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". The paper is accepted for BPM 2021 Blockchain Forum.

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 *(EC)*. 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.

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

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 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.

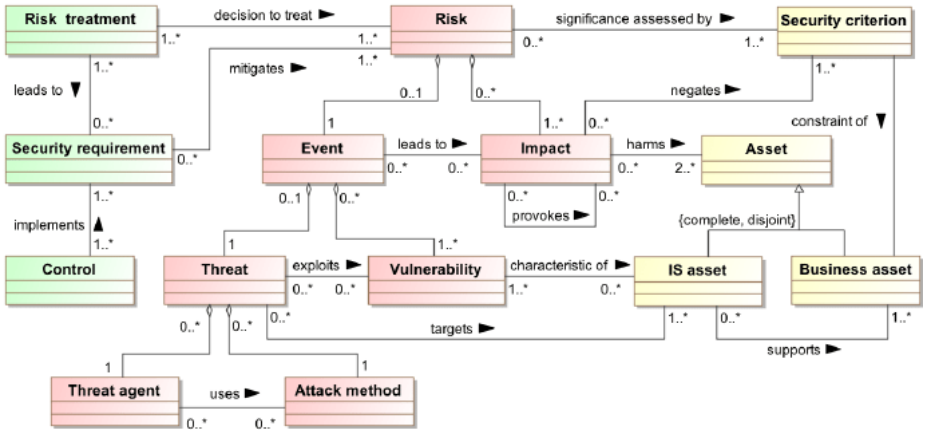

Fig. 1. The SRM domain model [adapted from: [5, 6]]

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 to protect, and blockchain-based countermeasures. In this section, we discuss the remaining six security threats in detail *(e.g., single-point failure, repudiation, insurance frauds, clinical trial fraud, tampering device settings, social engineering)*. The first five security threats *(e.g., data tampering, data theft, medical records mishandling, counterfeit drugs, man-in-the-middle)* are already discussed in the accepted paper *"Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications"*.

3.1 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* [8, 9] that could pose a threat of single-point failure and performance bottleneck. The *weak implementation of a system to handle large numbers of requests* [9] 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 [8, 10]. Moreover, blockchain-based applications do not rely on a single or central point server/service [8, 9].

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-anonymous
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	Clinical trial 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 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* [11]. 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* [12] 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 [12] to track who and when the particular operation was performed. Also, the authors [11] use the blockchain-based versioning scheme to track each performed operation over time.

3.3 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 [10].

Vulnerabilities: In centralised healthcare systems, there is a *lack of proper authenticity* [13] 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 [13] 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.

3.4 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 [14] 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 [14]. In centralised healthcare systems, *inadequate clinical trials data* [13] issues emerge because of lack of data integrity and provenance, *inefficiencies in patient recruitment and access to patient's medical data* [10].

Countermeasures: The distributed nature and use of cryptography ensure data is authentic [13] . Also, blockchain provides data ownership to patients [15] 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.

3.5 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* [16] (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 [16].

3.6 Social engineering

According to [17] 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* [18] (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 [19] 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 [15, 8].

4 Healthcare Security Ontology

Ontology elaborates the meaning of concepts within a domain to overcome the consequences of a misunderstanding. The authors [20] 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 [21], 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) [22]. OWL supports

resource descriptive framework (RDF) to define metadata model [23] 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 [24] 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
}
```

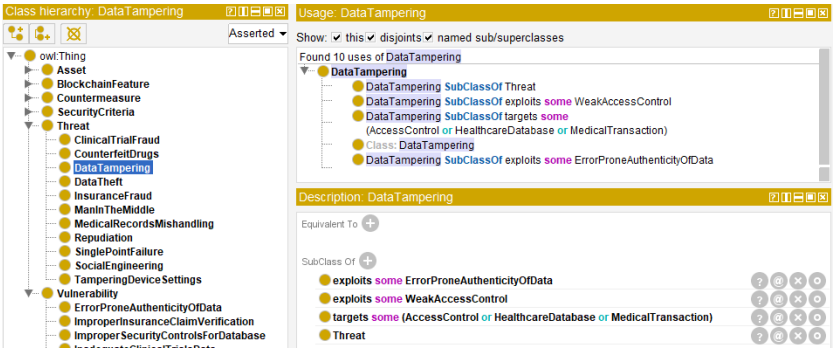

Fig. 2. Protege ontology editor

We utilise the **ontology construction method** [25] 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 [26], we follow the same ontology construction method to explore and build an ontology for security threats of Corda-based financial applications.

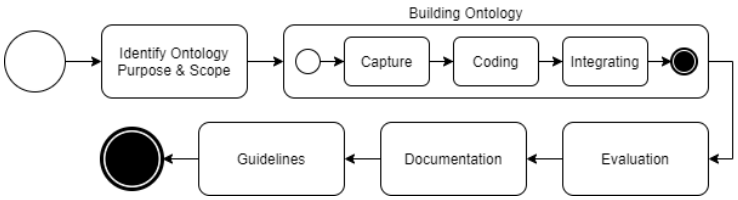

Fig. 3. Ontology construction method (adapted from: [25])

Ontology documentation: Inadequate documentation is the main barrier to effective knowledge sharing and understanding the ontology [27]. 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 (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 ontology visualisation tool to present a graphical look of HealthOnt. 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`

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. 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
9. 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)
10. Ramya, N., Narikimilli, S., B, A.K., Antu, A.D.: Blockchain Applications in Healthcare – A Review and Future Perspective. In: ICBC (2020)
11. 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
12. 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
13. 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
14. George, S.L., Buyse, M.: Data fraud in clinical trials. Clinical Investigation (2015) 161–173
15. 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
16. 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
17. HelpNetSecurity: More than 99% of cyberattacks rely on human interaction (2019) `https://bit.ly/3uL3CYW`.
18. 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
19. Francesco, D., Ricci, L., Iit-cnr, P.M.: Distributed Access Control Through Blockchain Technology Blockchain
20. Noy, N.F., McGuinness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology. in: Stanford Knowledge Systems Laboratory (2001) 1–25
21. Group, O.W.: Web Ontology Language (OWL) `https://www.w3.org/OWL`.
22. 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
23. Hector, U.R., Boris, C.L.: BLONDiE: Blockchain Ontology with Dynamic Extensibility. (2020)
24. Herzog, A., Shahmehri, N., Duma, C.: An Ontology of Information Security. In: IJISP (2007) 1–23
25. Uschold, M., Gruninger, M.: Ontologies : Principles , methods and applications. Knowledge Engineering Review (1996)

26. Iqbal, M., Matulevičius, R.: Corda security ontology: Example of post-trade matching and confirmation. In: Baltic Journal of Modern Computing (2021) 638–674
27. 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)