Exploring a New Security Framework for Future Healthcare Systems

Nattaruedee Vithanwattana, Gayathri Karthick, Glenford Mapp, Carlisle George
Faculty of Science and Technology
Middlesex University
Email: nv166@live.mdx.ac.uk and G.Karthick, G.Mapp, C.George@mdx.ac.uk

***Abstract*—The Internet of Things is driving impactful and significant changes in healthcare systems across the globe. The use of mobile and wireless technologies to support healthcare environments has enormous potential to transform healthcare. For example, healthcare data, which is considered to be very sensitive, must be securely accessed, processed and stored. However, digital healthcare IT platforms are increasingly coming under attack by malware such as Ransomware. In addition, there is now a need to integrate eHealth and mHealth mechanisms into national healthcare systems. New technologies, such as blockchain, are being used to address these issues. What is needed is a new framework which can use these technologies to secure healthcare. This paper proposes a new security framework that responds to these security concerns. The framework is then used to design an implementation framework with new mechanisms including Capabilities, Secure Remote Procedure Calls and a Service Management Framework.**

***Index Terms*—Healthcare System, Information Security, Futuristic Technologies, Cloud Computing, IoT**

I. Introduction

The COVID-19 pandemic has significantly changed the way that healthcare services are provided and delivered. Smart healthcare systems, including eHealth and mHealth, have become an emerging phenomenon in the healthcare industry. The majority of healthcare services have shifted from an in-person service to virtual healthcare. Face-to-face meetings are only conducted when they are necessary and unavoidable such as surgeries, or medical tests. Therefore, eHealth and mHealth services now appear to be widely recognised as the way to deliver services for future healthcare systems.

It is undeniable that smart healthcare services offer many benefits in terms of improving the quality of healthcare. They provide sustainable healthcare through better planning of patient treatments that results in dramatically reducing the number of required in-person meetings between healthcare professionals and patients. However, they may also generate concerns with regard to information security. Smart healthcare systems are prone to be targets of several attacks including unauthorised access to patient records, ransomware attacks, network-based attacks, etc.

Many security mechanisms have been proposed in order to tackle security concerns about the security of healthcare data. Futuristic technologies, such as blockchain technology, have the potential to transform healthcare systems since they are able to facilitate secure interactions within an enlarged healthcare environment. However, it is necessary to develop a security framework with a combination of security mechanisms that can be used to provide all the essential security requirements for healthcare systems. This paper addresses these issues by looking at a new framework and mechanisms for future healthcare.

The remainder of the paper is structured as follows. Section 2 analyses the related work and identifies a research gap to develop a secure framework for healthcare systems, while Section 3 explores a detailed analysis of security issues in future healthcare systems. Section 4 proposes a secure framework which combines new mechanisms together to achieve security requirements. Section 5 examines a developed prototype to test the proposed framework, while Section 6 evaluates how the proposed framework meets all the practical security requirements. Finally, the paper concludes in Section 7.

II. Related Work

In this section, we briefly analyse security frameworks and highlight the research gap needed to be addressed in order to develop a complete framework that is secure and efficient.

Recently, there are numerous researchers [1] [2] raising concerns about security and privacy issues in healthcare. Studies in [3] [4] [5] identified security requirements that are needed to provide secure Cloud storage for healthcare data. These security requirements include confidentiality, integrity, availability, authenticity, and reliability.

Research by Yahya in [6] aimed to develop an appropriate security framework for Cloud storage which is one of the main components of a modern healthcare environment. This framework indicates that security in Cloud storage can be determined by nine factors: (1) Security policies implementation; (2) Data access protection; (3) Modifications of data stored; (4) Data accessibility; (5) Non-repudiation; (6) Authenticity; (7) Reliability; (8) Accountability; and (9) Auditability.

A hybrid framework for IoT-Healthcare using blockchain technology was proposed by Rathee, Sharma, Saini, Kumar, and Iqbal [7]. They claimed that currently blockchain technology is the best technique to provide secrecy and protection of control systems in real-time conditions. Results of their research showed that their framework offers an 86 percent success rate and can prevent wormhole and falsification attacks. However, the drawback of their framework is that hashing of all blocks (nodes) becomes very complicated to predict at once since the entire network is maintained by the blockchain.

In [8] [9] [10], the authors proposed a security framework based on the use of blockchain techniques. It was designed to provide data integrity by using cryptographic primitives and authenticity as well as non-repudiation by using digital signatures. While data integrity, non-repudiation, and authenticity are provided by design, this framework does not provide any data confidentiality [11]. This is because blocks of data are linked together by cryptographic elements in a chain, therefore, it is not necessary to encrypt the information stored in blocks [12].

A reusable security requirements template was developed by Firesmith [13] [14]. It defined security as a quality factor that can be divided into underlying subfactors including Identification, Authentication, Authorisation, Immunity, Integrity, Intrusion Detection, Non-repudiation, Privacy, Security Auditing, Survivability, and Physical Protection. The idea behind reusable security templates is to develop security requirements that potentially can be reused by or extended for any system. Therefore, it can be used in order to develop an information security framework for healthcare systems.

Table I shows the comparison of the different security frameworks discussed in terms of providing the required security requirements.

TABLE I
A COMPARISON OF EXISTING STUDIES

Security Requirements	**Author**					
	[3]	**[4]**	**[5]**	**[6]**	**[7]**	**[14]**
Confidentiality	*	*	*	*	*	*
Integrity	*	*	*	*	*	*
Availability	*	*	*	*	*	*
Non-repudiation				*	*	*
Authentication		*	*	*		*
Authorisation						*
Accountability				*	*	
Auditability				*	*	*
Reliability		*	*	*		

Research Gap

As detailed above, there have been several studies related to security frameworks for healthcare systems and Cloud systems. However, they were usually involved in providing some security requirements, but not a full set of necessary security requirements which includes Confidentiality, Integrity, Availability, Non-repudiation, Authentication, Authorisation, Accountability, Auditability, and Reliability [15]. Therefore, there is a need to develop a security framework which provides end-to-end security for smart healthcare systems from where healthcare data is collected, transferred over the network, and stored on the Cloud storage, as well as supports those necessary security requirements.

III. ANALYSIS OF SECURITY ISSUES IN FUTURE HEALTHCARE SYSTEMS

In smart healthcare systems, healthcare data is collected from mHealth devices such as wearable devices or implanted devices. The collected healthcare data is transferred to mobile phones/tablets/PDAs on which mHealth applications are installed. The healthcare data will then be transferred over the network to store in the Cloud storage. Therefore, healthcare professionals will be able to access healthcare data through the Cloud storage without the need of a physical meeting with a patient. Figure 1 shows a smart healthcare system scenario.

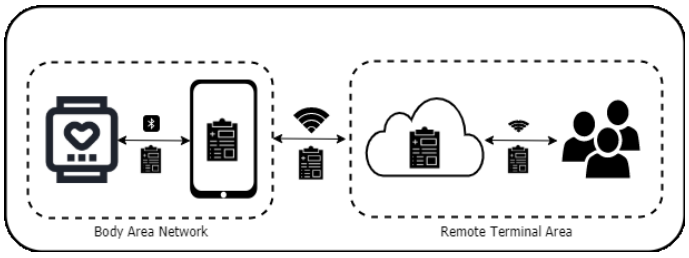

Fig. 1. A smart healthcare system scenario

A Detailed Analysis of Security Requirements for Smart Healthcare Systems

As we examine security in healthcare environments, we can divide the security issues into five subsystems.

1. The first requirement is the provision of AAAC (Authentication, Authorisation, Accounting, and Control) for all human users including medical staff, patients, retail workers, administrative staff, and visitors. The system should allow users to use the hospital environment simply and intuitively. One way of addressing this is to look at using mechanisms that support Role-Based Access Control (RBAC) which is a security framework for controlling user access rights to objects in the system, based on their roles [16] [17].

2. The second requirement is to protect devices from being misused, tampered with, or stolen. This now includes not just medical devices in hospitals and surgeries, but also devices used in the home or by mobile users with eHealth or mHealth functions.

3. The third requirement is the need to protect digital data such as the Electronic Health Records (EHRs) of patients. The misuse of EHRs can cause personal as well as economic damage. Hence, it is a legal requirement to protect EHRs as highlighted by the General Data Protection Regulation (GDPR) [18] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [19].

4. There is now also a need to protect hospital infrastructure. This is due to the fact that new types of attacks, such as ransomware, are being developed. Ransomware typically attacks victim machines in several ways including phishing emails, malicious links, and malvertisings [20] [21]. Network-based attacks such as Denial-of-Service (DoS), Distributed Denial of service (DDoS), and buffer-overflow attacks are on the rise [22] [23].

5. Finally, the presence of COVID-19 increases the need to protect access to certain physical sites and locations. This is becoming more important in the UK, where several large hospitals have many departments and access to different parts

of the hospital needs to be controlled. Some areas, such as car parks and concourse areas, clearly need to be publicly accessible while a large number of areas, such as offices and wards, need to have restricted access.

Previous research on security in healthcare usually involved looking at one or two of the five subsystems. However, this research looks at the combination of mechanisms that can be used to provide support for all five subsystems.

IV. A Proposed Framework

Although, there have been a few studies related to security frameworks for healthcare systems and Cloud systems, new technologies can now be applied to develop a security framework with a full set of security requirements that includes Confidentiality, Integrity, Availability, Non-repudiation, Authentication, Authorisation, Accountability, Auditability, and Reliability. Using these technologies, a new framework is proposed as shown in Figure 2.

APPLICATION
SERVICE MANAGEMENT LAYER
SECURE TRANSACTIONAL LAYER
BLOCKCHAIN
SECURE TRANSPORT LAYER
DIGITAL FILTER
STORAGE MANAGEMENT SYSTEM
CAPABILITY SYSTEM
ENCRYPTION

Fig. 2. A proposed information security framework for healthcare systems

This new security framework builds on previous work by Mapp, Aiash, Ondiege, and Clarke [24] and Firesmith [13] [14] that completely specified the required security requirements.

Key Mechanisms

1) Encryption as a Service: Encryption is a process to secure information from unauthorised accesses. It changes information which can be read (plaintext) into the form that cannot be read (ciphertext) [25], unless, you have a key that can decrypt the message. HIPAA [26] mandates standards used to secure EHRs, and requires a method to be implemented to encrypt and decrypt electronically protected health information. All electronic healthcare data that is created, transmitted in systems or stored on devices must be encrypted.

This encryption mechanism is applied to healthcare data. All healthcare data in the system must be encrypted to protect their confidentiality. Only the application that owns or has been given access by the authorised user is allowed to decrypt the data [27].

The main purpose of encryption is to protect the confidentiality of healthcare data that resides in the system. However, encryption does not protect end-to-end confidentiality nor prevent communication interceptions. Moreover, encryption itself provides only confidentiality of data but does not provide other security requirements such as integrity, authenticity, or non-repudiation. Therefore, other security mechanisms will be required in healthcare systems in order to protect healthcare data elsewhere in the system.

2) Capabilities: A Capability refers to a token that permits authorised users to access certain objects in a system [28]. It can be used in a flexible manner to provide essential security requirements in many environments including healthcare systems, Cloud computing systems, and Internet of Things (IoT).

In this proposed framework, the capability system is based on the address space of IPv6. IPv6 is the latest version of the Internet Protocol (IP) [29]. It provides an identification and location for every computer, mobile phone, and any other mobile device on networks across the internet through its IP address. The IPv6 protocol also provides several other advantages as it can handle packets more efficiently as well as improves performance and increases security [30].

In a healthcare system, every object and its properties are identified using capabilities. Therefore, it is necessary that capabilities must be carefully managed and be protected from being created or modified in an unauthorised manner.

Compared to the other capability structures previously proposed [24] [31] [32], the current research has simplified the structure by removing the Scope Field and expanding the Property Field. The System Flags, which are used to help managing capabilities, are also made explicit by placing them in a separate field called the Sys Field. This new arrangement provides more efficiency and greater flexibility. Hence, the recent format of a capability-based system is shown in Figure 3.

TYPE	SYS FIELD	PROPERTY FIELD	OBJECT ID	RANDOM BIT FIELD	HARSH FIELD

Fig. 3. Capabilities Format

Capabilities provide several benefits to healthcare systems. They can be used to provide Role-Based Access Control (RBAC) access for users. Some capabilities are therefore not assigned directly to users, instead, they are assigned to roles, and roles are assigned to users. These are called role-based capabilities. [31]. Hence, the access right can be identified by the role based on job functions of different people in the healthcare system such as doctors, nurses, patients, and researchers.

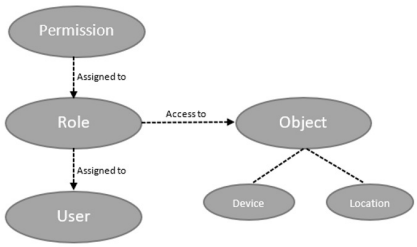

Fig. 4. Capability System Components

Moreover, Capability lists, which are groups of Capabilities, are used to manage people working at an institution such as a hospital. There are three different types of Capability lists developed in the proposed framework including: (1) *Common* which is a public capability list that belongs to all users in the system. (2) *Role-based* which is assigned to different employees based on their roles. For example, doctors are able to access EHRs and medical equipment, or request a blood test result from a laboratory. Hence, these lists of capabilities can be defined using different role-based types such as doctor, nurse, technician. (3) *Personal* which is a Capability list that is used to manage personal items or spaces of users. This includes access to the personal office, personal correspondences (text messages, emails), etc. Hence, this personal capability list will be a list of Private Capabilities associated with the owner of the object.

3) Storage Management System: This mechanism enables the management of security for each block of data in the Cloud infrastructure using encryption techniques such as AES (Advanced Encryption Standard) and 3-DES (Triple Data Encryption Standard) algorithms to protect the confidentiality of data. Moreover, each block of data is hashed after it has been modified in order to provide integrity so that data will not be able to be modified by an unauthorised user. In order to ensure the availability of data, each block may be replicated throughout the Cloud storage structure. Therefore, a coherency protocol within the storage layer is used to synchronise different copies of the block [24].

4) Digital Filter: In addition to traditional security measures, the use of digital filters in the proposed framework is an additional advantage in providing more control over who are able to access healthcare data.

In a digital filter, each healthcare record in the Cloud storage can have a set of filters which is used to prevent certain fields in that record from being accessed. In order to access a given field, the relevant filter must be removed. This usually requires authorisation from senior personnel. This mechanism provides authentication and authorisation. Moreover, it can also prevent unauthorised accesses, theft, destruction, and DoS attacks [33].

5) Secure Transport Layer: An examination of network interactions at the local area level clearly indicates that there is a need for more transactional support in the Cloud environment since there are many client/server interactions that use network services [24].

The Transport Control Protocol (TCP) and the User Datagram Protocol (UDP) have been widely used as the main transport protocols. TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. TCP provides reliable services while UDP provides fast, low latency but unreliable connections. However, recent research in vehicular networks has indicated the need for a low latency, reliable, secure transport protocol. As a result, the Simple Lightweight Transport Protocol (SLTP) has been developed to support these issues [34].

SLTP keeps packet processing as simple as possible to reduce latency and provide faster connection setup and take-down times. Moreover, it is designed to be used in many environments including UDP/IP and Raw Ethernet. The details of SLTP functionalities can be explored in [35].

SLTP can be combined with an encryption mechanism to provide secure communications while maintaining fast and reliable connections. Furthermore, SLTP supports the inclusion of Additional Headers which could be used to pass security parameters and certificates. Hence the Transport Layer Security (TLS) protocol can be easily supported using SLTP.

6) Blockchain: Nowadays, blockchain (or sometimes called distributed ledger technology) is a new technology that is being used to provide a more secure Internet [36]. A blockchain is a distributed data system where users share a consistent copy of a database and agree on changes by consensus. The data is represented in the form of blocks, where each block includes a cryptographic signature of the previous block, creating an immutable record [37]. The users must comply with ledger rules including permission-less ledgers which allow anyone to join and add new blocks, and permissioned ledgers in which participation is subject to rules of the members including contributing and adding new blocks. A combination of these two types of ledger technologies provides advantages in supporting, recording, and enhancing the administration of patient records [38].

Blockchain technology uses a type of consensus protocol in order to agree on the validity of a given transaction. It also uses digital signatures (private/public key) to sign and/or encrypt transactions on the ledger by which each signature could be linked to identity of the owner [39]. The blockchain provides an advantage to a distributed network of computers that do not necessarily trust each other to achieve consensus [40]. The use of this new blockchain technology in healthcare systems fulfils the security requirement of non-repudiation as well as the ability to discover security and privacy violations [32].

7) Secure Transactional Layer: The Secure Transactional Layer is developed to protect the remote procedure by applying an authentication mechanism to ensure that there is no one able to fool the system [41] [42]. The Secure Remote Procedure Call (SRPC) is an inter-process mechanism that is used for communication between clients and servers. It uses a strongly typed system in which the type as well as the value of data passed are explicitly declared. This is used to make sure that security attacks such as buffer overflow attacks can be avoided.

By combining encryption, capabilities and SRPC, it is possible to provide a secure transactional environment where clients and servers can be authenticated, and transactions validated to ensure proper interaction between clients and servers.

8) Service Management Layer: Since there is a large amount of data being generated in healthcare environments, Cloud storage systems are increasingly being used to store and process healthcare data [43]. EHRs must be securely stored, hence, the challenges of using Cloud services for healthcare environments must be addressed to ensure that patient, doctor, and hospital staff are safe.

There are several challenges to be addressed including a secure execution environment, the best place to run a service at any point in time, and the ability to securely transfer services between Clouds. This means that, among other things, it is important that servers are not hosted on unsafe Cloud hardware and Cloud Servers are not corrupted by malicious or badly implemented servers.

As a result, the Service Management Framework (SMF) has been developed (Figure 5). It provides a solution for issues of security, deployment, replication, or migration of services on different scales including geographical regional, national, and global contexts.

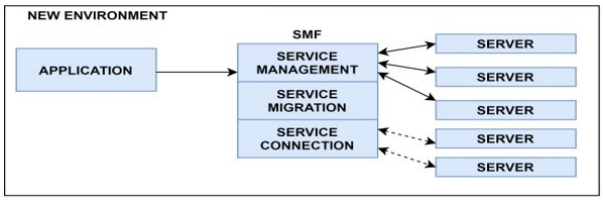

Fig. 5. Service Management Framework

The Service Management Framework is a new way of deploying and managing services in distributed environments. It allows clients to find services and provides communication endpoints and capabilities which allow a reliable session to be developed. It, therefore, increases the security, efficiency and management of services, and will be a key part of future IoT systems.

Table II shows how each layer of the new framework meets the overall security requirements.

TABLE II
THE SECURITY REQUIREMENT ANALYSIS FOR THE NEW INFORMATION SECURITY FRAMEWORK

Security Requirement	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Confidentiality	*	*	*		*	*	*	
Integrity		*	*		*	*	*	
Availability			*			*		*
Non-repudiation		*				*		
Authentication		*		*	*	*	*	
Authorisation		*		*	*			
Accountability		*				*		*
Auditability		*				*		*
Reliability		*			*		*	*

Therefore, this new framework has been designed to provide security at multiple levels and in multiple ways resulting in a thoroughly secure environment.

V. Prototype Implementation

The proposed framework consists of many different mechanisms and each of them is rather complex to implement. Therefore, developing a viable prototype that clearly embodies all features will require a significant effort.

As a result, a new security prototype is being developed for the purpose of testing. This prototype (Figure 6) consists of 4 layers including an mHealth Application, Service Management Layer, Secure Transactional Layer, and Capability System.

mHealth Application
Service Management Layer
Secure Transactional Layer
Capability System

Fig. 6. Prototype

Capability System: Every object in a healthcare system, such as user, device, and healthcare record, will be managed using Capabilities to organise access rights which can ensure that only authorised entities will be able to access each object.

Secure Transactional Layer: This layer uses the Secure Remote Procedure Call (SRPC) to protect the remote procedure between the client and the server by applying an authentication mechanism. An initial prototype of SRPC has been implemented and showed a 10 percent reduction in performance when compared with normal unsafe mechanisms. This is a small price to pay for such a great improvement in security. Furthermore, the use of new transport protocols such as SLTP will make up for the loss of performance at this layer.

Service Management Layer: This layer manages the service that is being provided in a healthcare system. It specifies the functions of the service as well as the requirements needed to run the service. A simple Service Management Framework Layer has already been implemented and will be extended as well as integrated into the prototype.

mHealth Application: A basic mHealth application, that can create, store, modify, and delete healthcare records using the other layers of the prototype framework, is being developed. The Filesystem in Userspace (FUSE) is being used as a filesystem to control how healthcare records are stored and retrieved. It will be tested against a Microsoft Access Database and a MySQL database environment.

VI. Evaluation

In this section, we show how the prototype meets the requirements of the detailed analysis described in Section 3.

TABLE III
REQUIREMENT ACHIEVEMENTS OF THE PROPOSED PROTOTYPE

Protection	Capabilities	SRPC	SMF	Application
Users of the system	*			
Devices&home access	*		*	
EHRs	*	*	*	*
Digital IT	*	*	*	
Physical space access	*			

VII. Conclusion

Information security is still a major concern in developing effective smart healthcare systems. However, the use of futuristic technologies can be used to address these security issues.

This paper has proposed a new framework for securing future healthcare environments. Various new security mechanisms are combined in order to develop this proposed framework. This is a promising approach and new prototypes and applications are being developed to move this research forward.

REFERENCES

[1] Sridhar, A.P., Lakshmi, P.V., and Mohana, T.K. (2020) "Wearable Devices in Healthcare 4.0: Effects, Trends and Challenges". In International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS 2020), pp. 229-237.

[2] Hathaliya, J.J., and Tanwar, S. (2020) An exhaustive survey on security and privacy issues in Healthcare 4.0. Journal of Computer Communications. 153: 311-335.

[3] Takabi, H., Joshi, J.B.D., and Ahn, G.J. "SecureCloud: Towards a comprehensive security framework for cloud computing environments". In International Computer Software and Applications Conference, 2010, pp.393-398.

[4] Zissis, D. and Lekkas, D. "Addressing cloud computing security issues". Future Generations Computer Systems. 28(2012). P.583-592.

[5] Brock, M., and Goscinski, A. "Toward a Framework for Cloud Security" in Lecture Notes in Computer Science, vol 6082, Springer Berlin Heidelberg, 2010, pp.254-263.

[6] Yayah, F. (2017) "A Security Framework to Protect Data in Cloud Storage", PhD Thesis. University of Southampton. Southampton.

[7] Rathee, G., Sharma, A., Saini, H., Kumar, R., and Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications. 79(15-16). 9711-9733.

[8] Angeletti, F., Chatzigiannakis, I., and Vitaletti, A. (2017). The role of blockchain and IoT in recruiting participants for digital clinical trials. In 2017 25th International Conference on Software, Telecommunications

[9] Lee, H. A., Kung, H. H., and Udayasankaran, J. G. (2020). An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study. Journal of Medical Internet Research, 22(6):e16748.

[10] Mitchell, I. and Hara, S., editors (2019). Quality Audits with Blockchain for Healthcare in the UK and Computer Networks (SoftCOM), pages 1–5.

[11] Julisch, K., and Widmer, F. (2019) Security Controls for Blockchain Applications [online] Available from: https://www2.deloitte.com/ch/en/pages/risk/articles/security-controls-for-blockchain-applications.html [Accessed: 7 August 2021]

[12] Hilary, G. (2019) Blockchain: Security and Confidentiality. Forthcoming, Revue de la Gendarmerie Nationale, Georgetown McDonough School of Business Research Paper No. 3327248.

[13] Firesmith, D. (2003) "Analyzing and Specifying Reusable Security Requirements". In IEEE 11th International Conference on Requirements Engineering, RHAS 2003, pp. 507-514.

[14] Firesmith, D. "Specifying Reusable Security Requirements" Journal of Object Technology. Vol.3, no.1, pp. 61-75, 2004.

[15] Vithanwattana, N., Mapp, G. and George, C. (2017) Developing a comprehensive information security framework for mHealth: a detailed analysis. Journal of Reliable Intelligent Environments 3, 21–39.

[16] Tahir, M.N. (2007) "C-RBAC: contextual role-based access control model". Ubiquitous Computing and Communication Journal. 2(3): 67-74.

[17] Barkley, J. (1995) "Implementing Role-Based Access Control Using Object Technology". In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC), pp. 93-98.

[18] NHS Digital (N/A) Transparency notice: how we use your personal data [online] Available from: https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register [Accessed: 3 August 2021]

[19] U.S. Department of Health and Human Services (2013) Summary of the HIPPA Privacy Rule [online] Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [Accessed: 3 August 2021]

[20] Aver, H. (2021) Ransomware attacks on healthcare [online] Available from: https://www.kaspersky.co.uk/blog/ransomware-vs-healthcare/22670/ [Accessed: 6 August 2021]

[21] Center for Internet Security (N/A) Ransomware: In the Healthcare Sector [online] Available from: https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/ [Accessed: 6 August 2021]

[22] Ashu, M.R., Zafar S. (2021) DDoS Attacks Impact on Data Transfer in IOT-MANET-Based E-Healthcare for Tackling COVID-19. In: Khanna A., Gupta D., Pólkowski Z., Bhattacharyya S., Castillo O. (eds) Data Analytics and Management. Lecture Notes on Data Engineering and Communications Technologies, vol 54. Springer, Singapore.

[23] Sami, I., Asif, M., Ahmad, M.B., and Ullah, R. (2018) DoS/DDoS Detection for E-Healthcare in Internet of Things. International Journal of Advanced Computer Science and Applications. 2(1): 297-300.

[24] Mapp, G., Aiash, M., Ondiege, B., and Clarke, M (2014) "Exploring a New Security Framework for Cloud Storage Using Capabilities". In: 2014 IEEE 8th Symposium on Service Oriented System Engineering (SOSE). Oxford: IEEE, P. 484-489

[25] Jaikaran, C. (2016) Encryption: Frequently Asked Questions [online] Available from: https://fas.org/sgp/crs/misc/R44642.pdf [Accessed: 8 August 2021]

[26] HIPAA Security Series (2007) Security Standards: Technical Safeguards [online] Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf [Accessed: 8 August 2021]

[27] Martin, K. (2012) Everyday Cryptography. United States of America: Oxford University Press Inc.

[28] Dennis, J.B., and Horn, E.C.V. (1966). Programming semantics for multiprogrammed computations. Communications of the ACM, 9(3):143-155.

[29] Hermann, S., and Fabian, B. (2014) A Comparison of Internet Protocol (IPv6) Security Guidelines. Journal of Future Internet, 6(1): 1-60.

[30] Shaw, K., and Fruhlinger, J. (2020) "What is IPv6, and why aren't we there yet?" [Online] Available from: https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html [Accessed: 2 August 2021]

[31] Ondiege, B., Clarke, M., and Mapp, G. (2017) Exploring a New Security Framework for Remote Patient Monitoring Devices. Journal of Computers. 6(1): 11.

[32] Mapp G, George C, Mitchell I, Hara S, Vithanwattana N, Jusob F and Samuels A: Securing eHealth and mHealth: moving from frameworks to prototypes: Presented at the Health IT Workshop, Middlesex University, London, 7th-8th November 2019.

[33] Cisco Press (2010) Developing Network Security Strategies [online] Available from: https://www.ciscopress.com/articles/article.asp?p=1626588seqNum=2 [Accessed: 10 August 2021]

[34] Ezenwigbo, O.A., Paranthaman, V.V., Trestian, R., Mapp, G., and Sardis, F. (2018) Exploring a New Transport Protocol for Vehicular Networks. In 2018 the 5th International Conference on Internet of Things: Systems, Management and Security (IoTSMS). pp.287-294.

[35] Mapp, g. (2017) The Simple Lightweight Transport Protocol (SLTP) for Low Latency Environments [online] Available from: https://moam.info/the-simple-lightweight-transport-protocol-sltp-for-low-latency5c593f7a097c47fa378b45ff.html [Accessed: 9 August 2021]

[36] TayloyWessing (N/A) How secure is blockchain? [online] Available from: https://www.taylorwessing.com /download/article-how-secure-is-block-chain.html [Accessed: 10 August 2021]

[37] Korolov, M. (2016) The blockchain is now being hyped as the solution to all inefficient information processing systems [online] Available from: http://www.csoonline.com/article/ 3050557/security/is-the-blockchain-good-for-security.html [Accessed: 10 August 2021]

[38] Mithchell, I. and Hara, S. Securing eHealth and mHealth: moving from frameworks to prototypes: Presented at the Health IT Workshop, Middlesex University, London, 7th-8th November 2019.

[39] ENISA (2017) Distributed Ledger Technology and Cyber Security – Improving information security in the financial sector [online] Available from: https://www.enisa.europa.eu/publications /blockchain-security [Accessed: 10 August 2021]

[40] Pair, S. (2015) The Secure Blockchain is Bitcoin's Biggest Asset [online] Available from: https://www.infosecurity-magazine.com/opinions/the-secure-Blockchain-is-bitcoins/ [Accessed: 10 August 2021]

[41] Hall, M., and Barry, J. (2013) The Sun Technology Papers. The United States of America: Springer.

[42] The Open Group (1997) Introduction to the RPC API [online] Available from: http://pubs.opengroup.org/onlinepubs/9629399/chap2.htm [Accessed: 3 August 2021]

[43] Kuo A. M. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3), e67. https://doi.org/10.2196/jmir.1867