Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications *(Technical report)*

Mubashar Iqbal[0000−0003−0543−613X] and Raimundas Matulevičius[0000−0002−1829−4794]

Institute of Computer Science, University of Tartu, Tartu, Estonia
{mubashar.iqbal,raimundas.matulevicius}@ut.ee

This technical report is associated with the paper "Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications".

1 Introduction

Healthcare applications are integrating technology infrastructure to empower patients and the entire healthcare sector. The change facilitates the healthcare sector to make more prompt and informed decisions using digital medical data. Blockchain technology is emerging in healthcare to overcome various security challenges, enhance data integrity, and transform the transacting process into a decentralised, transparent, and immutable manner. The advent of blockchain technology has opened several research areas within the healthcare sector to preserve medical data, to ensure data integrity, patient ownership to his data, easy exchange of medical data, and seamless medical insurance claims. However, there is conceptual ambiguity and semantic gaps about blockchain as a countermeasure solution for traditional healthcare applications. Therefore, we build an ontology by investigating the security threats of traditional healthcare applications and how these security threats could be mitigated by utilising blockchain.

2 Research Method

This paper aims to present an ontological framework based on the SRM domain model to show blockchain as a countermeasure to mitigate various security threats of traditional healthcare applications. In this case, a systematic literature review (SLR) is appropriate since it allows the systematic analysis of relevant literature. We followed the review guidelines of Kitchenham [1] and specified the review protocol to identify relevant papers and conduct this study.

2.1 SLR Settings

According to the Kitchenham [1] guidelines, we specify the research questions, design a search protocol to search, and identify relevant papers. We defined the following research questions, each covering a different aspect to achieve our objective.

RQ1: *What are the assets to protect in healthcare applications?*
RQ2: *What are the security threats of traditional healthcare applications?*
RQ3: *What are the security vulnerabilities of traditional healthcare applications?*
RQ4: *What are the blockchain-based countermeasures to mitigate vulnerabilities of traditional healthcare applications?*

The overall search strategy is to find a body of relevant studies. For this SLR two search strategies were used, as recommended by Okoli et al. [2], Fink et al. [3] and Levy et. al. [4], to secure identification of relevant studies. Accordingly, in the first step, called primary search, search strings were used to identify an initial set of papers [3]. Several electronic databases were used for this step. In the second step, a secondary search was performed by means of backward and forward tracing [2, 4]. The search strings included the keywords *"blockchain"* in combination with *"healthcare"*, *"security"*, or *"security threats"*. We applied the search strings on *ACM Digital Library*, *IEEE Xplore*, *springerLink*, *Scopus*, and *Web of Science*. We included other non-academic organisations (grey literature) as proposed in [1].

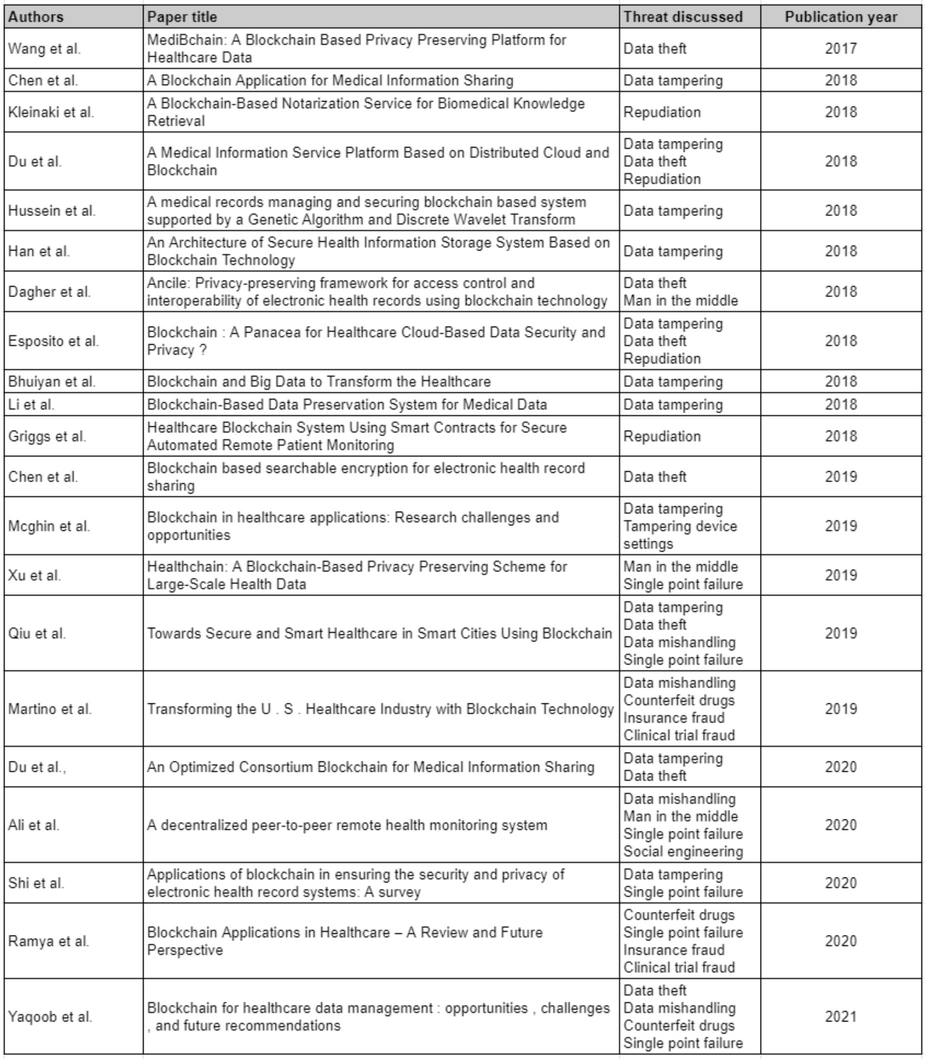
We applied *exclusion (EC)* and *inclusion (IC)* criteria to identify relevant papers. Papers that were duplicates, not in English, shorter than 5 pages, inaccessible (via University subscriptions or Internet search), or published before 2008, were excluded. Papers less than 5 pages were excluded as short papers would not contain enough information for our evaluation. Papers within the domain of blockchain *(IC1)*, covering the security aspects of healthcare applications with blockchain *(IC2)*, and providing a description of various countermeasures *(IC3)*, were included.

The search resulted in approximately 1900 articles from all the sources. Having removed the duplicates, and several iterations of filtering, considering the exclusion criteria and the first two inclusion criteria *(IC1 & IC2)*, a total of 50 papers remained. These were subjected to full-text examination *(IC3)*, which resulted in a *total of 21 studies* (Table 1).

2.2 SRM Domain Model

The SRM domain model (Fig. 1) [5, 6] helps us to structure the knowledge of blockchain as a countermeasure solution. Among other SRM approaches [7], the SRM domain model fulfils the criteria of ISO/IEC 27001 standard and explore three aspects *(e.g., assets-, risk-, and risk treatment-related)* during the early phases of information system development. The asset can be 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 the security needs. The risk combines a risk event and impact. The risk event constitutes the threat and one or more vulnerabilities. The threat targets the system asset and exploits the vulnerability. The vulnerability is connected to

Table 1. Systematic literature review papers.



Authors	Paper title	Threat discussed	Publication year
Wang et al.	MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data	Data theft	2017
Chen et al.	A Blockchain Application for Medical Information Sharing	Data tampering	2018
Kleinaki et al.	A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval	Repudiation	2018
Du et al.	A Medical Information Service Platform Based on Distributed Cloud and Blockchain	Data tampering Data theft Repudiation	2018
Hussein et al.	A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform	Data tampering	2018
Han et al.	An Architecture of Secure Health Information Storage System Based on Blockchain Technology	Data tampering	2018
Dagher et al.	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	Data theft Man in the middle	2018
Esposito et al.	Blockchain : A Panacea for Healthcare Cloud-Based Data Security and Privacy ?	Data tampering Data theft Repudiation	2018
Bhuiyan et al.	Blockchain and Big Data to Transform the Healthcare	Data tampering	2018
Li et al.	Blockchain-Based Data Preservation System for Medical Data	Data tampering	2018
Griggs et al.	Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring	Repudiation	2018
Chen et al.	Blockchain based searchable encryption for electronic health record sharing	Data theft	2019
Mcghin et al.	Blockchain in healthcare applications: Research challenges and opportunities	Data tampering Tampering device settings	2019
Xu et al.	Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data	Man in the middle Single point failure	2019
Qiu et al.	Towards Secure and Smart Healthcare in Smart Cities Using Blockchain	Data tampering Data theft Data mishandling Single point failure	2019
Martino et al.	Transforming the U . S . Healthcare Industry with Blockchain Technology	Data mishandling Counterfeit drugs Insurance fraud Clinical trial fraud	2019
Du et al.,	An Optimized Consortium Blockchain for Medical Information Sharing	Data tampering Data theft	2020
Ali et al.	A decentralized peer-to-peer remote health monitoring system	Data mishandling Man in the middle Single point failure Social engineering	2020
Shi et al.	Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey	Data tampering Single point failure	2020
Ramya et al.	Blockchain Applications in Healthcare – A Review and Future Perspective	Counterfeit drugs Single point failure Insurance fraud Clinical trial fraud	2020
Yaqoob et al.	Blockchain for healthcare data management : opportunities , challenges , and future recommendations	Data theft Data mishandling Counterfeit drugs Single point failure	2021

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.

3 Security Risk Analysis of Healthcare Applications

We analyse the literature studies using the SRM domain model to build a framework (Table 2) that presents the security threats, their vulnerabilities, assets

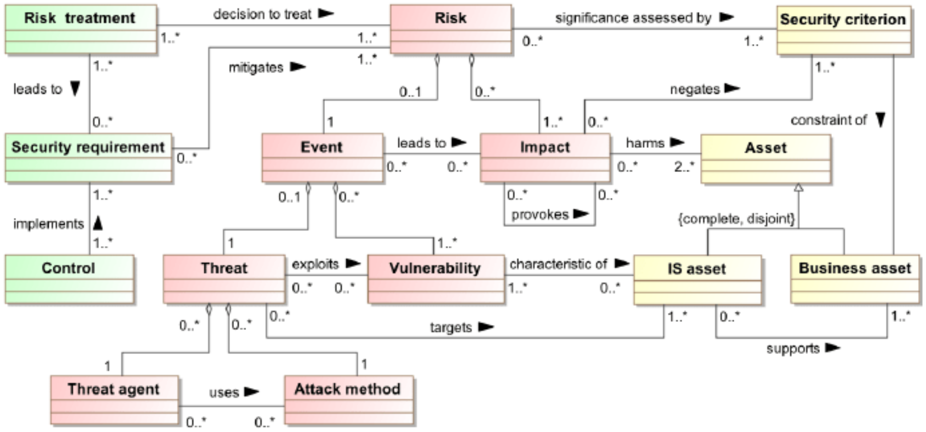


Fig. 1. The SRM domain model [adapted from: [5, 6]]

to protect, and blockchain-based countermeasures. In this section, we discuss the four security threats *(e.g., data tampering, data theft, medical records mishandling, counterfeit drugs)* in detail. Other security threats *(e.g., man-in-the-middle, single-point failure, repudiation, insurance frauds, clinical trial fraud, tampering device settings, social engineering)* are in the technical report [8].

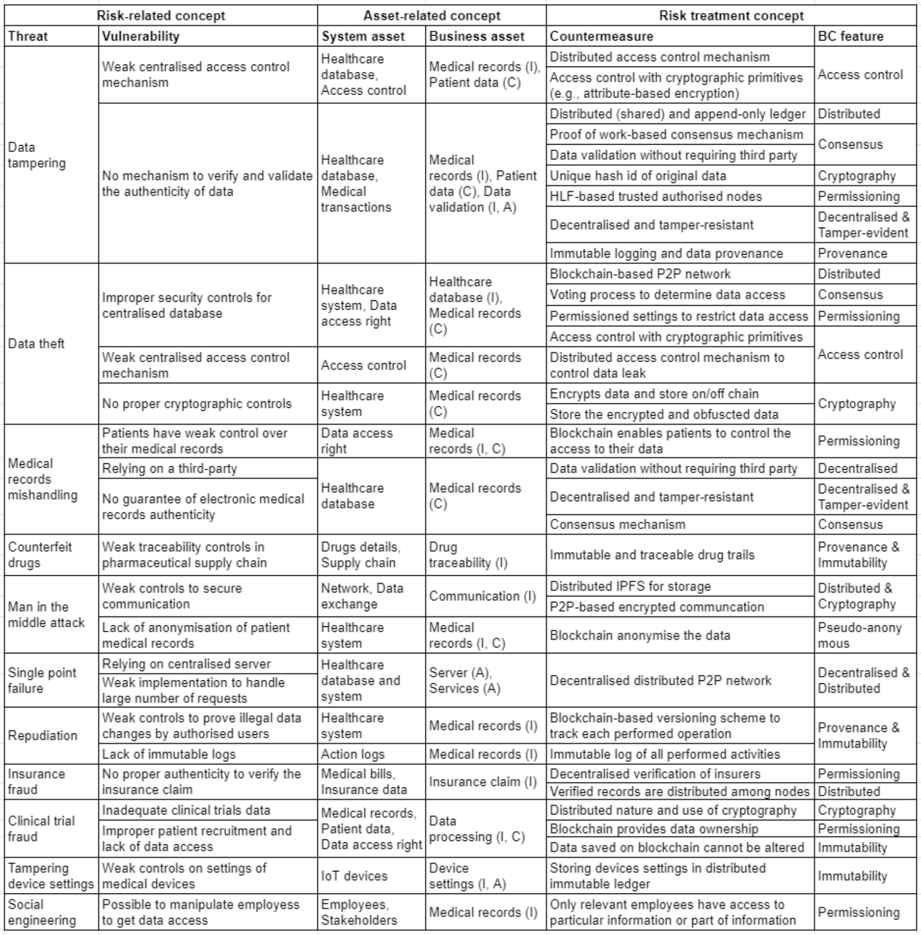
3.1 Data Tampering

The traditional approaches lack control over data security, which is a major concern for healthcare organisations because it can put patient's lives at risk.

Vulnerabilities: In traditional healthcare applications, the access control is managed by a designated authority/individual that could be error-prone. The *weak centralised access control* [9, 10, 11, 12] describes a case when the healthcare application fails to restrict unauthorised access to the resources. The attacker compromises the security and performs unauthorised actions that negate the integrity of medical records and confidentiality of patient data. The attacker uses unauthorised access to gain elevated privileges, execute commands, or bypass the security mechanisms to tamper with medical data. Moreover, traditional healthcare applications often rely on manual techniques or third-party providers to perform data verification and validation. These techniques *lack the proper mechanisms to verify and validate the authenticity of data* [13, 14, 15]. Consequently, the attacker can submit malicious content that the system can process and negate the integrity of medical records and confidentiality of patient data.

Countermeasures: Blockchain enables smart contracts-based distributed access control [16] that controls the stored medical data. The system authenticates and identifies associated users according to their access rights deployed in a decentralised and distributed environment. Also, strong cryptographic primitives (e.g., attribute-based encryption) [17] help to build fine-grained access control. The records are difficult to modify/delete because of the ledger redundancy among network nodes and append-only structure [18]. The healthcare applications on permissionless blockchain use PoW consensus to verify the executed transaction and data validation without requiring a third party before saving on the ledger [14]. Moreover, using the SHA-256 hashing algorithm, blockchain computes a unique hash id of original data that can be used to verify the authenticity of data [12]. Hyperledger fabric uses trusted authorised nodes to verify and validate the authenticity of data [13]. Blockchain is tamper-evident [11, 12] that detects any unauthorised modifications. Blockchain builds strong audit trails in immutable ledgers by keeping a log of each performed action [11] over time that could be used to verify and validate the authenticity of data.

Table 2. 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 centralised access control mechanism	Healthcare database, Access control	Medical records (I), 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 (I), Patient data (C), Data validation (I, 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 authorised nodes	Permissioning
				Decentralised and tamper-resistant	Decentralised & Tamper-evident
				Immutable logging and data provenance	Provenance
Data theft	Improper security controls for centralised database	Healthcare system, Data access right	Healthcare database (I), 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 centralised 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 obfuscted data	
Medical records mishandling	Patients have weak control over their medical records	Data access right	Medical records (I, 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	Decentralised
	No guarantee of electronic medical records authenticity			Decentralised and tamper-resistant	Decentralised & Tamper-evident
				Consensus mechanism	Consensus
Counterfeit drugs	Weak traceability controls in pharmaceutical supply chain	Drugs details, Supply chain	Drug traceability (I)	Immutable and traceable drug trails	Provenance & Immutability
Man in the middle attack	Weak controls to secure communication	Network, Data exchange	Communication (I)	Distributed IPFS for storage	Distributed & Cryptography
				P2P-based encrypted communcation	
	Lack of anonymisation of patient medical records	Healthcare system	Medical records (I, C)	Blockchain anonymise the data	Pseudo-anony mous
Single point failure	Relying on centralised server	Healthcare database and system	Server (A), Services (A)	Decentralised distributed P2P network	Decentralised & Distributed
	Weak implementation to handle large number of requests				
Repudiation	Weak controls to prove illegal data changes by authorised users	Healthcare system	Medical records (I)	Blockchain-based versioning scheme to track each performed operation	Provenance & Immutability
	Lack of immutable logs	Action logs	Medical records (I)	Immutable log of all performed activities	
Insurance fraud	No proper authenticity to verify the insurance claim	Medical bills, Insurance data	Insurance claim (I)	Decentralised verification of insurers	Permissioning
				Verified records are distributed among nodes	Distributed
Clinical trial fraud	Inadequate clinical trials data	Medical records, Patient data, Data access right	Data processing (I, C)	Distributed nature and use of cryptography	Cryptography
	Improper patient recruitment and lack of data access			Blockchain provides data ownership	Permissioning
				Data saved on blockchain cannot be altered	Immutability
Tampering device settings	Weak controls on settings of medical devices	IoT devices	Device settings (I, A)	Storing devices settings in distributed immutable ledger	Immutability
Social engineering	Possible to manipulate employess to get data access	Employees, Stakeholders	Medical records (I)	Only relevant employees have access to particular information or part of information	Permissioning

3.2 Data Theft

In healthcare, data theft has been on the rise for the past ten years, in 2020 reported 642 data thefts incidents [19] only in the United States.

Vulnerabilities: Databases are one of the most compromised assets [20] and centralised databases have *improper security controls* to protect against insider or outsider threats [17, 18]. The threats imposed by this vulnerability include: i) abuse of elevated privileges, ii) unauthorised access, iii) backup storage exposure, iv) database injection, v) default database accounts and configurations, vi) malware and the vii) human factor [19, 20]. Overall it negates the integrity of the healthcare system and confidentiality of medical data.

Similar to data tampering, the attacker can steal medical data due to *weak centralised access control* [17, 21] that leads the attacker to gain unauthorised access, elevated privileges, or bypass security mechanisms. As a result, it negates the confidentiality of medical data. Traditional healthcare applications use cryptography to save data securely and achieve information security objectives. However, it *lacks cryptographic control* [21] over data since the centralised authority/individual is responsible for the administration of the database (keeping elevated privileges, encryption/decryption keys). If the security of the system is compromised, then the attacker can steal the medical data.

Countermeasures: Blockchain works on a P2P-based distributed network where nodes behave both as a server and client to send and receive data directly with each other. This mechanism helps to protect the data leakage to unauthorised network users [13]. The [18] uses 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 data access only to authorised nodes [12, 21]. Similar to data tampering countermeasures, the strong cryptographic primitives (e.g., attribute-based encryption) [17] and smart contracts-based distributed access control mechanism [14] allows only authorised users to access medical data. The Ancile framework [18] uses the proxy re-encryption to encrypt the data and store hashes data on/off-chain, [17] suggests data obfuscation to protect data on/off-chain.

3.3 Medical Records Mishandling

Healthcare staff must ensure that medical records are kept private and safe. But medical records mishandling is one of the common HIPAA violations [22].

Vulnerabilities: The medical institutions control and manage the patient's medical data where the non-relevant individuals can access it as well. Thus, patients have *weak control over their medical records* [23]. Also, the patient has no idea how his data is processed or exchanged or with whom it is shared. In some cases, the individual from a medical institution involves in illegal medical data trade [24] that negates the integrity and confidentiality of medical records.

Hospitals and healthcare applications *rely on third-party* [15, 17] vendors (e.g., IT vendors, pharmacies, insurance companies, etc.) daily to perform their routine functions. These third-party vendors have access to the patient's medical data. They could intentionally sell medical data to data brokers or become a source of data breach and negate the confidentiality of medical data.

Also, the medical data is managed by a designated authority/individual, and the system administration governs the system with elevated privileges. If any such point is compromised, the attacker can manipulate and negate the integrity of medical data without leaving the traces. Therefore, traditional healthcare applications *cannot guarantee the authenticity* [15] of digital medical records.

Countermeasures: The permission settings and distributed access control enable patients to handle their medical data [10, 25]. The blockchain performs data validation during the consensus process before saving on the ledger. For example, blockchain provides a transparent platform to define data validation rules which are agreed upon by decentralised and distributed network nodes [26]. Then, all the nodes follow those rules to validate the data. The blockchain-based applications detect and discard all the unauthorised changes [25] if the majority of the network is honest (e.g., the adversary does not control 51% computing power). This process establishes a tamper-resistant environment [27].

3.4 Counterfeit Drugs (Fake Medicine)

For years, the pharmaceutical supply chain has been struggling to monitor its products and avoid fake medicine. According [10, 23], 10-30% (worth $200 billion) of drugs sold worldwide each year are counterfeit.

Vulnerabilities: Counterfeit drugs are on the rise, posing significant health risks. In pharmaceuticals, after manufacturing, drugs are moved from production stocks to wholesale distributors, which then move to retail firms. Customers purchase drugs from retailers. Due to *weak traceability controls* (e.g., ineffective data sharing, no traceable records) [28, 10, 23] in pharmaceutical supply chain. Thus, there is a risk of fake medicines being introduced during this process.

Countermeasures: 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 [28, 10, 23]. For example, IBM Research uses blockchain to reduce or eliminate the drug counterfeiting problems in Kenya [23] by using immutable and traceable logs at each stage of the pharmaceutical supply chain.

3.5 Man in the middle attack

Specops report [29] mentioned that man in the middle attacks are becoming common in healthcare systems. The attacker intercepts the communication between the healthcare provider and patient (or between healthcare providers) to gain sensitive information.

Vulnerabilities: The attacker can exploit the *weak controls of secure communication* [9] in traditional healthcare systems and negate the integrity of communication assets. For example, not properly implementing (or having) cryptographic functionality or lack of fine-grained access control mechanism.

In traditional healthcare applications, due to *lack of anonymisation of patient medical records* [30] the medical data is associated directly with patient identity. The attacker can get the data to trigger a ransomware attack. For example, pay a sum of money otherwise will publish it online or deny access to it.

Countermeasures: The authors [9] using blockchain introduce the distributed interplanetary file system (IPFS) for storage along with blockchain-based data encryption to reduce communication and computation overhead that establish a secure communication channel. Blockchain works on a P2P-based distributed network where nodes behave both as a server and client to send and receive encrypted data directly with each other. This feature of blockchain makes it hard for an attacker to intercept communication between patients and doctors, and protect against data analysis/sniffing [10, 13]. Blockchain maintains pseudo-anonymity, the patients and their medical data is linked with a public address. Also, the data processing on a blockchain is completely anonymous [10]. Thus, blockchain anonymises the medical data in blockchain-based healthcare applications to hide the actual identity [30].

3.6 Single point failure

Similar to other systems, in healthcare, the attacker locates the flaw in the design, implementation or configuration of the system's centralised dependency component and disables it, essentially shutting down the whole system.

Vulnerabilities: Currently, the healthcare system uses a *centralised server model* [9, 25] that could pose a threat of single-point failure and performance bottleneck. The *weak implementation of a system to handle large numbers of requests* [25] gives an opportunity to the attacker to target the server and services of the system to halt them for legit users.

Countermeasures: Blockchain is resilient to single point failure with the advantage of a decentralised P2P network [9, 28]. Moreover, blockchain-based applications do not rely on a single or central point server/service [9, 25].

3.7 Repudiation

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

Vulnerabilities: In centralised healthcare systems, there are *weak controls to prove illegal data changes by authorised users* [31]. 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, during data processing, unintentional data changes can happen that later are not traceable.

The centralised healthcare systems manage *centralised mutable logs* [32] that are handled (or have access) by a system administrator or other IT staff. Also, if the system is compromised then the attacker can easily remove the actions he performed from logs. Therefore, the authenticity of logs can not be proved on centralised systems.

Countermeasures: Blockchain keeps immutable logs [32] to track who and when the particular operation was performed. Also, the authors [31] 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 [28].

Vulnerabilities: In centralised healthcare systems, there is a *lack of proper authenticity* [23] to verify the insurance claim because of rigid/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 decentralised verification of insurers based on the predefined set of rules [23] before registering on the ledger. Once the insurer is verified and registered then 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 trials frauds [33] 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 [33]. In centralised healthcare systems, *inadequate clinical trials data* [23] issues emerge because of lack of data integrity and provenance, *inefficiencies in patient recruitment and access to patient's medical data* [28].

Countermeasures: The distributed nature and use of cryptography ensure data is authentic [23] . Also, blockchain provides data ownership to patients [18] to control the access of their data and once data is saved on the blockchain, it cannot be altered. Thus, eliminate the threat of clinical trial fraud.

3.10 Tampering device settings

The use of medical devices connected with the internet and the internet of things (IoT) enables healthcare professionals to be more watchful and connected with patients. Progressively, IoT is becoming the heart of digital healthcare, which introduces new security challenges.

Vulnerabilities: In healthcare, the *medical devices are subject to heedless settings* [34] (e.g., lack of network segmentation, insufficient access control, and reliance on legacy systems). The changes in device settings either intentional (e.g., attacker) or unintentional (e.g., authorised user) could lead to false readings that put the patient's life at risk.

Countermeasures: Blockchain follows the append-only structure to save data. Thus, device settings stored in blockchain are distributed and immutable [34].

3.11 Social engineering

According to [35] report, only 1% of cyber-attacks in the year 2019 exploited hardware or software vulnerabilities and 99% of cyber-attacks utilised some form of human intervention.

Vulnerabilities: In healthcare, employees/staff is one of the weakest points and the attackers use *social engineering techniques* [30] (e.g., phishing, fake identity, bating, honey trap, etc.) to target them to approach patient's medical data.

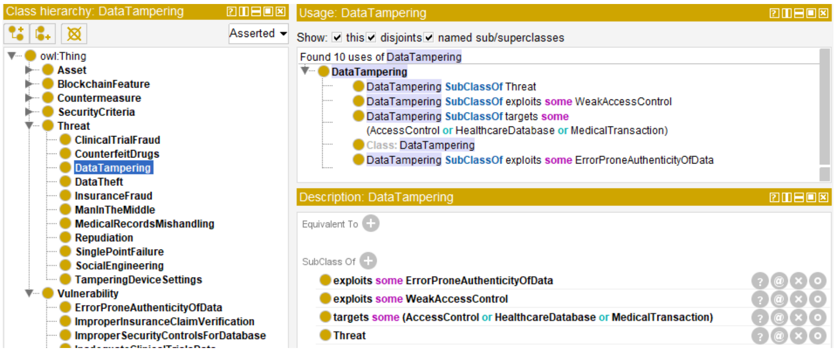
Countermeasures: As discussed above, blockchain implements smart contracts-based distributed access control [16] that ensures only relevant users have access to particular information or part of the information. Thus, unauthorised users can not access the medical data or other related sensitive information [18, 9].

4 Healthcare Security Ontology

Ontology elaborates the meaning of concepts within a domain to overcome the consequences of a misunderstanding. The authors [36] explain why to develop 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, v) analyse domain knowledge.

HealthOnt is based on web ontology language (OWL) and WWW Consortium (W3C). OWL is a semantic web language to illustrate rich and complex knowledge about things, their relations [37], and description logics (DL). DL deals with formal knowledge representation and provides a logical formalism for ontology. DL-based knowledge includes two components: i) Terminological component (TBox), and ii) Assertion component (ABox) [38]. OWL supports resource descriptive framework (RDF) to define metadata model [39] that supports triplet format (e.g., subject-predicate-object) for describing the ontology concepts. We build HealthOnt using Protege (Fig. 2) and SPARQL (SPARQL Protocol and RDF Query Language) as a semantic query language [40] to get results from an ontology. For example, the following SPARQL query gets the system assets from HealthOnt.

```
SELECT DISTINCT ?System_Asset  WHERE {
    ?System_Asset rdfs:subClassOf HealthOnt:SystemAsset
}
```


Class hierarchy: DataTampering
Asserted
Usage: DataTampering
Show: ☑ this ☑ disjoints ☑ named sub/superclasses
Description: DataTampering
Equivalent To
SubClass Of

owl:Thing
- Asset
- BlockchainFeature
- Countermeasure
- SecurityCriteria
- Threat
  - ClinicalTrialFraud
  - CounterfeitDrugs
  - DataTampering
  - DataTheft
  - InsuranceFraud
  - ManInTheMiddle
  - MedicalRecordsMishandling
  - Repudiation
  - SinglePointFailure
  - SocialEngineering
  - TamperingDeviceSettings
- Vulnerability
  - ErrorProneAuthenticityOfData
  - ImproperInsuranceClaimVerification
  - ImproperSecurityControlsForDatabase

Found 10 uses of DataTampering

DataTampering
- DataTampering SubClassOf Threat
- DataTampering SubClassOf exploits some WeakAccessControl
- DataTampering SubClassOf targets some (AccessControl or HealthcareDatabase or MedicalTransaction)
- Class: DataTampering
- DataTampering SubClassOf exploits some ErrorProneAuthenticityOfData

SubClass Of
- exploits some ErrorProneAuthenticityOfData
- exploits some WeakAccessControl
- targets some (AccessControl or HealthcareDatabase or MedicalTransaction)
- Threat

Fig. 2. Protege ontology editor

We utilise the **ontology construction method** [41] that has five stages: i) Identify purpose & scope, ii) Building ontology, it includes capture, coding and integrating phases, iii) evaluation, iv) documentation, and v) guidelines. In [42], we follow the same ontology construction method to explore and build an ontology for security threats of Corda-based financial applications.

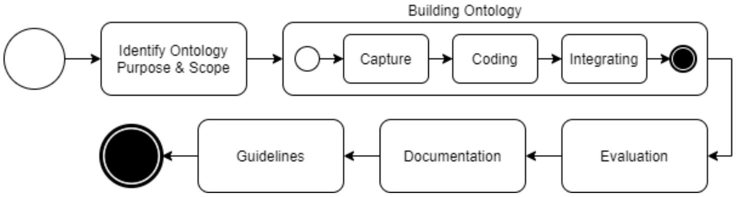


Fig. 3. Ontology construction method (adapted from: [41])

Scope and purpose: The instructions [36] help us to define the scope and purpose of our ontology. The purpose is to build a knowledge base of blockchain-enabled countermeasures for healthcare applications. The scope covers the *domain of ontology* (e.g., blockchain as a countermeasure solution), *use of ontology* (e.g., SRM of healthcare applications using blockchain), *questions that ontology answers* (e.g., what assets to protect, what are the threats, vulnerabilities, and countermeasures), *who will maintain the ontology?* (e.g., security experts).

Building ontology: We use Protege to capture and code domain knowledge (e.g., concepts and their relationships) into taxonomic classifications. The classifications refine the concepts belonging to assets, security criteria, threats, vulnerabilities, countermeasures, and blockchain features associated with countermeasures. The classifications related to *Threats*, *Vulnerabilities* and *Countermeasures* are available in this study and classifications of *Security criteria*, and *Blockchain features* are in the technical report [8].

Assets classification: Assets are classified as business and system (Fig. 4) assets. Security criteria is a constraint of business assets, and system assets support business assets. For example, business asset “MedicalRecord” hasConstraint Integrity, and System assets “AccessControl” supports “MedicalRecord”. The DL for relation “supports” and “hasConstraint” is:

```
supports some BusinessAsset / hasConstraint some SecurityCriteria
```

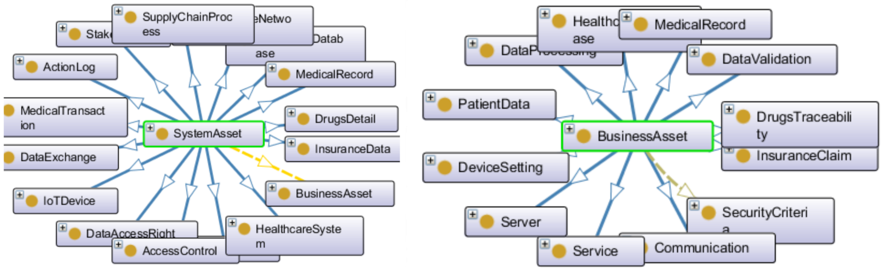


Fig. 4. Assets classification

The asset class definition explains sub-classes (e.g., SystemAsset and BusinessAsset) and restrictions “hasConstraint” and “supports”.

```
Class (Asset SubClass (SystemAsset BusinessAsset)
    SystemAsset supports someValuesFrom (BusinessAsset)
    BusinessAsset hasConstraint someValuesFrom (SecurityCriteria)
)
```

Threats classification: Security threats classification (Fig. 5) is built upon the threats that are mitigated using blockchain. In traditional healthcare applications, security threats exploit vulnerabilities and target some system asset(s).

Threat class has a restriction "exploits" on someValuesFrom the Vulnerability. Another restriction "targets" on someValuesFrom the SystemAsset. The DL for relation "exploits" and "targets" is:

```
exploits some Vulnerability / targets some SystemAsset
```

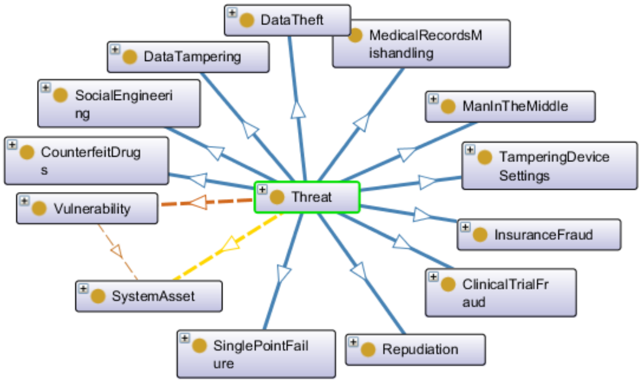


Fig. 5. Security threats classification

```
Class (Threat SubClass ( DataTampering DataTheft .... )
    restriction ( exploits someValuesFrom (Vulnerability) )
    restriction ( targets someValuesFrom (SystemAsset) )
)
```

For example, in traditional healthcare applications, the attacker can trigger "DataTampering" threat by exploiting a vulnerability "ErrorProneAuthenticityOfData" or "WeakAccessControl". The "DataTampering" threat targets the system assets (e.g., AccessControl, HealthcareDatabase, & MedicalTransaction).

Vulnerabilities classification: Vulnerabilities classification (Fig. 6) is built by identifying the weaknesses within the traditional healthcare applications that enable a particular security threat. A vulnerability is a characteristic of system asset(s) and negates the security criteria of a business asset(s). The DL for relation "characteristicOf" and "negates" is:

```
characteristicOf some SystemAsset / negates some SecurityCriteria
```

The vulnerability class definition explains various vulnerabilities that are characteristic of system assets and negates the security criteria of business assets.

```
Class (Vulnerability SubClass (
        WeakAccessControl ErrorProneAuthenticityOfData ....
    )
    restriction ( negates someValuesFrom (SecurityCriteria) )
    restriction ( characteristicOf someValuesFrom (SystemAsset) )
)
```

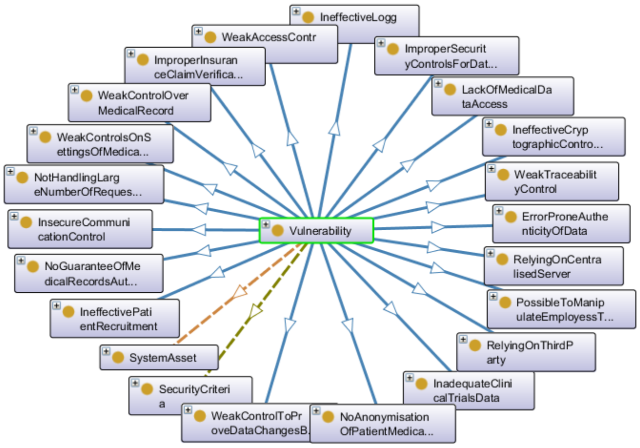

IneffectiveLogg
WeakAccessContr
ImproperSecurit yControlsForDat...
ImproperInsuran ceClaimVerifica...
LackOfMedicalDa taAccess
WeakControlOver MedicalRecord
IneffectiveCryp tographicContro...
WeakControlsOnS ettingsOfMedica...
WeakTraceabilit yControl
NotHandlingLarg eNumberOfReques...
ErrorProneAuthe nticityOfData
InsecureCommuni cationControl
Vulnerability
RelyingOnCentra lisedServer
NoGuaranteeOfMe dicalRecordsAut...
PossibleToManip ulateEmployessT...
IneffectivePati entRecruitment
RelyingOnThirdP arty
SystemAsset
InadequateClini calTrialsData
SecurityCriteri a
WeakControlToPr oveDataChangesB...
NoAnonymisation OfPatientMedica...

Fig. 6. Vulnerabilities classification

For example, the weak implementation of access control presents a weakness that the attacker can exploit and get unauthorised access. A vulnerability "WeakAccessControl" is a characteristicOf "SystemAsset" (AccessControl, HealthcareDatabase) and negates some (Integrity or Confidentiality).

Countermeasures classification: Countermeasures classification (Fig. 7) presents the counteract that mitigates the vulnerabilities and improves the security of the system. The countermeasures belong to the blockchain features. The DL for relation "belongsTo" and "mitigates" is:

```
belongsTo some BlockchainFeature / mitigates some Vulnerability
```

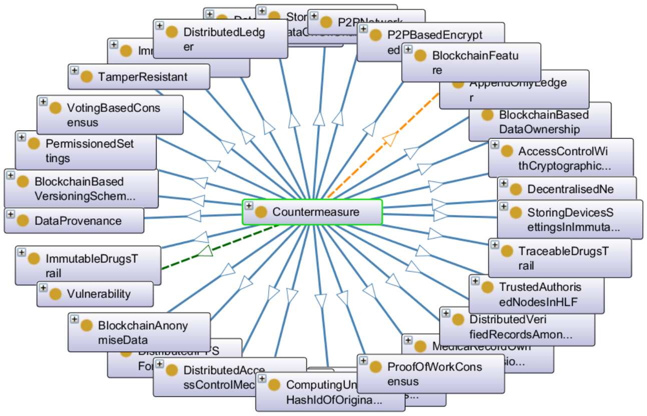


Fig. 7. Countermeasures classification

Countermeasure class definition explains that it contains various countermeasures that belong to blockchain features and mitigates various vulnerabilities. For example, the countermeasure "DistributedAccessControlMechanism" belongs to "DistributedAccessControl" feature and mitigates the "WeakAccessControl" vulnerability in traditional healthcare applications.

```
Class (Countermeasure SubClass (
        DistributedAccessControlMechanism DistributedLedger ....
    )
    restriction ( belongsTo someValuesFrom (BlockchainFeature) )
    restriction ( mitigates someValuesFrom (Vulnerability) )
)
```

Security criteria: Security criteria classification (Fig. 8) is based on the concepts of CIA triad. Security criteria represent the constraint of business assets. The relation "constraintOf" is an inverse of "hasConstraint". For example, security criteria "Integrity" is a constraint of business asset "MedicalRecord", the same example is presented in Asset classification with the "hasConstraint" relation. The DL for relation "constraintOf" is:

```
constraintOf some BusinessAsset
```

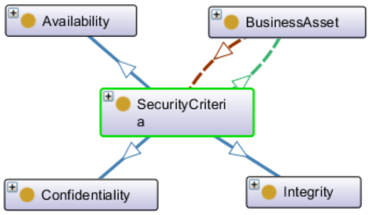


Fig. 8. Security criteria classification

If a security expert wants to explore security criteria of business assets, he can browse to HealthOnt to examine class definition. The class definition of SecurityCriteria is:

```
Class (SecurityCriteria SubClass (
        Confidentiality Availability Integrity
    )
    restriction ( constraintOf someValuesFrom (BusinessAsset) )
)
```

The definition explains a class SecurityCriteria has subclasses (e.g., Confidentiality, Availability, Integrity) and a restriction "constraintOf" on someValuesFrom the BusinessAsset. The someValuesFrom restriction presents that security criteria is not a constraint of all the business assets.

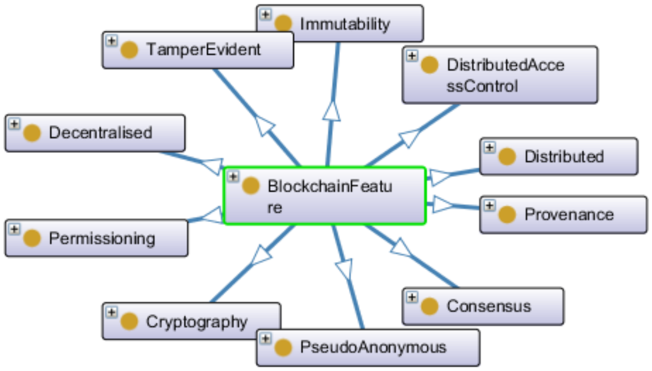


Fig. 9. Countermeasures classification

Blockchain feature classification: The classification (Fig. 9) of blockchain features presents the characteristics that are associated with blockchain-based countermeasures. The blockchain features are explained in Table **??**.

For example, the countermeasure "DistributedAccessControlMechanism" belongs to "DistributedAccessControl" feature.

```
Class (BlockchainFeature SubClass (
        DistributedAccessControl Immutability Provenance ....
    )
)
```

Ontology documentation: Inadequate documentation is the main barrier to effective knowledge sharing and understanding the ontology [43]. In order to overcome this issue, we document all the important assumptions and concepts, for example, the classes and sub-classes defined in the ontology, relations, individuals and meta-ontology to clarify what ontology is about and to interpret the meaning of ontological claims. Also, we use the Protege annotation properties to document the terms (e.g., for classes, relations and individuals) separately that we used to build our ontology.

Ontology usage guidelines: This section belongs to the usage of ontology that explains how to use, integrate or extend this ontology. The guidelines include the resources of HealthOnt (Table 3) and educate the users that are not familiar with OWL or OWL-based tools. Our ontology is created by using Protege ontology editor and the ontology is available and accessible online. We use the OntoGraf Protege plugin to generate classifications graphs and the Pellet reasoner to validate the consistency of our ontology. We also use PyLODE[1] (Python Live OWL Documentation Environment) tool to make a human-readable form of ontology that give intuitive look to understand the encoded concepts within ontology and OWLGrEd[2] ontology visualisation tool to present a graphical look of HealthOnt.

[1] https://github.com/rdflib/pyLODE
[2] http://owlgred.lumii.lv/

In order to use HealthOnt, first, install Protege and open ontology. Second, retrieve information from ontology using SPARQL queries. The HealthOnt could be integrated with other security ontologies, HealthOnt is available online and could be extended.

Table 3. HealthOnt resources

Resource	**Resource URL**
HealthOnt	`https://mmisw.org/ont/~mubashar/HealthOnt`
GitHub	`https://github.com/mubashar-iqbal/HealthOnt`
Protege	`https://protege.stanford.edu/`
OntoGraf	`https://protegewiki.stanford.edu/wiki/OntoGraf`
Pellet Reasoner	`https://protegewiki.stanford.edu/wiki/Using_Reasoners`
PyLODE	`https://mmisw.org/pylode?url=https://mmisw.org/ont/~mubashar/HealthOnt`
OWLGrEd	`http://owlgred.lumii.lv/online_visualization/jfns`

5 Ontology Evaluation

We use the task-based [44] evaluation technique. This technique allows learning about HealthOnt applicability. The efficient evaluation technique contributes to the scientific value of ontology. For instance, consider healthcare security experts working on a healthcare application or a healthcare organisation looking at viable solutions to address the security threats associated with medical data tampering and theft. Due to the conceptual ambiguity and semantic gaps, both the healthcare security experts and organisation are unaware of the blockchain's countermeasures to mitigate both security threats.

In this case, HealthOnt supports the selection of blockchain to mitigate both threats in traditional healthcare applications and determine what assets to protect. Also, HealthOnt can assist the conceptual design and technological implementation of both security threats. For example, HealthOnt helps to identify the vulnerabilities of security threats, assets (business and system assets) to protect, and blockchain-based countermeasures.

The SPARQL queries can be used to retrieve information from an ontology. The following header code will remain the same for all the queries listed in this section.

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX HealthOnt: <https://mmisw.org/ont/~mubashar/HealthOnt#>
```

The SPARQL **Query #1** retrieves the security threats related to data tampering & theft, their vulnerabilities, and assets to protect from HealthOnt. The query compiles results based on the defined relationships *(exploits and targets)*. For example, **Threat** (DataTampering) *exploits* **Vulnerability** (WeakAccessControl), and **Vulnerability** (WeakAccessControl) *targets* **SystemAsset** (AccessControl or HealthcareDatabase or MedicalTransaction). Similar results for DataTheft and other security threats (reference Table 2).

```
Query# 1 SELECT ?Threat ?Vulnerability ?SystemAsset WHERE {
    ?Threat rdfs:subClassOf ?Vulnerability .
    ?Threat rdfs:subClassOf ?SystemAsset .
    ?Vulnerability owl:onProperty HealthOnt:exploits .
    ?SystemAsset owl:onProperty HealthOnt:targets .
    ?Threat rdfs:label ?FilterByThreat .
    FILTER regex(?FilterByThreat, "DataTampering|DataTheft") .
}
```

The SPARQL **Query #2** retrieves the countermeasures and vulnerabilities that are associated with data tampering & theft. The query fetch results based on the relationship *(mitigates)*. For example, **Countermeasure** (DistributedAccessControl) *mitigates* **Vulnerability** (WeakAccessControl). Similar results for DataTheft and other security threats (reference Table 2).

```
Query# 2 SELECT ?Countermeasure ?Vulnerability WHERE {
    ?Countermeasure rdfs:subClassOf HealthOnt:Countermeasure .
    ?Countermeasure rdfs:subClassOf  ?Vulnerability .
    ?Vulnerability owl:onProperty HealthOnt:mitigates .
    ?Countermeasure HealthOnt:Mitigates ?FilterByThreat .
    FILTER regex(?FilterByThreat, "^DataTampering|DataTheft") .
}
```

The SPARQL **Query #3** retrieves system assets that support business assets.

```
Query# 3 SELECT DISTINCT ?System_Asset ?Supports_Business_Asset  WHERE {
    ?System_Asset rdfs:subClassOf HealthOnt:SystemAsset .
    ?System_Asset rdfs:subClassOf ?Supports_Business_Asset .
    ?Supports_Business_Asset owl:onProperty HealthOnt:supports .
}
```

The SPARQL **Query #4** gets the business assets that have security criteria constraints.

```
Query# 4 SELECT DISTINCT ?Business_Asset ?Constraint  WHERE {
    ?Business_Asset rdfs:subClassOf HealthOnt:BusinessAsset .
    ?Business_Asset rdfs:subClassOf ?Constraint .
    ?Constraint owl:onProperty HealthOnt:hasConstraint .
    { ?Constraint owl:someValuesFrom HealthOnt:Confidentiality . }
    UNION
    { ?Constraint owl:someValuesFrom HealthOnt:Integrity . }
    UNION
    { ?Constraint owl:someValuesFrom HealthOnt:Availability . }
}
```

References

1. Kitchenham, B., Charters, S.: Guidelines for Performing Systematic Literature Reviews in Software Engineering. (2007)
2. Okoli, C.: A Guide to Conducting a Standalone Systematic Literature Review. In: Communications of the Association for Information Systems (2015)
3. Fink, A.: Conducting Research Literature Reviews: From the Internet to Paper. In: SAGE Publications, Inc (2019)
4. Levy, Y., J. Ellis, T.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. In: Informing Science: The International Journal of an Emerging Transdiscipline (2006) 181–212
5. Dubois, É., Mayer, N., Heymans, P., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering (2010) 289–306
6. Matulevičius, R.: Fundamentals of Secure System Modelling. 1 edn. Springer International Publishing (2017)
7. Ganji, D., Privacy, C.K., Mouratidis, H., Gheytassi, S.M.: Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review. In: International Journal on Advances in Software (2019) 228–238
8. Iqbal, M., Matulevičius, R.: Blockchain as a Countermeasure Solution forSecurity Threats of Healthcare Applications (Technical report) (2021) `https://github.com/mubashar-iqbal/HealthOnt`.
9. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., Yu, N.: Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. In: IEEE Internet of Things Journal (2019) 8770–8781
10. Yaqoob, I.: Blockchain for healthcare data management: opportunities, challenges, and future recommendations. In: Neural Computing and Applications (2021)
11. Bhuiyan, Z.A., Wang, T., Wang, G.: Blockchain and Big Data to Transform the Healthcare. (2018) 2–8
12. Han, H., Huang, M., Zhang, Y.: An Architecture of Secure Health Information Storage System Based on Blockchain Technology. In: ICCCS (2018) 578–588
13. Chen, J., Ma, X., Du, M., Wang, Z.: A Blockchain Application for Medical Information Sharing. In TEMS-ISIE (2018) 1–7
14. Hussein, A.F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J.M.R., de Albuquerque, V.H.C.: A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. In: Cognitive Systems Research (2018) 1–11
15. Du, M., Chen, Q., Chen, J., Ma, X.: An Optimized Consortium Blockchain for Medical Information Sharing. In: IEEE Transactions on Engineering Management (2020) 1–13
16. Francesco, D., Ricci, L., Iit-cnr, P.M.: Distributed Access Control Through Blockchain Technology Blockchain
17. Esposito, C., Tortora, G., Chang, H., Choo, R.: Blockchain : A Panacea for Healthcare Cloud-Based Data Security and Privacy? (2018) 31–37
18. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. In: Sustainable Cities and Society (2018) 283–297
19. HIPAA: 2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020 (2021) `https://bit.ly/3uN16BN`.

20. Hathaliya, J.J., Tanwar, S.: An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications (2020) 311–335
21. Wang, G.: MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In: SpaCCS (2017) 534–543
22. Zabel, L.: 10 common HIPAA violations and preventative measures to keep your practice in compliance (2016) `https://bit.ly/34E8Hrx`.
23. Martino, F.D.D., Klein, S.D., Neil, J.O., Huang, Y., Nisson, L., Race, M.: Transforming the U . S . Healthcare Industry with Blockchain Technology. (2019) 1–7
24. Thielman, S.: Your private medical data is for sale – and it's driving a business worth billions (2017) `https://bit.ly/3ceaacp`.
25. Shi, S., He, D., Li, L., Kumar, N., Khurram, M.: Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. In: Computers & Security (2020)
26. Dexter, S.: How Are Blockchain Transactions Validated? Consensus VS Validation (2018) `https://www.mangoresearch.co/blockchain-consensus-vs-validation`.
27. Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., Njilla, L.: Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack. In: 17th IEEE/ACM International Symposium CCGRID (2017) 458–467
28. Ramya, N., Narikimilli, S., B, A.K., Antu, A.D.: Blockchain Applications in Healthcare – A Review and Future Perspective. In: ICBC (2020)
29. SpecOpsSoft: The countries experiencing the most 'significant' cyber-attacks (2020) `https://bit.ly/3idba4m`.
30. Ali, M.S., Vecchio, M., Putra, G.D., Kanhere, S.S., Antonelli, F.: A decentralized peer-to-peer remote health monitoring system. Sensors (Switzerland) (2020) 1–18
31. Kleinaki, A.S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P.S., Kaldoudi, E.: A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. Computational and Structural Biotechnology Journal (2018) 288–297
32. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of Medical Systems (2018) 1–7
33. George, S.L., Buyse, M.: Data fraud in clinical trials. Clinical Investigation (2015) 161–173
34. Mcghin, T., Choo, K.k.R., Zhechao, C., He, D.: Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications (2019) 62–75
35. HelpNetSecurity: More than 99% of cyberattacks rely on human interaction (2019) `https://bit.ly/3uL3CYW`.
36. Noy, N.F., McGuinness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology. in: Stanford Knowledge Systems Laboratory (2001) 1–25
37. Group, O.W.: Web Ontology Language (OWL) `https://www.w3.org/OWL`.
38. Gao, J.B., Zhang, B.W., Chen, X.H., Luo, Z.: Ontology-based model of network and computer attacks for security assessment. In: Journal of Shanghai Jiaotong University (2013) 554–562
39. Hector, U.R., Boris, C.L.: BLONDiE: Blockchain Ontology with Dynamic Extensibility. (2020)
40. Herzog, A., Shahmehri, N., Duma, C.: An Ontology of Information Security. In: IJISP (2007) 1–23
41. Uschold, M., Gruninger, M.: Ontologies : Principles , methods and applications. Knowledge Engineering Review (1996)
42. Iqbal, M., Matulevičius, R.: Corda security ontology: Example of post-trade matching and confirmation. In: Baltic Journal of Modern Computing (2021) 638–674

43. Skuce, D.: Conventions for reaching agreement on shared ontologies. In: Proc. 9th Banff Knowledge Acquisition for Knowledge-Based Systems Workshop, Banff Conference Centre, Banff, Alberta, Canada (1995)
44. Raad, J., Cruz, C.: A Survey on Ontology Evaluation Methods. HAL archives-ouvertes (2018)