionately large influence. Once Sybil nodes gain recognition, the attacker forces victim nodes to process blocks under his control, out-votes (or blocks) the honest nodes, interrupts the flow of information, distorts the block generation process, and refuses to receive or transmit information (Zhang and Lee, 2019). Also, if the blockchain system has *insufficient computing-power* (Sayeed and Marco-Gisbert, 2019), the attacker with higher computing power exploits this limitation by using Sybil nodes and disrupting the healthcare operations. Moreover, the *poor implementation of node authentication* (Swathi *et al.*, 2019) (e.g. no network joining fee, not validating IP address, or source of node connection) negates the integrity of the transaction verification process.

Countermeasures: To overcome Sybil attacks in BBHAs, incorporate network joining fee (Swathi *et al.*, 2019) and stake requirements in PoS consensus (Banchhor *et al.*, 2021) to make identity creation more expensive. Monitor node behaviour (Swathi *et al.*, 2019) to spot any unusual activity of nodes and disconnect them from the network. If the system uses PoW consensus, the network should have enough computational power (Sayeed and Marco-Gisbert, 2019) based on the network's available nodes. Regularly monitor the computing power to ensure no one is misusing it. In addition, before joining the blockchain network, perform node authentication. For instance, requesting a network joining fee, validating node connections, and monitoring node activities (Swathi *et al.*, 2019).

4.2. *Double-spending*

The double-spending is categorized under data consistency attack (Nicolas *et al.*, 2021) to spend the same transaction twice (Pérez-Solà *et al.*, 2019). Similarly, in BBHAs, the attacker can change the transaction state and spend the same transaction twice.

Vulnerabilities: The attacker uses *51% or more computing-power* to control the network (Ratta *et al.*, 2021) to weaken the P2P network to perform double-spending (e.g. insurance frauds) (Iqbal and Matulevičius, 2021a). This vulnerability can also affect the availability of network resources, the attacker can trigger selfish-mining, prevent new transactions

Table 4
Framework that presents security risk analysis of blockchain-based healthcare applications.

Risk-related concept		Asset-related concept		Risk treatment concept	
Threat	Vulnerability	System asset	Business asset	Countermeasure	Strategy
Sybil attack	Possible to create fake identities in the network	Nodes (miners). Nodes identity, P2P Network, Transactions	New nodes (A), Information flow (A), Ledger (I, A), Block generation (A)	Network joining fee	Detection
				Monitor nodes behaviour	Monitoring
				Stake requirements in PoS consensus	Inform
	Lack of computing power	Nodes, P2P Network, Computing power	Network reputation (I), Healthcare operations (A)	Increase computing power	Detection
				Monitor computing power	Monitoring
	No proper authentication of nodes	Nodes, P2P Network, Network reputation, Transactions	Transaction validation (I)	Network joining fee	Detection
				Validating node connection	Detection
				Monitor nodes behaviour	Monitoring
Double-spending	51% vulnerability	Computing power, Nodes (miners), P2P network	Transaction (I), Ledger (I), Network resources (A)	Insert observers	Conceptual
				Use power monitoring tool	Monitoring
				Transaction fee	Inform
				Pluggable consensus	Conceptual
	Accepting unconfirmed transactions	Transactions, Block confirmations	Fast transaction (I, A), Digital assets (I), Ledger (I)	Increase confirmed blocks	Detection
				Closed-form formula probability	Conceptual
				Enhance network policy	Inform
				Listening period	Conceptual
				Insert observers	Monitoring
				Alerting honest nodes	Broadcasting
Eclipse attack	Poisoning nodes' routing table	Nodes, IP addresses, Node connection. Transactions, Routing table	Communicating/ gossiping (A), Transaction validation (I), Transaction (I), Medical data (C, I)	Disable direct incoming connections	Inform
				White-listed nodes	Forwarding
				Random outgoing connections	Conceptual
				Deterministic random eviction	Detection
				Incorporate feeler and anchor connections	Inform
Smart contracts attacks	Faulty and error-prone smart contracts	Smart contracts, Transaction validation, Ledger	Digital assets (I), Transaction (I), Medical data (C, I, A)	Smart contracts code analysers (e.g. SmartCheck)	Detection
				Penetration testing tool	Detection
Block withholding delay	Possible to delay the submission of valid blocks	Transaction validation, Blocks, Mining incentives	Medical operations (A) Information processing (A), Block confirmations (A)	Enforce immediate block submission scheme	Conceptual
				Increase risk of earning less incentives	Inform

(*continued on next page*)

Table 4
(*continued*)

Risk-related concept		Asset-related concept		Risk treatment concept	
Threat	Vulnerability	System asset	Business asset	Countermeasure	Strategy
Sybil-based DoS	Sybil nodes can participate in the consensus mechanism	Nodes, P2P network, Mining protocol	Medical operations (A) Mining process (A)	Use computational constraint-based techniques	Conceptual
	Dusting transactions	Transactions, P2P network, Ledger	Medical operations (A) Network resources (A)	Anti-dust model	Detection
Deanonymization attack	Network analysis and listening	Transactions. Medical data	Medical dala (C)	Use mixing techniques	Broadcasting
				Use anonymity uveilay nelwoiks (e.g. Toi)	Conceptual
				Ring signatures and zero-knowledge Proofs	Detection
Quantum computing threats	Not using quantum-resistant cryptography schemes	Cryptography, Ledger	Transactions (I), Ledger (I), Medical data (C, I)	Quantum computing resistant cryptography	Conceptual
Endpoint security threats	Lack of awareness and knowledge	Wallets, Keys, Computers/devices, User	Healthcare services (A), Digital assets (I), Medical data (C, I, A)	Multi-level authentication (MLA) method	Detection
				Security awareness	Inform
				Hardware security module (HSM)	Detection

from gaining confirmations, and blockchain forks (El-Gazzar and Stendal, 2020). However, this vulnerability is practically impossible on high computing power blockchains (e.g. Bitcoin and Ethereum) (Iqbal and Matulevičius, 2021a). Moreover, *accepting unconfirmed transactions* (Pérez-Solà *et al.*, 2019) enables the attacker to indulge in a race to make his double-spend transaction valid by exploiting the intermediate time between two conflicting transactions and using a higher transaction fee. If it is successful, it negates the integrity and availability of fast transaction mechanisms and the loss of digital assets (such as insurance claims) and the ledger's integrity.

Countermeasures: Implement a power monitoring tool to monitor the computing power of nodes continuously and restrict when reaching a certain amount of computing-power (Alcarria *et al.*, 2018). Also, incorporate transaction fee (Jonathan and Sari, 2019) as an incentive to keep nodes honest in a blockchain system. Use a pluggable consensus mechanism (Dinh *et al.*, 2017) to facilitate consensus diversity based on the blockchain system's requirements. Furthermore, Rosenfeld (2014) states that increasing the number of confirmed blocks would decrease the double-spending threat. Grunspan and Perez-Maro (2018) present a closed-form formula to calculate the likelihood of double-spending in a race attack. In addition, enhance network policy (Nicolas *et al.*, 2021) to guide about how to set a block confirmation number considering the value of the transaction.

4.3. *Eclipse Attack*

In an eclipse attack, the attacker takes control of all the neighbuoring peers of the victim node and hides the correct ledger from the victim node (Rahmadika and Rhee, 2018).

Vulnerabilities: Eclipse attack targets particular node (Zhang and Lee, 2019) by flooding with his IP addresses. The attacker *poisons victim node's routing table* (Rahmadika and Rhee, 2018) by filling it with his IP addresses. Once the node restarts, it loses its current outgoing and incoming connections and makes the new connections with the attacker's IP addresses. If the attack is successful, the attacker inhibits the victim node from learning about the rest of the blockchain network by preventing it from communicating with other peer nodes, disrupting the transaction verification process, and gaining access to the medical data. Moreover, this attack allows the attacker to alter transactions to perform double-spending and selfish mining (Rahmadika and Rhee, 2018).

Countermeasures: The first countermeasure is to stop direct incoming connections (Henningsen *et al.*, 2019; Heilman *et al.*, 2015) and make incoming and outgoing connections via white-listed nodes (Heilman *et al.*, 2015), such as well-connected peers/miners, to prevent the eclipse attack. Also, include a random outgoing connections method (Henningsen *et al.*, 2019) to prohibit all connections with the attacker's IP addresses. Use deterministic random eviction (Heilman *et al.*, 2015) to keep track of new and tried connections. It minimizes the number of attack addresses used by the attacker when making connections. Moreover, the feeler connections (Heilman *et al.*, 2015) to make short-lived test connections with randomly-selected addresses. If the connection is successful, the address includes in white-listed nodes. The anchor table method (Heilman *et al.*, 2015) allows to keep track of current outgoing connections, and when the node restarts, it selects and makes a connection with the old addresses from the anchor table.

4.4. *Smart Contracts Attacks*

The security of smart contracts has become a major concern in recent years (Singh *et al.*, 2021) as a result of different security issues originating in blockchain-based applications from the execution of smart contracts.

Vulnerabilities: The security issues in smart contracts are associated with the bugs in the source code (*e.g. transaction-ordering dependency, timestamp dependency, mishandled exceptions, reentrancy, unpredictable state, transaction overflow, and underflow, etc.*) (Singh *et al.*, 2021; Sayeed *et al.*, 2020). According to Li *et al.* (2020), in Ethereum around 45% smart contracts are vulnerable and the attacker can exploit *faulty and error-prone smart contracts* (Sayeed *et al.*, 2020) to harm the valuable assets in BBHAs. For example, Ethereum smart contract reentrancy attack on the decentralized autonomous organization (DAO) when the attacker stole $60 million Ethers (Singh *et al.*, 2021). Many blockchain platforms are introducing smart contracts to construct decentralized applications, but their security has yet to be fully studied (Sayeed *et al.*, 2020). In BBHAs, the attacker can exploit these vulnerabilities and target the digital assets, steal or modify the medical data, and interrupt the medical operations (Musamih *et al.*, 2021).

Countermeasures: The developers should employ smart contract code analysers to discover flaws, race situations, and sanitize the smart contract code before deploying it on a blockchain. For example, the SmartCheck (Musamih *et al.*, 2021) to detect vulnerabilities in the smart contract at different severity levels, Oyente tool (Musamih *et al.*, 2021) to detect callstack depth and re-entrancy attacks. On top of these, use penetration testing tool (Bhardwaj *et al.*, 2021) to test blockchain-based applications before deployment.

4.5. *Block Withholding Delay*

In PoW-based blockchains, a block withholding delay is common. The attacker miner joins a victim mining pool and refuses to submit blocks on time (Liu *et al.*, 2019).

Vulnerabilities: The attacker miners deliberately *delay the submission of valid blocks* (Liu *et al.*, 2019) that results in the discarding of the blocks that can distort the operations of BBHAs. Also, the strategy leads the attacker to gain higher rewards than honest mining nodes (Tosh *et al.*, 2017). In BBHAs, this attack can hinder medical operations and delay block confirmations needed for the transaction finality.

Countermeasures: To mitigate this attack, the system should enforce an immediate block submission (Guru *et al.*, 2021) to submit the block as soon as it is found. Moreover, implement an incentive payoff scheme (Liu *et al.*, 2019) to increase the risk of earning fewer incentives to demotivate those who deliberately delay block submissions.

4.6. *Sybil-Based DoS*

Blockchain-based applications operate over a P2P network. Despite being operated on a P2P network, they are still vulnerable to DoS attacks (Guru *et al.*, 2021).

Vulnerabilities: By design, permissionless blockchains let anybody participate in the consensus process. The attacker takes advantage of this situation by *participating in the consensus with his Sybil nodes* (Quintyne-Collins, 2019) to postpone medical operations and interrupt the mining process. Also, the attacker creates numerous *dust transactions* (Wang *et al.*, 2018) between his Sybil nodes, and blockchains process a limited number of transactions per block in a given time. The Sybil nodes participating in the consensus do not share their verified transactions or blocks. Thus, the large number of transactions with small values congest the blockchain network (Iqbal and Matulevičius, 2021a), delay the medical operations, exhaust the network resources, and halt the mining process.

Countermeasures: The Sybil-based DoS attacks cannot be mitigated entirely but it is possible to restrict them. For example, incorporate computational constraint-based Sybil resistance techniques like Bitcoin uses PoW (Quintyne-Collins, 2019). Moreover, utilize the anti-dust model (Wang *et al.*, 2018) that checks different parameters in the transaction (e.g. transaction volume and fees) to identify and prevent dust attacks (Wang *et al.*, 2018).

4.7. *Deanonymization Attack*

Anonymization is a characteristic of blockchains that refers to hiding an identity, but still possible to link a user or company behind each transaction (Quintyne-Collins, 2019).

Vulnerabilities: Patients' privacy is the utmost requirement in healthcare. However, in BBHAs, it is possible to identify the patient by performing *network analysis and listening* (Junejo *et al.*, 2020; Biryukov and Tikhomirov, 2019). For example, analysing the transaction contents, transaction relationship with other transactions, and the way the transaction is broadcasted. Moreover, the attacker can perform graph analysis (Junejo *et al.*, 2020) on publicly available transactions to deanonymize the identities of patients.

Countermeasures: Narayanan *et al.* (2016) use the mixers as a service to enhance the privacy and anonymity of transactions by obfuscating the transaction flow. Biryukov and Tikhomirov (2019) suggests using anonymity overlay networks such as Tor. Moreover, incorporate ring signatures and zero-knowledge proofs (Junejo *et al.*, 2020) to achieve the required level of privacy on medical data, and users get only relevant information.

4.8. *Quantum Computing Threats*

Quantum computing research is advancing, and many cryptographic protocols in use currently are vulnerable to quantum computing (Shankland, 2021). Blockchain platforms rely on cryptographic protocols that are also vulnerable to quantum computing.

Vulnerabilities: The quantum computing threat is real, and blockchain platforms are *not using quantum-resistant cryptography* (Yaqoob *et al.*, 2021; Velissarios *et al.*, 2019) to tackle it. Thus, the BBHAs are vulnerable to quantum computing (Gao *et al.*, 2018) in a post-quantum era. For example, blockchain platforms are using an elliptic curve digital algorithm (ECDSA) that is not a quantum-resistant cryptography scheme, and it could be solved by quantum computers (Gao *et al.*, 2018).

Countermeasures: The blockchains should implement quantum computing resistant cryptography schemes (*e.g. lattice-based, multivariate, hash-based, code-based cryptography*) (Yin *et al.*, 2018). For example, Yin *et al.* (2018) implemented the anti-quantum transaction authentication scheme using lattice-based cryptography. Gao *et al.* (2018) present the post-quantum blockchain using a lattice-based delegation algorithm.

4.9. *Endpoint Vulnerability*

The easy way of attacking technology solutions is through endpoint vulnerabilities, which occur where humans and technology interact (Velissarios *et al.*, 2019). Hence, the protection of endpoints is paramount in BBHAs (Velissarios *et al.*, 2019).

Vulnerabilities: The attacker coerces the victim through social engineering or phishing into using numerous strategies that are under his control (Radhakrishnan *et al.*, 2019). For example, the flawed key generations and signatures tool exposes users' private keys. Moreover, the *lack of awareness and knowledge* about security could trigger the endpoint vulnerability (Velissarios *et al.*, 2019). For example, if the attacker learns about the private key, he can utilize it to acquire access and ownership of data. Anyway, endpoint vulnerabilities remain susceptible through social engineering, real-world theft, or physical access to user wallets, phones, or computers (Velissarios *et al.*, 2019).

Table 5
Security threats not yet investigated in blockchain-based healthcare applications but may appear.

Threat	Detail
BGP hijacking	The attacker can intercept the blockchain network by manipulating the border gateway protocol (BGP), after which data can be routed, and the traffic can be modified in the attacker's favour (Singh *et al.*, 2021).
Liveness attack	This attack can delay the transaction confirmation time and proceeds in three stages: preparation (build private chain), transaction denial (delay the genuine block), and blockchain delay (decrease the rate at which the chain transaction grows) (Singh *et al.*, 2021).
Timejacking	Timejacking exploits the handling of blockchains' timestamps. The attacker can forge or broadcast a false timestamp of a transaction when connecting to a network node allowing him to change the node's network time and trick it into accepting an alternative blockchain. This attack can cause a double-spending (Guru *et al.*, 2021).
Blockchain poisoning	The attacker adds stolen data (e.g. addresses, credit card numbers), illegal files (e.g. malware), and malicious content and force blockchain nodes to download such content (Banchhor *et al.*, 2021). Blockchain poisoning can lead to DoS or DDoS attacks or disrupt the operations of a blockchain network.
Transaction malleability	The attacker alters the transaction signature responsible for generating unique identifiers of the transaction. The attacker changes the transaction identifier before the transaction confirmation on the network to pretend the transaction did not happen. This technique causes the victim to pay twice (Banchhor *et al.*, 2021; Guru *et al.*, 2021).
Selfish mining	This attack happens on mining pools to earn extra mining rewards. The attacker holds a mined block in his private chain. Once his chain is longer, he broadcasts the blocks in the network at once and makes other miners lose their blocks. The purpose of selfish mining is to waste the efforts and rewards of honest miners (Banchhor *et al.*, 2021; Liu *et al.*, 2019).
Balance attack	Balance attack combines mining power with communication delay to affect fork-able blockchains (e.g. Ethereum). The attacker isolates a blockchain branch from one subgroup and convinces another competing subgroup to influence the branch selection process. This successful attack can lead to a double-spending (Singh *et al.*, 2021).
Race attacks	In race attacks, the attacker sends two or more conflicting transactions in the network and exploits the fast transaction mechanism where the merchant (a victim) accepts a transaction with 0 confirmations (Rahmadika and Rhee, 2018).

Countermeasures: To minimize endpoint vulnerabilities, implement a multi-level authentication method (Radhakrishnan *et al.*, 2019) when accessing wallets or generating wallet keys, use multi-signature wallets, cold wallets, and do not share private keys of wallets with anyone. Users should be aware of social engineering, always use authentic and legitimate sources to protect against phishing, and utilize hardware security modules (Radhakrishnan *et al.*, 2019; Velissarios *et al.*, 2019).

4.10. *Other Security Threats*

In this section, we outline numerous possible security threats of blockchain systems (Table 5) that have yet to be studied in BBHAs but may appear. Therefore, blockchain developers and practitioners should be aware of these security threats.

We build this framework (Table 4) aiming to provide the details about the security threats that may appear in BBHAs, and the controls to mitigate them. Both frameworks (Tables 3 and 4) complement one another in the context of the SRM constructs we used. However, the aforementioned frameworks represent the knowledge base in a static manner

and are difficult to update when new security threats, vulnerabilities, or countermeasures appear. To overcome these issues, we build a blockchain-based healthcare security ontology, HealthOnt, where these frameworks serve as a foundation.

5. Healthcare Security Ontology

Ontology is a collection of concepts and their relationships (Herzog *et al.*, 2007). To avoid the repercussions of a misunderstanding, ontology elaborates the meaning of concepts within a domain (Kang and Liang, 2013). In the security domain, ontology is frequently used to systematically classify security risks, preventative measures, and associated security implementation technologies (Kang and Liang, 2013). Furthermore, the Noy and McGuinness (2001) illustrate the reasons that motivate the development of an ontology. For instance, ontology makes it possible to i) share a common understanding, ii) reuse of domain knowledge, iii) make domain assumptions explicit, iv) separate domain and operational knowledge, and v) analyse domain knowledge. As a result, we present HealthOnt[2] which is available online[3] and encapsulates security threats of THAs and BBHAs.

HealthOnt is based on web ontology language (OWL) and WWW Consortium (W3C). OWL is a semantic web language based on description logic (DL) to illustrate rich and complex knowledge about things (e.g. concepts), groups of things, and their relations. OWL supports a resource descriptive framework (RDF) to define a metadata model to build a readable semantic infrastructure (Hector and Boris, 2020). RDF supports triplet format (e.g. subject-predicate-object) for describing the ontology concepts. For example, in this triplet *(DataTampering **exploits** ErrorProneAuthenticityOfData)*, *DataTampering* threat is a **subject**, *exploits* is a relation that represent a **predicate** and *ErrorProneAuthenticityOfData* vulnerability is an **object**. To get results from an ontology, we use SPARQL (SPARQL Protocol and RDF Query Language) as a semantic query language.

We utilize the *ontology construction method* (Uschold and Gruninger, 1996) and this approach has also been applied in Iqbal and Matulevičius (2020) to build an ontology for security threats of Corda-based financial applications. We start the ontology building process by identifying its purpose and scope. Second, we collect the domain information (e.g. concepts and relations) and categorize it in the frameworks (Tables 3 and 4). This process refines the concepts and improves the technical domain language related to assets, security criteria, threats, vulnerabilities, and countermeasures. Thereby, the frameworks provide a coherent structure and required level of understanding for a successful implementation of HealthOnt. Third, we used Protege[4] to formalize the domain knowledge in our ontology by coding the concepts and relations. Our previous work (Iqbal and Matulevičius, 2021b) presents the details related to the ontology construction.

[2] https://github.com/mubashar-iqbal/HealthOnt
[3] https://mmisw.org/ont/~mubashar/HealthOnt
[4] https://protege.stanford.edu

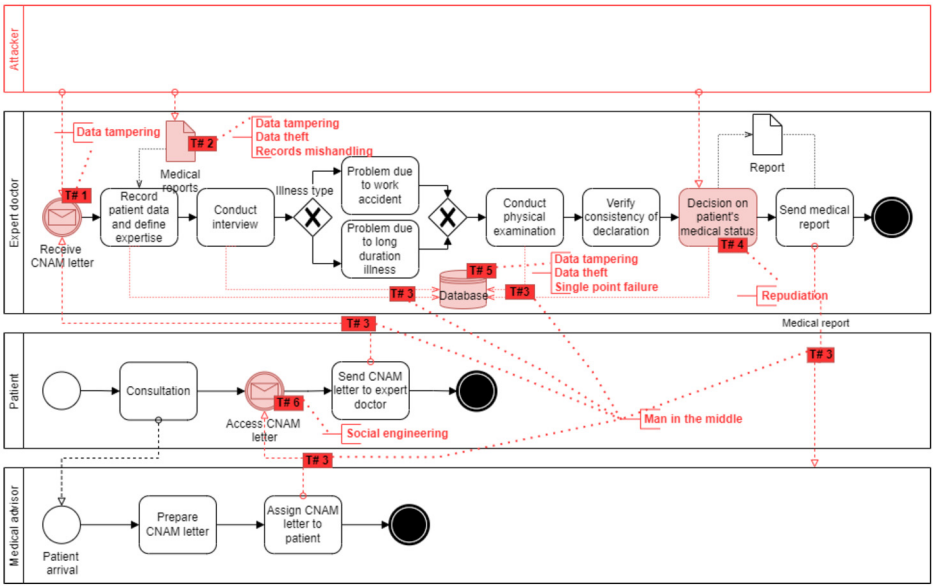

Fig. 2. Mapping of security threats that can appear in traditional BPPHA using HealthOnt.

6. Ontology Validation

Ontology validation is important to ensure the correctness of ontology, the meaning of ontological reasoning, and the effective use of an ontology (Steiner and Albert, 2017). In (Iqbal and Matulevičius, 2021b), we use the qualitative assessment criteria (Raad and Cruz, 2015) to validate the HealthOnt. This approach helps in the early phases to check whether the coded concepts model the real-world domain for which the ontology is built. The qualitative assessment criteria contribute to the quality of ontology, but it does not address how good the developed ontology is? To answer this question, we use a back-pain patient's healthcare journey to map the coded knowledge of healthcare security.

6.1. *Analysis of the Back-Pain Patients' Healthcare Application Case*

We use HealthOnt to map the healthcare applications' security knowledge on a back-pain patients' healthcare application (BPPHA), described in Section 2.4. HealthOnt helps to identify the security threats of it that are highlighted as threat points in Fig. 2.

Threat Point 1: Due to the weak access control mechanism to share CNAM letter, the unauthorized user can get access and tamper it. Also, the patient can intentionally or unintentionally tamper the CNAM letter. In both cases, the system does not have a proper mechanism to verify and validate the legitimacy of the CNAM letter.

Threat Point 2: The data tampering can happen on medical reports due to weak centralized access control. Thus, an unauthorized user can access the patient's medical reports

and tamper them. In the current system, the medical reports are stored in human-readable formats (e.g. PDF, docs, Xrays), and no proper cryptographic controls (e.g. encryption) are implemented. The attacker can access them to pursue various activities (e.g. insurance frauds, wrong drug prescriptions). The data theft undermines the confidentiality of medical reports and patient privacy, eventually jeopardizing the integrity and trust of the system. Furthermore, the patients have weak control over their medical reports. For example, medical institutions control and manage the patient's medical data where non-relevant individuals can access and manipulate it. Thus, the current BPPHA does not guarantee the authenticity of electronic medical reports.

Threat Point 3: The attacker can exploit the weak controls of secure communication to get medical records, medical reports, and CNAM letter. Moreover, due to the lack of anonymization of patient medical records, the medical data is associated directly with patient identity. With the MitM, the attacker can sniff the data to pursue various activities (e.g. publishing the data online or ransomware attack). The MitM attack can affect the data exchange, medical records, medical reports, CNAM letter, and communication assets.

Threat Point 4: The patient's medical data is life-critical, and the healthcare system should trace all actions performed (either intentionally or unintentionally). The BPPHA does not use immutable logs to maintain track of all actions taken on a patient's medical data over time. As a result, the existing system lacks a means for proving intentional or unintentional modifications to a decision of a patient's medical status.

Threat Point 5: Weak centralized access control refers to a situation in which the system fails to prevent unauthorized access to the database. The attacker breaches security and performs unauthorized actions that negate the integrity of medical records and healthcare database. Currently, the BPPHA does not have any security or cryptography controls to protect the database from data theft attacks. Overall, this threat negates the confidentiality of medical records, healthcare database, and patient privacy. Also, the BPPHA has a centralized database server and network services. The attacker can locate the flaw in the design or implementation of the systems and cause database overhead or disables the medical services, essentially shutting down the whole system.

Threat Point 6: BPPHA is also vulnerable to social engineering, where patients and hospital personnel are the weakest links. The attacker can target them using social engineering tactics (e.g. phishing, false identity, honey trap) to get the CNAM letter.

6.2. *Blockchain as a Countermeasure Solution*

We present blockchain as a countermeasure solution (Fig. 3) to illustrate the blockchain-based BPPHA that implements various security controls by design and mitigates security threats of traditional BPPHA. For example, the blockchain-based role-based access control (RBAC) can restrict access to the CNAM letter. Blockchain provides a consensus mechanism to verify and validate the CNAM letter transaction without requiring a third party, a unique hash id of the original CNAM letter stored in the blockchain to verify its authenticity, and an immutable ledger to keep track of each performed action. Similarly, medical reports can be protected against data tampering using RBAC and blockchain-based

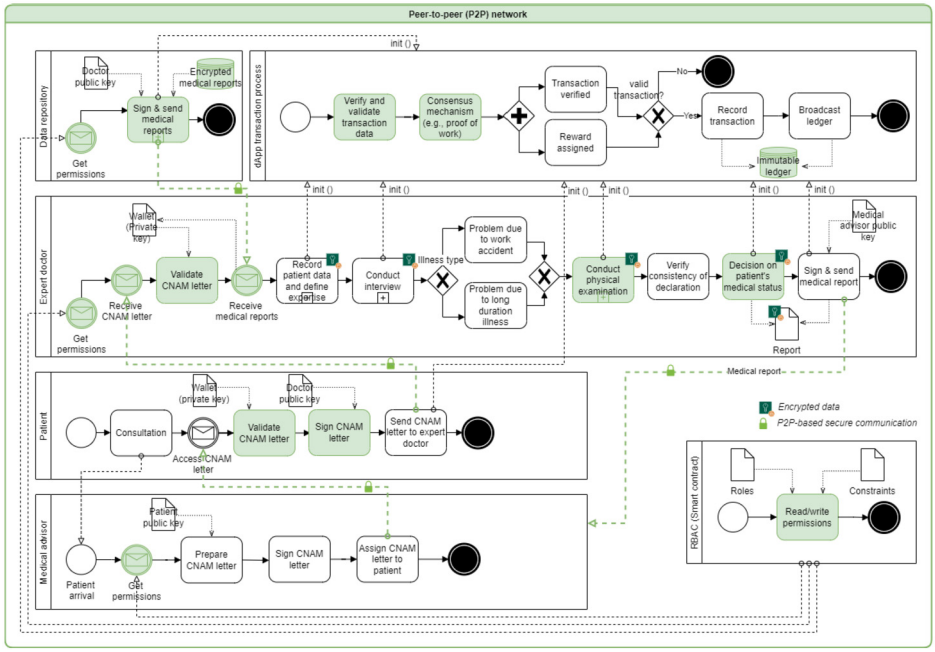

Fig. 3. Blockchain as a countermeasure solution to mitigate security threats of traditional BPPHA.

controls to verify and validate the authenticity of medical reports. The use of RBAC and cryptography (e.g. to store only encrypted medical reports on-chain and off-chain) overcome data theft. Also, the permission settings and access control enable patients to control their medical reports, and the tamper-resistant environment of blockchain guarantees the authenticity of medical reports.

Blockchain-based BPPHA works on a P2P-based distributed network to exchange data (e.g. CNAM letter, medical reports, medical records). It makes it hard for an attacker to intercept the communication, data analysis, or sniffing. Blockchain enables pseudo-anonymity because the patients and their medical data are linked with an anonymous public address. Blockchain-based BPPHA has an immutable ledger that keeps immutable logs to track who and when the particular operation (intentional or unintentional) was performed. Thus, overcoming the repudiation threat. Medical records and healthcare database can be protected against data tampering by using decentralized access control and blockchain controls to verify and validate the authenticity of medical records and healthcare databases. Decentralized access control and cryptography overcome the threat of data theft. Moreover, blockchain is decentralized, operates over a P2P network, and does not rely on a single or central point server and service. Thus, it is resilient to a single-point failure. Blockchain-based BPPHA employs RBAC to guarantee that only relevant people have access to specific information, and unauthorized users cannot access it.

7. Other Challenges of Blockchain-Based Healthcare Applications

Blockchain technology is advancing in the healthcare domain, and along with the security issues, it is also facing scalability, privacy, and regulatory challenges.

Scalability: Scalability is a big problem in blockchains' widespread adoption (Banchhor *et al.*, 2021). Blockchains have prefixed block size, block creation time, and process a fixed number of transactions per block. These settings help to achieve immutability, tamper-evident feature, ledger redundancy, and decentralized verification and validation of transactions but make the transaction processing (throughput) slow. For example, the Ethereum platform processes only 15 transactions per second (Neisse *et al.*, 2017). Also, blockchains maintain a ledger starting from the first (genesis) block that grows over time (e.g. Ethereum full node sync size is now 1+ Terabytes and increasing[5]). The blockchain network shares the ledger with all the participant nodes. Therefore, each node requires tremendous network resources and storage to store the ledger.

Various solutions are explored to overcome scalability issues (e.g. permissioned blockchains, lighting protocol, sharding, delegated proof of stake, directed acyclic graph) (Singh *et al.*, 2021). These techniques can help to increase the volume of transactions, although more work is needed in this direction.

Privacy: Permissionless blockchains have privacy issues by design (Yaqoob *et al.*, 2021). The ledger is disseminated across network nodes in permissionless blockchains, and transactions are publicly accessible. The attacker can utilize the ledger and apply different approaches (graph analysis, social engineering, phishing, transaction linkage) to track user activity and get private information. These privacy concerns are growing, and it is restraining the use of blockchain in healthcare applications since it distributes personal information in a publicly accessible database (Yaqoob *et al.*, 2021).

To overcome privacy challenges, different privacy-preserving proposals (e.g. secure multi-party computation, zero-knowledge proof, homomorphic encryption, ring signatures, transaction mixers) (Bernal Bernabe *et al.*, 2019) and blockchain platforms (such as Enigma, Zcash, Monero) (Khan and Nassar, 2019) are advancing to preserve the privacy of confidential information. These solutions primarily address overall transaction privacy in cryptocurrency-based blockchain platforms. Therefore, more research is required in the area of privacy-preserving blockchains for healthcare applications.

Regulations: Blockchain supports disintermediation where nobody takes responsibility for providing services, controls, and associated data sets. Privacy laws (e.g. EU general data protection regulation (GDPR), health insurance portability and accountability act (HIPPA)) can overwhelm the standardization and regulations for BBHAs. For example, under GDPR, the users are controllers of their data, but the immutable ledger cannot let the user delete (or update) their data (Yaqoob *et al.*, 2021). In governance, a key question for regulators is who should be held accountable for breaches of laws and regulations.

Many organizations are collaborating on regulatory guidance (such as a legal framework for data storage and sharing over blockchains) (Yaqoob *et al.*, 2021). However, more research is needed to standardize blockchains for healthcare applications.

[5] https://etherscan.io/chartsync/chaindefault

8. Concluding Remarks

Limitation: To ensure the quality of empirical research, we expanded our discussion by outlining the threats to validity (Zhou *et al.*, 2016). The relevant threats are restricted time span, publication bias, subjective interpretation, and lack of expert evaluation. The researcher cannot forecast further relevant studies beyond the defined time period because of the *restricted time span*. For example, blockchain is a relatively new technology that is constantly evolving. As a result, a wide range of countermeasures will arise in the future. The *publication bias* is the tendency of linked research to disclose good outcomes rather than negative results. The threat of *subjective interpretation* exists since we might have different interpretations and opinions related to identified threats, vulnerabilities, and countermeasures. Moreover, a *lack of expert evaluation* may also lead to a subjective interpretation and erroneous conclusion.

Conclusion: We present blockchain-based healthcare security ontology using the concepts of the SRM domain model. HealthOnt presents blockchain as a countermeasure solution (Table 3) and supports the decision to build blockchain-based healthcare applications to mitigate the security threats of traditional healthcare applications. However, blockchain-based healthcare applications are also not secure because there are several ways to negate the security in the context of confidentiality, integrity, and availability of the system. Also, there are conceptual ambiguities and semantic gaps when performing the SRM of traditional and blockchain-based applications. To address these issues, we present the HealthOnt, where we define the classifications of assets, security threats, vulnerabilities, and countermeasures. Compared to the previous works, HealthOnt encodes the information into a dynamic ontology-based knowledge that can be extended, reused, or integrated with other security ontology representations. HealthOnt can support the iterative process of SRM and can be updated continuously when new security threats, vulnerabilities, or countermeasures emerge. Furthermore, the evaluation using back-pain patients' healthcare application shows the practical applicability of HealthOnt. HealthOnt may assist in the modelling and analysis of the real-world situations and helps to address the important security concerns from a stakeholder point of view.

Future work: We will continue using the HealthOnt in different healthcare scenarios including various stakeholder perspectives. For example, it is necessary to explore how domain experts (e.g. healthcare specialists, blockchain engineers, and security analysts) perceive the significance of HealthOnt's contribution to derive the missing security components, to determine the comprehensiveness, and technical correctness of the healthcare system. As noted in Sections 3.11 and 4.9, the human aspect is crucial in healthcare. Blockchain offers a suitable infrastructure to solve security concerns related to the human factor. So, another potential future work is to investigate how blockchain might overcome challenges linked to a human factor, as well as the relevance of various vulnerabilities associated with human interaction.

References

Agbo, C.C., Mahmoud, Q.H., Eklund, J.M. (2019). Blockchain technology in healthcare: a systematic review. *Healthcare*, 7(2). https://doi.org/10.3390/healthcare7020056.

Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., Alizadeh, M. (2019). The application of internet of things in healthcare: a systematic literature review and classification. *Universal Access in the Information Society*, 18(4), 837–869. https://doi.org/10.1007/s10209-018-0618-4.

Alcarria, R., Bordel, B., Robles, T., Martín, D., Manso-Callejo, M.Á. (2018). A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. *Sensors (Switzerland)*, 18(10), 3561.

Ali, M.S., Vecchio, M., Putra, G.D., Kanhere, S.S., Antonelli, F. (2020). A decentralized peer-to-peer remote health monitoring system. *Sensors (Switzerland)*, 20(6), 1656.

Aljedaani, B., Babar, M.A. (2021). Challenges with developing secure mobile health applications: systematic review. *JMIR Mhealth Uhealth*, 9(6), 15654. https://doi.org/10.2196/15654.

Arunkumar, S., Muppidi, S. (2019). Secure your blockchain solutions. https://developer.ibm.com/articles/how-to-secure-blockchain-solutions.

Banchhor, P., Sahu, D., Mishra, A., Ahmed, M.B. (2021). A systematic review on blockchain security attacks, challenges, and issues. *International Journal of Engineering Research and Technology (IJERT)*, 10(04), 386–391.

Bernal Bernabe, J., Canovas, J.L., Hernandez-Ramos, J.L., Torres Moreno, R., Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: review and challenges. *IEEE Access*, 7, 164908–164940.

Bhardwaj, A., Shah, S.B.H., Shankar, A., Alazab, M., Kumar, M., Gadekallu, T.R. (2021). Penetration testing framework for smart contract Blockchain. *Peer-to-Peer Networking and Applications*, 14, 2635–2650.

Bhuiyan, M.Z.A., Zaman, A., Wang, T., Wang, G., Tao, H., Hassan, M.M. (2018). Blockchain and Big Data to transform the healthcare. In: *Proceedings of the International Conference on Data Processing and Applications, ICDPA 2018*. Association for Computing Machinery, New York, NY, USA, pp. 62–68. 9781450364188. https://doi.org/10.1145/3224207.3224220.

Biryukov, A., Tikhomirov, S. (2019). Deanonymization and linkability of cryptocurrency transactions based on network analysis. In: *2019 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 172–184. https://doi.org/10.1109/EuroSP.2019.00022.

Chen, J., Ma, X., Du, M., Wang, Z. (2018). A blockchain application for medical information sharing. In: *2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE)*, pp. 1–7. https://doi.org/10.1109/TEMS-ISIE.2018.8478645.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K.R., Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 95, 420–429. https://doi.org/10.1016/j.future.2019.01.018.

Chukwu, E., Garg, L. (2020). A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. *IEEE Access*, 8, 21196–21214. https://doi.org/10.1109/ACCESS.2020.2969881.

Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014.

Dexter, S. (2018). How Are Blockchain Transactions Validated? Consensus VS Validation. https://www.mangoresearch.co/blockchain-consensus-vs-validation.

Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.-L. (2017). BLOCKBENCH: a framework for analyzing private blockchains. In: *Proceedings of the 2017 ACM International Conference on Management of Data, SIGMOD '17*. Association for Computing Machinery, New York, NY, USA, pp. 1085–1100. 9781450341974. https://doi.org/10.1145/3035918.3064033.

Douceur, J.R. (2002). The Sybil Attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (Eds.), *Peer-to-Peer Systems, IPTPS 2002*, Lecture Notes in Computer Science, Vol. 2429. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45748-8_24.

Dubois, É., Mayer, N., Heymans, P., Matulevičius, R. (2010). *A Systematic Approach to Define the Domain of Information System Security Risk Management*. Springer, Berlin, Heidelberg, pp. 289–306. https://doi.org/10.1007/978-3-642-12544-7_16.

El-Gazzar, R., Stendal, K. (2020). Blockchain in health care: hope or hype? *Journal of Medical Internet Research*, 22(7). https://doi.org/10.2196/17199.

Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.-K.R. (2018). Blockchain: a panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712.

Fatima, A., Colomo-Palacios, R. (2018). Security aspects in healthcare information systems: a systematic mapping. *Procedia Computer Science*, 138, 12–19. https://doi.org/10.1016/j.procs.2018.10.003.

Fink, A. (2019). *Conducting Research Literature Reviews: From the Internet to Paper*. 9781544318479, SAGE Publications, 304 pp.

Ganji, D., Kalloniatis, C., Mouratidis, H., Gheytassi, S.M. (2019). Approaches to develop and implement ISO/IEC 27001 standard – information security management systems: a systematic literature review. *International Journal on Advances in Software (IARIA)*, 12(3–4), 228–238.

Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X., Yang, Y.-X. (2018). A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, 6, 27205–27213. https://doi.org/10.1109/ACCESS.2018.2827203.

George, S.L., Buyse, M. (2015). Data fraud in clinical trials. *Clinical Investigation (Lond)*, 5(2), 161–173. https://doi.org/10.4155/cli.14.116.

Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, 42(130), 1–7. https://doi.org/10.1007/s10916-018-0982-x.

Grunspan, C., Perez-Maro, R. (2018). Double spend races. *International Journal of Theoretical and Applied Finance*, 21(08), 1850053. https://doi.org/10.1142/s021902491850053x.

Guru, D., Perumal, S., Varadarajan, V. (2021). Approaches towards blockchain innovation: a survey and future directions. *Electronics (Switzerland)*, 10(10), 1–15. https://doi.org/10.3390/electronics10101219.

Han, H., Huang, M., Zhang, Y., Bhatti, U.A. (2018). An architecture of secure health information storage system based on blockchain technology. In: *ICCCS (2)*, Lecture Notes in Computer Science, Vol. 11064. Springer International Publishing, Cham, pp. 578–588. 978-3-030-00009-7.

Hathaliya, J.J., Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 153, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018.

Hector, U.-R., Boris, C.-L. (2020). BLONDiE: Blockchain Ontology with Dynamic Extensibility. https://doi.org/10.48550/arXiv.2008.09518.

Heilman, E., Kendler, A., Zohar, A., Goldberg, S. (2015). Eclipse attacks on Bitcoin's Peer-to-Peer network. In: *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, DC, pp. 129–144. 978-1-939133-11-3.

HelpNetSecurity (2019). More than 99% of cyberattacks rely on human interaction. https://www.helpnetsecurity.com/2019/09/10/cyberattacks-human-interaction/.

Henningsen, S., Teunis, D., Florian, M., Scheuermann, B. (2019). Eclipsing ethereum peers with false friends. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE Computer Society, Los Alamitos, CA, USA, pp. 300–309. https://doi.org/10.1109/EuroSPW.2019.00040.

Herzog, A., Shahmehri, N., Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, 1(4), 1–23. https://doi.org/10.4018/jisp.2007100101.

Hussein, A.F., N., A., Ramírez-González, G., Abdulhay, E.W., Tavares, J.M.R.S., de Albuquerque, V.H.C. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research*, 52, 1–11. https://doi.org/10.1016/j.cogsys.2018.05.004.

IBM-Blockchain (2022). Blockchain in healthcare. https://www.ibm.com/blogs/blockchain/category/blockchain-healthcare.

Iqbal, M., Matulevičius, R. (2019). Blockchain-based application security risks: a systematic literature review. In: Proper, H.A., Stirna, J. (Eds.), *Advanced Information Systems Engineering Workshops*. Springer International Publishing, Cham, pp. 176–188. 978-3-030-20948-3. https://doi.org/10.1007/978-3-030-20948-3_16.

Iqbal, M., Matulevičius, R. (2020). Corda security ontology: example of post-trade matching and confirmation. *Baltic Journal of Modern Computing*, 8(4), 638–674. https://doi.org/10.22364/bjmc.2020.8.4.11.

Iqbal, M., Matulevičius, R. (2021a). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, 9, 76153–76177. https://doi.org/10.1109/ACCESS.2021.3081998.

Iqbal, M., Matulevičius, R. (2021b). Blockchain as a countermeasure solution for security threats of healthcare applications. In: González Enríquez, J., Debois, S., Fettke, P., Plebani, P., van de Weerd, I., Weber, I. (Eds.), *Business Process Management: Blockchain and Robotic Process Automation Forum*. Springer International Publishing, Cham, pp. 67–84. 978-3-030-85867-4.

Iwaya, L.H., Ahmad, A., Babar, M.A. (2020). Security and privacy for mHealth and uHealth systems: a systematic mapping study. *IEEE Access*, 8, 150081–150112. https://doi.org/10.1109/ACCESS.2020.3015962.

Jin, H., Luo, Y., Li, P., Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, 7, 61656–61669. https://doi.org/10.1109/ACCESS.2019.2916503.

Jonathan, K., Sari, A.K. (2019). Security issues and vulnerabilities on a blockchain system: a review. In: *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE, Yogyakarta, Indonesia, pp. 228–232. https://doi.org/10.1109/ISRITI48646.2019.9034659.

Junejo, A.Z., Hashmani, M.A., Alabdulatif, A.A. (2020). A survey on privacy vulnerabilities in permissionless blockchains. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(9), 130–139.

Kang, W., Liang, Y. (2013). A security ontology with MDA for software development. In: *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, Beijing, China, pp. 67–74. https://doi.org/10.1109/CyberC.2013.20.

Khan, N., Nassar, M. (2019). A look into privacy-preserving blockchains. In: *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. IEEE Computer Society, Abu Dhabi, United Arab Emirates, pp. 1–6. https://doi.org/10.1109/AICCSA47632.2019.9035235.

Kitchenham, B., Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. *EBSE Technical Report, Version 2.3*.

Kleinaki, A.S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P.S., Kaldoudi, E. (2018). A blockchain-based notarization service for biomedical knowledge retrieval. *Computational and Structural Biotechnology Journal*, 16, 288–297. https://doi.org/10.1016/j.csbj.2018.08.002.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020.

Linn, L.A., Koo, M.B. (2016). Blockchain for health data and its potential use in health IT and health care related research. In: *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. NIST, Gaithersburg, MD, USA, pp. 1–10.

Liu, L., Chen, W., Zhang, L., Liu, J.Y., Qin, J. (2019). A type of block withholding delay attack and the countermeasure based on type-2 fuzzy inference. *Mathematical Biosciences and Engineering*, 17(1), 309–327. https://doi.org/10.3934/mbe.2020017.

Maesa, D.D.F., Ricci, L., Mori, P. (2017). Distributed access control through blockchain technology lockchain. *ERCIM News*, 110, 31–32.

Mansfield-Devine, S. (2016). Your life in your hands: the security issues with healthcare apps. *Network Security*, 2016(4), 14–18. https://doi.org/10.1016/S1353-4858(16)30038-1.

Martino, F.D.D., Klein, S.D., Neil, J.O., Huang, Y., Nisson, L., Race, M. (2019). Transforming the U.S. Healthcare Industry with Blockchain Technology. *Lex Mundi Blockchain White Paper Series*.

Matulevičius, R. (2017). *Fundamentals of Secure System Modelling*, 1st ed. Springer International Publishing, Cham.

McGhin, T., Choo, K.-K.R., Zhechao, C., He, D. (2019). Blockchain in healthcare applications: research challenges and opportunities. *Journal of Network and Computer Applications*, 135, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*, 9, 9728–9743. https://doi.org/10.1109/ACCESS.2021.3049920.

Narayanan, A., Bonneau, J., Felten, E.W., Miller, A., Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, Princeton and Oxford.

Narikimilli, N.R.S., Kumar, A., Antu, A.D., Xie, B. (2020). Blockchain applications in healthcare – a review and future perspective. In: Chen, Z., Cui, L., Palanisamy, B., Zhang, L.-J. (Eds.), *Blockchain – ICBC 2020*. Springer International Publishing, Cham, pp. 198–218. 978-3-030-59638-5.

Neisse, R., Steri, G., Nai-Fovino, I. (2017). A blockchain-based approach for data accountability and provenance tracking. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3098954.3098958.

Nicolas, K., Wang, Y., Giakos, G.C., Wei, B., Shen, H. (2021). Blockchain system defensive overview for double-spend and selfish mining attacks: a systematic approach. *IEEE Access*, 9, 3838–3857. https://doi.org/10.1109/ACCESS.2020.3047365.

Noy, N.F., McGuinness, D.L. (2001). Ontology development 101: a guide to creating your first ontology. *Stanford Knowledge Systems Laboratory*, 32, 1–25.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37, 879–910.

Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., Herrera-Joancomartí, J. (2019). Double-spending prevention for Bitcoin zero-confirmation transactions. *International Journal of Information Security*, 18(4), 451–463.

Quintyne-Collins, M. (2019). Short Paper: Towards Characterizing Sybil Attacks in Cryptocurrency Mixers. *IACR Cryptology ePrint Archive*, 1111.

Raad, J., Cruz, C. (2015). A survey on ontology evaluation methods. In: *Proceedings of the International Conference on Knowledge Engineering and Ontology Development, Part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. SciTePress, Lisbonne, Portugal, pp. 179–186.

Radhakrishnan, B.L., Sam Joseph, A., Sudhakar, S. (2019). Securing blockchain based electronic health record using multilevel authentication. In: *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, USA, pp. 699–703. https://doi.org/10.1109/ICACCS.2019.8728483.

Rahmadika, S., Rhee, K.H. (2018). Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management*, 10, 1–12. https://doi.org/10.1177/1847979018790589.

Randall, D., Goel, P., Abujamra, R., et al.(2017). Blockchain applications and use cases in health information technology. *Journal of Health & Medical Informatics*, 8(3), 1–17.

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. *Journal of Food Quality*, 2021, 7608296. https://doi.org/10.1155/2021/7608296.

Rosenfeld, M. (2014). Analysis of Hashrate-Based Double Spending. arXiv preprint arXiv:1402.2009, 1–13.

Saha, A., Amin, R., Kunal, S., Vollala, S., Dwivedi, S.K. (2019). Review on "Blockchain technology based medical healthcare system with privacy issues". *Security and Privacy*, 2(5), 83. https://doi.org/10.1002/spy2.83.

Sardi, A., Rizzi, A., Sorano, E., Guerrieri, A. (2020). Cyber risk in health facilities: a systematic literature review. *Sustainability*, 12(17). https://doi.org/10.3390/su12177002.

Sayeed, S., Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, 9(9). https://doi.org/10.3390/app9091788.

Sayeed, S., Marco-Gisbert, H., Caira, T. (2020). Smart contract: attacks and protections. *IEEE Access*, 8, 24416–24427.

SecurityMetrics (2015). Healthcare: Recognize Social Engineering Techniques. https://www.securitymetrics.com/blog/healthcare-recognize-social-engineering-techniques.

Shankland, S. (2021). Cryptocurrency faces a quantum computing problem. https://www.cnet.com/personal-finance/crypto/cryptocurrency-faces-a-quantum-computing-problem.

Shi, S., He, D., Li, L., Kumar, N., Khurram, M. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. *Computers & Security*, 97, 101966.

Singh, S., Sanwar Hosen, A.S.M., Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access*, 9, 13938–13959.

SpecOpsSoft (2020). The countries experiencing the most 'significant' cyber-attacks. https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.

Steiner, C.M., Albert, D. (2017). Validating domain ontologies: a methodology exemplified for concept maps. *Cogent Education*, 4(1). https://doi.org/10.1080/2331186X.2016.1263006.

Swathi, P., Modi, C., Patel, D. (2019). Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, Kanpur, pp. 6–11. https://doi.org/10.1109/ICCCNT45670.2019.8944507.

Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., Njilla, L. (2017). Security implications of blockchain cloud with analysis of block withholding attack. In: *17TH IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 458–467. https://doi.org/10.1109/CCGRID.2017.111.

Uschold, M., Gruninger, M. (1996). Ontologies: principles, methods and applications. *The Knowledge Engineering Review*, 11(2), 93–136. https://doi.org/10.1017/S0269888900007797.

Velissarios, J., Herzig, J., Didem, U. (2019). Blockchain's potential starts with security. https://www.accenture.com/us-en/insights/blockchain/potential-starts-security.

Wang, Y., Yang, J., Li, T., Zhu, F., Zhou, X. (2018). Anti-dust: a method for identifying and preventing blockchain's dust attacks. In: *2018 International Conference on Information Systems and Computer Aided Education (ICISCAE)*. IEEE, Changchun, pp. 274–280. https://doi.org/10.1109/ICISCAE.2018.8666834.

Wani, T.A., Mendoza, A., Gray, K. (2020). Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. *JMIR Mhealth Uhealth*, 8(6), 18175. https://doi.org/10.2196/18175.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., Yu, N. (2019). Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal*, 6(5), 8770–8781. https://doi.org/10.1109/JIOT.2019.2923525.

Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-020-05519-w.

Yeng, P.K., Szekeres, A., Yang, B., Snekkenes, E.A. (2021). Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: systematic mapping study. *JMIR Human Factors*, 8(2), 17604. https://doi.org/10.2196/17604.

Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, 6, 5393–5401. https://doi.org/10.1109/ACCESS.2017.2788411.

Zhang, A., Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, 42(8). https://doi.org/10.1007/s10916-018-0995-5.

Zhang, S., Lee, J.-H. (2019). Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*, 15(10), 5715–5722. https://doi.org/10.1109/TII.2019.2921566.

Zhou, X., Jin, Y., Zhang, H., Li, S., Huang, X. (2016). A map of threats to validity of systematic literature reviews in software engineering. In: *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, Hamilton, New Zealand, pp. 153–160. https://doi.org/10.1109/APSEC.2016.031.

R. Matulevičius received his PhD diploma from the Norwegian University of Science and Technology in computer and information science in 2005. He was a postdoctoral researcher at the University of Namur in Belgium from 2005 to 2009. From 2010 to 2018 he worked as an associate professor at the University of Tartu. Currently, Matulevičius holds a professor of information security position at the University of Tartu (Estonia). His research interests include security and privacy of information, security risk management, and model-driven security. His publication record includes more than 111 articles published in peer-reviewed journals, conferences, and workshops. Matulevičius has been a program committee member (e.g. NordSec, PoEM, REFSQ, and CAiSE and others), steering committee member (e.g. BIR, ADBIS, Baltic DB&IS) at international conferences. Matulevičius is an editorial board member of the *Requirements Engineering Journal* (REEN, Springer), *Business and Information Systems Engineering* (BISE, Springer) and a few other international journals. He is a co-editor of six books in the field of computer science and information systems, and an author of a book on "Fundamentals of Secure System Modelling" (Springer, 2017). Currently, he is involved in the SPARTA H2020 project (task: Privacy-by-Design) and is a principal researcher in the Erasmus+ projects on securing against phishing (CyberPhish) and blockchain skills development (CHAISE).

M. Iqbal began his PhD degree in computer science at the University of Tartu (UT), Estonia, in 2018 and has been working as a junior research fellow at the UT since 2019. M. Iqbal is also a member of UT's highly recognized information security research group, where he conducts impactful research while also teaching two blockchain-related courses. His research interests include the security implications of blockchain systems and the implementation of a security risk management framework for blockchain systems, concentrating specifically on the security of blockchain-based decentralized applications. Currently, he is involved in the ERASMUS+ sectoral alliance program, CHAISE. He has co-authored 12+ research papers in premier journals and conferences.

E. Ammar Elhadjamor received her PhD in computer science from the University of Sousse in Tunisia. She is a contractual teacher of computer science at the Institut Supérieur des Sciences Appliquées et de la Technologie, University of Sousse. She is a member of the RIADI laboratory. She has taught courses related to databases, business intelligence, data warehouse, algorithms and data mining. Her research interests include machine learning, business process management, process mining, e-Learning and e-Health.

S.A. Ghannouchi obtained her PhD in computer science from the University of Manouba in Tunisia and her HDR in enterprise computing from the University of Sousse in Tunisia. She is a full professor in business computing at the High Institute of Management of Sousse, in the University of Sousse. Her taught courses include: "Databases", "Information systems", "Software Engineering" and "Business Process Reengineering". Her research interests include: software engineering and reengineering, business process modelling, business process management, process mining, e-learning and e-health.

M. Bakhtina received the MA degree in innovation and technology management from the University of Tartu (UT), Estonia. There, she is pursuing a PhD degree in computer science. Also, she is working as a junior research fellow with UT. Her research interests include the influence of technologies and digital products on organisations, particularly how intelligent systems should be managed in terms of information security and privacy.

S. Ghannouchi is a doctor of medicine from the Faculty of Medicine of Sousse since 1986, orthopedic surgeon since 1990 and professor of anatomy at the Faculty of Medicine of Sousse since 1995. He holds a PhD in biomechanics from the Ecole Supérieure d'Arts et Métier – Paris (1998). He also graduated with a degree in legal compensation for bodily injury from the Faculty of Medicine of Marseille (2008) and he is a judicial expert at the courts since 1995 and expert with the National Health Insurance Structure (CNAM) since 1991.