eHEALTHCARE SECURITY CONCEPT BASED ON PKI AND BLOCKCHAIN TECHNOLOGY

Dejan Cizelj,
Tomislav Unkašević*,
Zoran Banjac

Institute VLATACOM,
Belgrade, Serbia

Abstract:

Technological advances in information and communication technologies induce the inevitable automation of life processes. The transition of social and business activities to cyberspace has brought a new quality to everyday life, but at the same time, it has produced new challenges in the field of data protection. One of the areas where this issue is particularly sensitive is the field of healthcare. Unauthorized access to a patient's data can cause many almost insurmountable problems in life, ranging from theft and identity abuse to putting them in an unequal life situation compared to insurance companies, credit and banking systems, transportation systems, and many other life situations. In this paper, the concept of eHealthcare data protection based on PKI and Blockchain technology is proposed. PKI technology ensures reliable identification of all entities in the system by applying digital certificates of the appropriate type and controlling data integrity at the time of creation. Blockchain technology ensures the integrity of data in time in the sense that data entered into the blockchain cannot be changed, deleted, or inserted into new ones without violating a chaining structure.

Finally, it was shown that the electronic healthcare information system based on these principles is compatible with the GDPR of the European Union. The proposed principles are also in line with the main directions of designing secure information systems known under the name zero trust information systems.

Keywords:

eHealthcare, Information Security, PKI, Blockchain, Digital Certificate.

INTRODUCTION

Technological advances made in the past few decades in the field of information and communication technologies, sensors, microprocessor devices, and the application of software solutions and artificial intelligence have enabled tremendous progress in people's daily lives. By transferring business and life processes into the digital space, a symbiosis of machines and people was formed - Cyberspace. Progress is reflected in the efficiency of the implementation of processes, reducing their costs and the necessary time for implementation. Digitalization of business and life processes as an essential prerequisite has an unambiguous identification of participants and their rights to participate in this process.

Correspondence:
Tomislav Unkašević

e-mail:
tomislav.unkasevic@vlatacom.com

DOI: 10.15308/Sinteza-2023-85-93

In this context, the challenges of information security within these processes come into play. An impressive example of this is the healthcare system [1].

In the healthcare system data collection, storage, and processing, as well as in all complex systems, is the basis of their functioning. Data are collected on patients, their ailments, the results of medical procedures, treatment, and the results of therapeutic procedures. In addition, records of personnel in the system and their role, services provided and charged, the state of resources and medical infrastructure, and many other data are kept. Managing this data is a serious challenge from the point of view of its role, privacy, and availability. Therefore, information security plays an essential role in this system because it ensures confidentiality, integrity, and availability of data. Confidentiality protects the identity of the user and his medical data as well as all the sensitive data of the healthcare system. Integrity achieves credibility of registered data and availability ensures access to data and resources at the time they are needed. For the realization of these functionalities, it is essential to have reliable and verifiable electronic identities, manage them and ensure data integrity.

This paper presents the concept of information security in healthcare systems based on digital certificates as a method of identification of entities and Blockchain technology as a means of maintaining the integrity of information in communications and time.

The paper consists of an introduction after which, in the second part, the nature of information in the infrastructure information system is discussed, the importance of their protection, and the preservation of their integrity. This section describes techniques for identifying and preserving data integrity relevant to this concept. The third part describes the concept of protection of the information healthcare system and the scenario of its implementation. In the end, the security characteristics of the proposed concept are presented. In the final part of the paper, a conclusion is given and then the references used in this paper are listed.

2. E-HEALTHCARE INFORMATION AND SECURITY

An electronic healthcare system is created by applying Information and Communication Technologies in the process of healthcare. This involves networking of medical sensors, devices, and entities in the healthcare system to more efficiently collect information, and apply business, patient surveillance, and health procedures. For an individual to enjoy health care, they must agree to the collection and use of necessary information as part of medical procedures, such as test results, medical staff notes, or even the use of technological devices that allow patients to register their health status in the process of examination, self-monitoring or treatment [2]. This information, to a greater extent, is collected by professionals, organizations, and the state administration for research purposes, necessary administration, and other business reasons. As can be seen, it is private patient data, and unauthorized access to such information can be harmful to both the person and the system. In many cases, scammers or cybercriminals exploit health data to create false identities to buy medicines, medical equipment, and even health insurance fraud [3]. On the other hand, there is an objective need to access these data not only for the treatment of the patient but also for the needs of the state administration, research projects, and more. This approach must be strictly controlled and under the conditions regulated by law and this is the point at which information security comes into play.

A modern approach in the organization of health care is directed towards the patient and the patient directly decides on the use of personal medical data, [4]. This approach is fully in line with the basic postulates of modern data and information systems protection based on the approach that each entity (devices, people, software, and hardware) has a unique identification in the health information system. The system keeps precise records of who, when, and what did so that in the event of incident detection, the system's operating records enable the responsible entities identification and undertake the necessary recovery activities. For records to be credible in an electronic health system, all entities must possess a unique identity that cannot be falsified and the record of events in the system must be so realized that it is impossible to falsify it in the sense of unauthorized changes.

This paper will present the concept of a security solution based on asymmetric cryptography and digital electronic certificates as a way to establish a unique electronic identity in the digital world and blockchain technology for securing and verifying the integrity of data.

2.1. DIGITAL IDENTITY AND PKI

To realize any form of organization in the electronic world, it is necessary to have mechanisms for identifying and distinguishing the entities that makeup it. The discovery of asymmetric cryptography created the conditions for creating electronic identities using digital certificates, [5], [6]. The identity of the entities in the system (people, devices, software) is defined by the public key of the selected asymmetric cryptographic algorithm. Correspondence between the physical identity of an entity and its electronic identity is achieved by issuing a digital certificate that establishes a unique link between physical and electronic identity. Digital certificates are issued by an authorized certification authority within the legally identifiable public key infrastructure (PKI). The accuracy and integrity of the data contained in the digital certificate are guaranteed by the certification body that issues the digital certificate with its electronic signature. Hence it follows that one entity may belong to multiple PKI systems and for the sake of interoperability there should be a standardized model of issuance and format of electronic certificates. To this end, standard digital certificate formats used in the digital world have been defined, for example, ITU-T X.509, ISO/IEC 9594-8, [7]. The profile of the digital certificate according to this standard is shown in Table 1 (a).

As we have mentioned earlier, a health information system is a complex information system of heterogeneous devices (sensors, wearable devices, various types of mobile devices, complex medical devices...) so the application of this universal standardization carries with it several conditionally stated difficulties:

- The size of a standard digital certificate is about two kilobytes, [8]; and
- Digital certificates under this standard, in general, can have a very complex structure due to recursive definitions in the standard and potentially pose a problem for devices with limited resources (sensors, mobile devices ...) in terms of memory and available energy.

To overcome these problems in [8], [9] a different digital certificate profile has been proposed based on the idea of reducing the complexity of the description and consequently the need for smaller storage memory and power for processing. The main characteristics of the described CBOR, [10], profile are given by:

- The proposed profile is compatible with X.509.V3;
- A fixed asymmetric algorithm (ECDSA With SHA256) is used for electronic signature; and
- All entity names are explicit, simpler than allowed naming per X.500 standard

The CBOR certificate profile format is shown in Table 1 (b).

Table 1 - Certificate profile format.

(a)		
Standard X.509 certificate profile		
Field		**Content description**
Version		X.509 Version of certificate
Serial Number		Serial number of the certificate
Signature Algorithm ID		Identification of the signature algorithm
Issuer (CA) name		X.500 Name of the certificate issuer
Validity Period		(beginning date, ending date)
Subject name		Certificate owner X.500 name
Subject Public Key Info	Algorithm ID	Public key algorithm ID
	Public Key Value	Value of the public key
Issuer Unique ID		Identification of the certificate issuer
Subject Unique ID		Identification of the certificate owner
Extension		Additional information
CA Digital Signature		Digital signature of the certificate by CA

(b)	
CBOR X.509 certificate profile for IoT	
Field	**Content description**
Version	Fixed to 3
Serial Number	Unsigned integer
Signature Algorithm	ECDSA With SHA256
Issuer (CA) name	EUI-64 as UTF8 String
Validity Period	UTCTime
Subject name	EUI-64 as UTF8 String
Public Key Value	ecPublicKey followed by secp256r1 and 64-byte uncompressed ECC public key
Issuer Unique ID	Not present
Subject Unique ID	Not present
Extension	Additional information
CA Digital Signature	ECDSA With SHA256 Sig value

The management of this type of certificate can theoretically take place in the same way as the management of certificates according to the X.509 V3 standard. This is supported by the fact that these devices are applied in the health system and at the time of use must have connectivity to the system

2.2. BLOCKCHAIN TECHNOLOGY

Blockchain technology in the literature has different definitions but can best be described from the point of view of data structures as a linked list of blocks of data that form a collection of records called a Ledger. The Ledger is not stored in a classic way as a memory object or a static database but is an object that is stored as its multiple copies within different computers/information systems, possibly geographically distant. Synchronization and integrity of data in the Ledger are realized by applying the protocol for managing the blocks, the way of creating new blocks, and the conditions of their entry in the Ledger list. These protocols based on the use of cryptographic mechanisms ensure the integrity of the blocks constructed in such a way that it is almost impossible to falsify/change the Ledger and enter unverified data into it. Any attempt to enter incorrect blocks in the Ledger is easily detected and the entry of such blocks in the list is not allowed. Connecting data blocks in a specific way with the use of cryptographic electronic signature mechanisms and hash functions allow powerful protection of the integrity of the Ledger [11], [12].

The method of entering blocks in Ledger can be recognized as

1. public blockchains;
2. private blockchains;
3. consortium blockchains; and
4. hybrid blockchains.

2.2.1. Block structure

Each block has two separate parts one part consists of the transaction/data that the block contains and the second part of the block makes up its header. Each transaction/data is electronically signed by the transaction initiator and by the transaction/data creator. The block header consists of the following fields:

- Merkel hash represents the hash value of all transactions carried by a block and allows you to easily and quickly check whether a transaction belongs to the block or not;
- The hash value of the previous block represents the hash value of the header of the previous block and the control data to check the integrity of the previous block;
- A timestamp is data on the time of the creation of a block that is electronically signed by the competent authority; and
- The system weight factor and random value are the data involved in reaching a consensus on whether a newly formed block is valid for entry in a bookkeeping list.

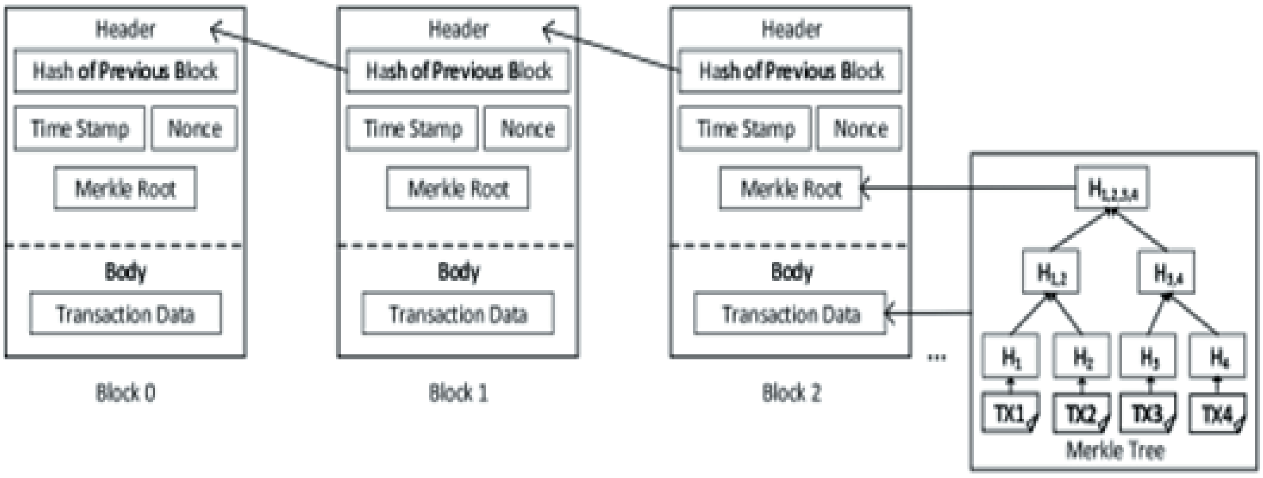

Figure 1 - Illustration for block structure and blockchain, [13].

2.2.2. Creating correct blocks for entry in the Ledger

The data contained in the transaction part of the block may be different by its nature and may also have different origins and storage locations.

2.2.2.1. Entering a block in a public blockchain

The data source is available to all entities that want to try to form a list entry block and the process proceeds as follows:

1. The creator of the candidate block selects from the data set a certain number of data to include in the block as data. She then constructs their Merkel hash and writes the time in the timestamp field;
2. In the hash value box of the previous block, writes the hash value of the previous block;
3. In the field for the weight factor enters its value;
4. It selects a random number, at its discretion, and writes it into a random value field; and
5. The hash function calculates the hash value of the candidate block header. If the resulting value is less than the weight factor, the creator has found the correct block and forwarded it to the community for verification. If the value is not less than the weight factor, it goes back to step 4.

When other members of the community receive a candidate for admission to the linked list, they conduct a check on him or her as follows:

1. Check whether the hash field of the previous block contains the hash value of the last block entered in the sheet. This prevents inconsistent copies of a linked list from appearing. If the check is negative, the candidate is discarded;
2. It is checked whether all data contained in the candidate block exists in the data source and if not, the candidate is discarded as defective;
3. The value of Merkel's hash for the bloc is checked and if the check is negative, the candidate is rejected;
4. It is checked whether the hash value of the block header is less than the weight ingestion factor. If the check is negative, the candidate is discarded; and
5. If all checks are positive, the block is written to the linked list, and the data that makes it up is deleted from the data source.

The process of constructing a block so that its hash value is less than the weight factor is called Proof-of-work and is proof that the block is formed correctly. In digital currency systems, constructors of the correct blocks that are entered in the linked list receive financial compensation. For details about various mechanisms created block credibility see [11].

2.2.2.2. Entering block in private blockchain

In private blockchains, the mechanism of registering new blocks differs in that it is not necessary to reach a community consensus on the correctness of the block, but the role of verifying the validity of the block is entrusted to authorized entities. This achieves administrator control over the blockchain and significantly improves the performance of block entry into the blockchain.

The blockchain consortium represents the integration of public and private blockchains in terms of connecting their good properties and hybrids, as its name suggests, the integration of elements of previous models.

3. E-HEALTHCARE SECURITY CONCEPT

The electronic health system is network-oriented in the sense that it involves collecting data, processing it, and exchanging it between different entities, often geographically distant, to achieve the best possible results. The basic element of the electronic health system is the electronic record of health data (EHR). The data contained in the EHR are primarily used for the health care of the individual to whom they relate. Their secondary use refers to their social usability, the need for application in medical research, the improvement of the scope and level of health care, and the reduction of costs in the functioning of the health system. These two aspects further point to the need for strong security and privacy mechanisms in electronic health systems so that access to and compliance with legal regulations in the management of the data subject can be strongly controlled. For the desired high levels of access control and management, it is essential to distinguish between all elements in the system. This is achieved by defining methods of identifying the factors of the system and assigning a unique identifier to each of them, [14].

3.1. ENTITY IDENTIFICATION

Bearing in mind that digitalization is strongly represented in many countries, including ours, a legal regulation has been developed that regulates the way of assigning electronic identities to people so that electronic transactions are unambiguously and undeniably recognized in business and legal processes. Therefore, in the electronic health insurance system, they are identified by the public key of the selected asymmetric cryptographic algorithm and a qualified digital certificate in the format X.509v3 that confirms the connection between the person and the assigned public key. A qualified certificate is issued under the legal regulations of the environment in which the system is implemented.

Each person, user of the electronic healthcare system has a smart card, and an e-health patient ID (eHPID), and every person belonging to the electronic healthcare system has an identification card (eHID).

The records of users of the electronic health system, patients, are formed and stored within a protected database, for example, basic identification data are stored in cryptographically protected form. The system members' records are kept in another protected database.

Devices in the system are assigned identities represented by a public key related to the elliptical curve SECP256R1 and the electronic and physical identity of the device are connected by a digital certificate in CBOR format.

In this context, all entities participating in the electronic health system have unique electronic identities, [15], [16]. This way of establishing identity enables effective protection of the privacy of patients' data.

3.2. MEDICAL EXAMINATION AND RESULT EVIDENCE AND RECORD

Let's consider the following simplified scenario, as an illustration of the concept. The patient has a health problem and comes to the primary health institution for consultation with a physician. The review procedure takes place as follows:

1. In the physician's office, the physician and the patient using their eHPID and eHID card are presented to the system;
    a. If the physician and the patient are recognized as a legitimate user of the health care system, the physician is allowed to open the patient's EHR and create a new examination record identification number and enter data on problems and conclusions about the treatment;
    b. If the process of diagnosis and therapeutic determination is completed at this level, the doctor prescribes therapy, the system determines the identification number of the generated prescription.
2. If the medical indications are such that additional medical tests need to be carried out for each additional medical examination the physician generates a request with the necessary data;
3. Each prescription and request for additional medical examinations individually is digitally signed by the physician. Each electronically signed prescription/request for additional medical examinations constitutes a medical transaction and is placed in the appropriate blockchain; and
4. Prescription and medical procedure identification numbers are recorded in the patient's medical history blockchain. The patient's medical history blockchain is identified by a unique numerical identifier that exists only in a protected database containing the patient's identification data.

Conceptually, this way of creating and managing medical records enables the independent existence of medical data from the identity of the patient whose interaction with the system they were created. The only link between the patient's identity and his medical history is the blockchain identifier of his medical history, which is stored in a protected database the register of users of the health system. The concept of the system is shown in Figure 2.

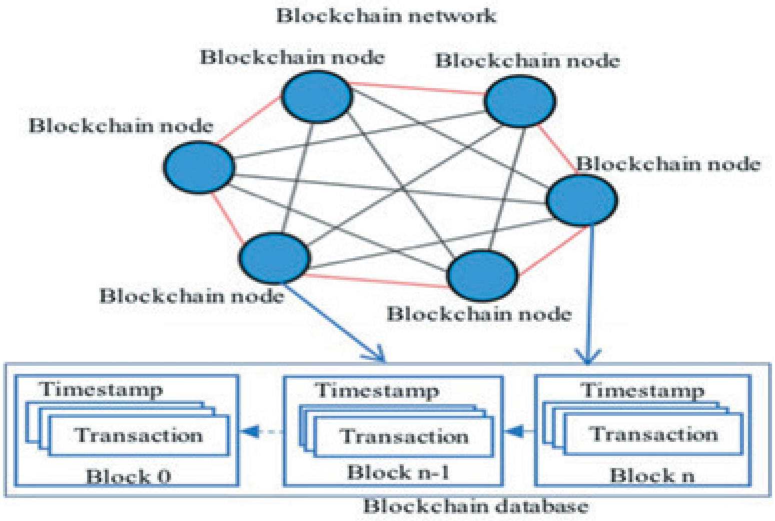

Figure 2 – General concept of blockchain technology in healthcare, [17].

3.3. SECURITY ANALYSIS

Given the complexity and importance of a healthcare system for every community its safety and reliability of functioning are essential for any organized society. By transferring procedures and data into a digital world, in addition to the existing challenges, all those security challenges that the processes in cyberspace carry with them have entered the game. In this way, technological improvements simultaneously contribute to the quality of systems and services on the one hand and impose security challenges on the other.

Given the security incidents related to patient data privacy, the first component we will consider is the proposed model of entity identification in the system.

The electronic identity of each entity is defined by the assigned to it reliable electronic certificate. In this way, conditions were created for reliable identification, authentication, and authorization of entities in the system. A reliable identification mechanism, such as this proposed one, allows unique recording and tracking of system events and detects and prevent any activity of an entity that does not comply with the role assigned to it in the system. In this way, the role of monitoring the operation of the system and supporting the reliability and proper operation of the system is achieved.

But as previously stated in safety terms, the basic security problem in the health information system is the collection, use, and management of patient data. The system must be organized in such a way that, without collision, it allows the primary and secondary use of the patient's medical data without compromising his privacy. Additional use, storage, and management of this data must be implemented in such a way as to preserve its privacy and integrity.

In the proposed concept, the patient's identification data are located only and exclusively in a protected database that can only be accessed under defined conditions for example with the patient's consent demonstrated by reading his eHPID document. The registration record in the database of users of the health system also contains a static numerical identifier of the patient that is identified in medical procedures and records in a vase with them. The use of numerical identifiers in medical reports and therapeutic procedures allows the use of this data without infringing on the patient's privacy rights.

Patient data privacy is guaranteed by the applied method of establishing randomized numerical identification of patient medical documentation blockchain. That numerical identification is stored in the protected database of the healthcare system patient record and represents the only connection between patient medical data and its identity. Access to that numerical identification is possible only using the patient's eHPID smart card. The situation when a patient on his own will allow usage of his eHPID, for example giving physical access to it or entering a PIN number, will be recognized as his consent to access his medical data. The anonymity of the patient regarding requested medical procedures and prescribed health care therapy and medicine is achieved by their randomized numerical identification which is described in the paper's second part. The integrity of medical examination requests and reports is guaranteed by the digital signatures made by the initiators of medical and therapeutic procedures, and report creators. Data integrity over time is achieved by their storage in the appropriate blockchain.

This analysis shows that the proposed concept meets the primary security requirements of the health insurance information system, which is to preserve the privacy, integrity, and availability of medical data with their primary and secondary use.

4. CONCLUSION

Technological advances and orientation towards a digitized society by transferring social and business interactions into cyberspace have greatly improved everyday life. At the same time, this change has brought inevitable challenges in the field of information security. One of the largest is the establishment and reliable exploitation of the electronic healthcare system. In this paper, a safety concept for electronic health systems is proposed. The concept is based on reliable identification by digital certificates within the legal PKI infrastructure. The system recognizes two types of certificates, qualified for people in the format X.509V3 and CBOR [10] for devices and software taking into account the existence of devices with limited resources. In this way, each entity becomes unambiguously recognizable in the system. In security terms, by these following objectives are achieved:

1. Undeniable record of events in the system, their analysis, and establishment of responsibility in the event of an incident as well as analysis and undertaking of activities to prevent security incidents in the future;
2. The establishment of an unambiguous identity enables the realization of such a way of recording the patient's medical data, which ensures the primary and secondary use of medical data in a way that does not endanger patient privacy; and
3. Registering medical information and system data by applying digital signing and blockchain technology, ensures that data integrity is preserved at the time of creation and during the time.

Achieving the stated goals is the foundation for compliance with the EU GDPR [18] and an inevitable basis for the implementation of zero-trust information systems [19], [20], [21].

5. REFERENCES

[1] C. A. Shoniregun, K. Dube and F. Mtenzi, Electronic Healthcare Information Security, Springer US, 2010.

[2] S. P. Murphy and D. M. Seymour, Healthcare Information Security and Privacy, McGraw-Hill Education, 2015, p. 560.

[3] V. Hordern, "Data Protection Compliance in the Age of Digital Health," *European Journal of Health Law*, vol. 23, p. 248–264, June 2016.

[4] A. K. Singh and H. Zhou, Medical Information Processing and Security, Institution of Engineering & Technology, 2023.

[5] J. R. Vacca, Public Key Infrastructure, Taylor & Francis Group, 2019.

[6] J. A. Buchmann, E. Karatsiolis and A. Wiesmaier, Introduction to Public Key Infrastructures, Springer, p. 209.

[7] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC Editor, 2008.

[8] J. Höglund, S. Lindemer, M. Furuhed and S. Raza, "PKI4IoT: Towards public key infrastructure for the Internet of Things," *Computers & Security*, vol. 89, p. 101658, February 2020.

[9] F. Forsby, "Digital Certificates for theInternet of Things," 2017.

[10] C. Bormann and P. E. Hoffman, *Concise Binary Object Representation (CBOR)*, RFC Editor, 2013.

[11] A. Judmayer, Blocks and Chains, Morgan & Claypool Publishers, 2017.

[12] A. Summers, Understanding Blockchain and Cryptocurrencies, CRC Press, 2022.

[13] Y.-C. Liang, "Blockchain for Dynamic Spectrum Management," in *Dynamic Spectrum Management, Springer Singapore*, 2019, p. 121–146.

[14] K. Sandhu, Handbook of Research on Cybersecurity for Digital Transformation, IGI Global, 2021.

[15] P. Windley, Learning Digital Identity, O'Reilly Media, Incorporated, 2022.

[16] A. Preukschat and D. Reed, Self-Sovereign Identity Decentralized Digital Identity and Verifiable Credentials, Manning Publications Co. LLC, 2021.

[17] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *{IEEE} Communications Surveys & Tutorials*, vol. 21, p. 858–880, 2019.

[18] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation : A Practical Guide, Springer, p. 392.

[19] J. Garbis and J. W. Chapman, Zero Trust Security : An Enterprise Guide, Apress, p. 324.

[20] B. Pillai and A. Kudrati, Zero Trust Journey Across the Digital Estate, CRC Press LLC, 2022, p. 236.

[21] R. Rais, C. Morillo, E. Gilman and D. Barth, Zero Trust Networks, O'Reilly Media, 2024(Early Release).