Design of Cross Border Healthcare Integrated System and its Privacy and Security Issues

Savoska Snezana, Jolevski Ilija, Ristevski Blagoj, Blazeska-Tabakovska Natasha, Bocevska Andrijana, Jakimovski Boro, Chorbev Ivan and Vassilis Kilintzis

***Abstract**: Healthcare systems generate large amounts of data, collected from different healthcare systems and sources and stored in large data sets. It is particularly interesting for a wide range of user groups and stakeholders in healthcare. As the data volume increases over time, the risk of abuse and unauthorized access to the personal and sensitive data arises. Data are collected by using of numerous means and are stored in different datacenters. These data are related to the patients, doctors, insurance companies, health providers and other users as stakeholders in one or more countries, and data can be a subject of misuse at many levels. When dealing with such complex systems, a complex data security management is needed. IPA 2 project Cross4all intends to integrates health and social care system across the border area and gather patient data from both sides of the Republic of N. Macedonia and Greece. We proposed a model of secure system architecture that deals with the data security and privacy standards of two countries taking into account their data protection regulations and laws.*
***Key words:** healthcare data security and privacy, healthcare integrated system, healthcare services, mobile applications.*

1. INTRODUCTION

Cross border IPA2 project, titled as “Cross-border initiative for integrated health and social services promoting safe ageing, early prevention and independent living for all (Cross4all), has intention to create a multilayer healthcare system in the cross border area between R. of N. Macedonia and Greece. Project activities are connected with creation of digital assets that have to be used as integrated cloud e-health cross border services. Digital assets have to be connected to the patient health records (PHR), and then to integrate them with the applications as e-prescription and e-referral and tools for increasing the healthcare digital literacy on e-health according to web accessibility standards (WCAG2.0) [1]. It is essential to provide smooth usage for the people with disabilities. The integrated system also has to be connected with mobile applications for short period of time for tele-monitoring of professionals and citizens. Mobile application has to be managed by citizens or medical professionals. Data from electronic patient records (EPRs), which are not owned by patients, have to be included through medical practitioners’ access to them. The supporting architecture of this complex digital structure has to be cloud oriented with a complex infrastructure for security and privacy protection of the patients that are involved in this project [2]. Such project usually collects a huge amount of different data types with big data properties (variety, velocity, value, volume, veracity and variability) [3] and demands healthcare big data (HBD) resolving the security and privacy issues, information, knowledge and wisdom (DIKW) [3].

The paper is organized as follows. First, related work for healthcare security and privacy are described as well as characteristics of the HBD for whole DIKW pyramid [3]. The known architectural security models used in healthcare systems are also considered in related works. The next section depicts the project needs and security demands in big data era. The proposed security and privacy model for the project and integrated healthcare system is described in the next section. Finally, the conclusion and key points of the proposed model are highlighted. Some recommendations for the further works and model validation are also given.

2. RELATED WORKS

Nowadays, data security researchers pay attention to the symbiosis of HBD the security and privacy. As they demanded more and more space for storage and tools for data analysis and visualization [3], they can be stored only in the cloud Cyberspaces [4]. Cloud-based healthcare (CBH) has many advantages such as increased availability, decreased expenses, data sharing and scalability. But, there are many security problems connected with vulnerability risks on safety and security of healthcare information [5], especially when big data features are considered [4] [5] [7]. Many relations can be done in healthcare systems, connecting patient data with different data sets of selected healthcare data and variability of parameters over time, depending on some other parameters that are changing over time, incidentally or stochastically [5], depending on the state conditions [8]. Data

vulnerability is the factor of limitation for research associated with individual healthcare or partial exposome [9] instead the fact of gaining benefits from mobile device sensors for biomedical data measuring. These problems are ethical and have to be solved according to the law and privacy policies [2] [7].

Traditional security mechanisms as authentication and authorization are not sufficient for HBD. There is a need for using combination of advanced safety and security mechanisms such as dynamically checking of identity on different levels, encryption, digital signature and other security mechanisms [10]. They have to be used in different security levels [3]. Many of the security researchers proposed model of TA (Trusted Authority) with check of clients' authenticity and their security and safety demands and privacy attributes on cloud, data modification and migration aiming to ensure integrity and privacy policies. For that reason, some researchers explain how to deliver quality system that is able to manage big data of the patients [11], for physicians and others stakeholders [7]. Some researchers [12] proposed u-healthcare service integration platform (u-HCSIP) applying RBAC security model that can be used for mobile platforms, too.

When access control model is used as fundamental security barrier, the patient privacy is addressed as well as confidentiality [13]. Some novel architectures are proposed with a combination of four modules: Role Based Access Control Module (RBAC), Mandatory Access Control Module (MAC), Discretionary Access Control Module (DAC) and a Purpose Based Access Control Module (PBAC) [13]. In [14], authors proposed an access control framework that applies a Hierarchy Similarity Analyzer (HSA) that uses centralized and decentralized approaches [14].

A new information access method based on a the zero-knowledge protocol combined with two-stage key access control is proposed in [15] aiming to preserves both authentication and access control in cloud-based e-Health systems. A two-step combination of public key encryption and DUKPT is implemented for secure connections between different entities in the system. In [16], architecture for electronic health, which can guarantee efficiency, is proposed.

Other architecture for patient centric personal data and access control scheme with enhanced encryption method, with applying of digital signature and patient pseudo identity is proposed in [11]. Multi Authority Attribute Based Encryption (MA-ABE) techniques with Advance encryption standard (AES) can be implemented to secure PHR data. But, we explore how SPOC (single point of contact) can be helpful for solving security issues in Cross4all project. The Agency for Healthcare Research and Quality (AHRQ) has cited that clinical decision support systems and knowledge management IT systems can be effective in improving healthcare process measures [19]. Also, the using of organizational healthcare knowledge management systems (HKMS) is effective in the supporting concept "patient in the center", providing decision making in drug prescription and disease management protocols [20], [21], [22]. HKMS assist in medical errors and costs reduction [23], enabling cooperation and quality control between different healthcare providers [24]. One of the challenges in knowledge management is maintaining security threats that can range from unauthorized access of confidential patient's information to the potential loss or unauthorized modification of information [25]. Security awareness has to be an integral part of the security strategy of all health care organizations. It has to enforce some form of access control such as RBAC, credential mechanism, and encryption. Many other researchers propose different models for ensuring knowledge management in healthcare organizations [26], but none of these security technologies can be a solution for all of HKMS security problems. For effective authentication, combination of many mechanisms can be used such as: biometrics authentication that uses personal uniquely identifying attributes (e.g., fingerprints, retinal scans, facial imaging, voice recognition, hand readers, etc.). Also smartcards can increase system security because of the smartcard user-specific data and private key or a digital fingerprint. Public key cryptography can also be used as a part of public key infrastructure (PKI) and digital signature. Some research proposed using of many mechanisms as: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Privilege Management Infrastructure [26] [10].

As conclusion, privacy and integrity in healthcare have to assured the trustworthy. Data security and data integrity have to employ some technologies such as: data encryption, security data transfer protocol (e.g. SSL), firewalls, and wireless technology based on the IEEE 802.11 standard [10].

3. PROJECT'S NEEDS AND SECURITY DEMANDS

The project cloud structure has appeared from the project aims and purposes associated with the cross border users needs and with PHR centric healthcare system information security (HSIS) [2] and HL7 standards [9]. As a very complex project, Cross4all cloud system have to pay special attention on the security and privacy concerns, especially in the part of PHR and e-prescription and e-referral system, as well as mobile applications for patients [2]. There were five planned scenarios and three roles of users in the first phase: Physicians, Visitors and Patient. Visitors can access cross border public web portal in order to have public information to the e-learning web platform to increase digital and health literacy. Patients who have their PHR in the system, can give consent for participating in the Cross4all project with a profound description of privacy and security of Cross4all cloud system. They have to grant access to their own data to medical professionals (physicians) in same part of the

systems. The security and privacy policies have to cover use cases with services from the healthcare professionals such as: e-prescription, e-referral, applying sensors for vital sign measuring connected with mobile applications for professionals and storage of patient data in the PHR web platform. Patients will have also possibility to use PHR mobile application for citizens. Sensitive data have to be protected with an important security and privacy protection system, so the purposed model has to be suitable for solving security and privacy concerns [2]. Users' data contain sensitive data such as personal information, health family history, and data from healthcare professionals' and users' measurements. They have to be protected properly [10] following the national regulation regarding personal data.

Healthcare applications deal with personal patient data with embedded privacy and security protection. One of the main HBD issue is the security and privacy of personal identifiable information. The issues of security can be classified into: information security (data encryption, data integration, authentication and freshness protection), and system security (administrative, physical and technical security levels) [28]. Techniques as authentication, encryption, data masking, and access control and monitoring and auditing [27] [17] can be applied to protect and enable their security and privacy. Most of cryptographic protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) use Trusted digital certificates to prevent man-in-the middle attacks and communication security over Internet. Data encryptions algorithms prevent unauthorized access of the sensitive patient data at rest. Healthcare service providers have to ensure easy to use, efficient and easily extensible access to the new EHRs using data encryption framework [27]. Authenticated users, based on the level of digital identity assurance level, as well as on the defined RBAC, and possibly patient consent, will have access to this information.

Standardization is another challenge that enables security access protocols, intrusion detection and prevention techniques to prevent malicious system misusing. Implementation of Security Information and Event Management (SIEM) systems, with audit logs of all user and administrator activities, is also recommended [17].

Explosion of the medical and healthcare data had led to the HBD and appropriate addressing the privacy and security of medical data, suitable for regulation of strict law data protection. Commonly used methods for privacy preserving are de-identification, hybrid execution model HybrEx and identity based anonymization [27]. To provide the privacy of the personally identifiable information and other sensitive healthcare and medical data in cloud environment, ensuring security of the underlying cloud architecture is crucial. In healthcare, an efficient data encryption at rest and in transit by the cloud infrastructure and services has to be deployed [6].

4. PROPOSED SECURITY AND PRIVACY MODEL FOR HEALTHCARE

Cross4all cloud cyberspace (CCC) relies on a security model that enables security, privacy and regulatory aspects of PHR data, enabling data access and management. The key component of the security model addressing issues is Authentication/ Authorization/ Accounting (AAA) server. The AAA server is integrated with attribute authority that provides Role and Routing information for the data storage regulatory requirements, as shown on Fig. 1. AAA *system* is divided into several subsystems as *Authentication* (authentication mechanisms), *Authorization* (Role based access control based on who accesses), *Accounting* (audit trail of user activities) and *Routing* (data storage). We implement a solution where the PHR information of the patients that are physically residing in their country of origin (Greek patient data are residing on servers in Greece and Macedonians patient data are residing on servers in R. of N. Macedonia). So, *AAA layer* of the system is designed to use the keycloack Server [18], which is the most prominent Open Source Identity and Access Management server used in today's modern applications and services. Some geographic distributed requirements of the PHR system in two countries also dictate the authentication and authorization and geo distributed data as well. The distribution has to be user-transparent, i.e. the system has to have a unique and integral ingest API URL location that the end-user apps and integrations would use according to the origin of the request. With multiple keycloak servers that reside in every country and are joined in SSO federation we will solve the geo data distribution. The authentication and authorization requests from end-users and apps are filtered and processed according to the origin domain of their username and then routed to the country and specific keycloak server for further processing. Authentication and Authorization process have to be finished and then the client receives an authenticated token, in order to access the API endpoints and then to PHR data, as shown on Fig. 2.

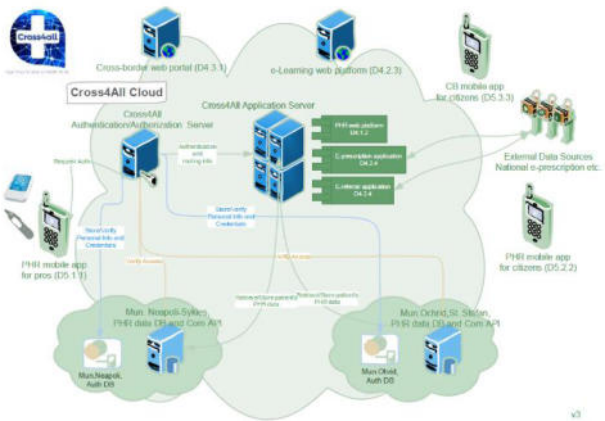

Figure 1. *Core Cross4all Cloud system.*

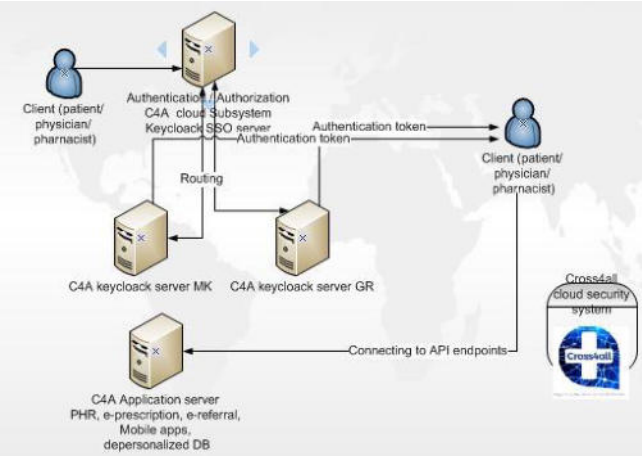

Figure 2. *Proposed model for integrated HCC Cross4all security and privacy.*

The *user access* data are partitioned on the country basis, depending on the country of origin of the user. The user can have associated several roles out of which more important are the patient role, which is the owner of the PHR data and doctor/physician/pharmacist role that can access and create additional PHR data. The *Role based access control for accessing the PHR data* is defined as roles of the users defined in the keycloak SSO servers. Sub-systems that enable appropriate API endpoints follow those Authorization rules and provide or deny access to the PHR data. The authentication rules can be modified in this way, while the system is in production and additional data access segmentation rules can be also added.

The *data acquisition* from the patients or doctors/ physicians is done via customized smartphone and tablet applications from smart medical devices such as bluetooth enabled devices. Healthcare data are linked to the PHR according to the access rules assigned and encrypted using AES256 or RSA2048/RSA4096. Data cannot be accessed even with direct access to the MongoDB database. Encryption at rest provides support for GDPR and HIPAA compliance rules and generates a lag in the data access that is needed for encryption and decryption of the data while it is being accessed. Encrypted data can be further segmented in two parts: user-identifiable part and depersonalized medical data part. These two parts use different encryption keys and provide better security segmentation. The possibility to provide access to depersonalized health record data, for specific roles that need access to the data for data analysis purposes can be also defined in keycloak system layer and enforce on the API layer access.

This kind of design of the PHR and used topology of its security and privacy system, have to enable several layers of data access and data application. Managers and health policy makers can have access through dashboards with depersonalized and aggregated healthcare data of suitable participating countries. Security layer implementation has to provide controlled access to the sensitive data with patient consent and knowledge. Usage of depersonalized patient's data for data analysis will satisfy managers and policy makers' demands without violating patients' data security and privacy.

5. CONCLUSION AND FUTURE WORK

The proposed cloud architecture intends to provide information security for the project users that have to use Cross4all cloud with defined roles. The controlled connection for patient and physicians as well as pharmacists have to be provide in order to gain access to a part of digital assets created for the project. The most critical point of the project's cloud system is PHR data access for the patient as owners. Second critical point is the access of medical practitioners and physicians, involved in the pilot project in municipality and project's technical staff, who are in charge for technical support of the project architecture, hardware and software used as Cross4all cloud.

The model for Authentication/ Authorization server for security and privacy, proposed for this project, has many security levels. The Authentication layer is designed using the keycloack Server. When authentication and authorization are finished, patient of physician will receive an authenticated token. It can be used to access the API endpoints and then to PHR data. PHR data are stored in non-relational document-based database with encrypted at rest data with AES256 or RSA2048/RSA4096, so data are protected. Encryption at rest provides support for GDPR and HIPAA compliance rules generating a lag in the data access, needed for encryption and decryption. The validation of the model is done in small number of trials, with intention to be verified at 500 patients and physicians in the pilot project in the Ohrid and Sykies municipalities, implementing the digital assets created by the project partners.

Software application developing methods and APIs have to ensure security and privacy of PHR data and computation over hybrid cloud ecosystems. Data will be stored in several datacenters, which is still a developing activity. Our efforts will be directed towards developing computationally efficient privacy preserving methods taking into account the multiple big data sources that have to be analyzed in an elastic hybrid cloud infrastructure.

REFERENCES:

[1] Web Content Accessibility Guidelines (WCAG) 2.0; https://www.w3.org/TR/WCAG20/, Accessed 10.5.2019
[2] Cross4all FIKT web site, crodd4all project matherials, https://cross4allfikt.wixsite.com/project-mk, Accessed 1.4.2019

[3] Wan K.Y., Alagar V., Characteristics and Classification of Big Data in Health Care Sector, 2016, 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 978-1-5090-4093-3/16, IEEE
[4] Ristevski, B. and Chen, M., 2018. Big Data Analytics in Medicine and Healthcare. Journal of integrative bioinformatics, 15(3)
[5] M. Househ &all, Big data, big challenges: A Healthcare Perspective, Background, Issues, Solutions and Research Directions, Elizabeth M. Borycki and Andre W. Kushniruk, Big Data and Patient Safety, Springer, 2019, ISBN 978-3-030-06109-8 (eBook)
[6] Nepal, S., Ranjan, R. and Choo, K.K.R., 2015. Trustworthy processing of healthcare big data in hybrid clouds. IEEE Cloud Computing, 2(2), pp.78-84.
[7] Weber G.M., Mandl K.D. and Kohane I.S., Finding the Missing Link for Big Biomedical Data, JAMA, June 25, 2014, Volume 311, Number 24
[8] Savoski Z., Savoska S., E-health, Need, Reality or Mith for R.of Macedonia, In proceedings of AIIT 2018 conference, 4-5.10.2018, DOI:10.20544/AIIT2018.P12, pp.56-59
[9] M. Househ &all, Big data, big challenges: A Healthcare Perspective, Chapter: Fernandez-Luque L. and all, Health Lifestyle Data-Driven Application Using Pervasive Computing, Springer, 2019, ISBN 978-3-030-06109-8 (eBook)
[10] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Framework for Improving Critical Infrastructure Cyber security and related news, information: www.nist.gov/cyberframework, Additional cybersecurity resources: http://csrc.nist.gov/F.
[11] Shrestha N.M. and all, Enhanced e-Health Framework for |Security and Privacy in Healthcare System, ISBN: 978-1-4673-7503-0, @2016 IEEE
[12] Shin M, Jeon H, Ju Y, Lee B, Jeong S., Constructing RBAC based security model in u-healthcare service platform. Sci World J 2014;1–13
[13] Gajanayake R, Iannella R, Sahama T., Privacy oriented access control for electronic health records. e-J Health Inf 2014;8(2):175–86
[14] Bhartiya, S, Mehrotra, D, Girdhar, A., Proposing hierarchy - similarity based access control framework: A multilevel Electronic Health Record data sharing approach for interoperable environment. Journal of King Saud University – Computer and Information Sciences, 1-15 (August 2015)
[15] Kahani, N, Elgazzar, K, Cordy, K., Authentication and Access Control in e-Health Systems in the Cloud. In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (BigDataSecurity),New York, NY, USA, 2016, pp. 13–23.
[16] Azeez N.A., Vyver C.v.d., "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", Egyptian Information Journal, vol. 93, pp. 237-255, Apr. 2019.
[17] Abouelmehdi, K., Beni-Hessane, A. and Khaloufi, H., 2018. Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), p.1.
[18] RedHat keycloak web site, https://www.keycloak.org, Accessed 12.4.2019
[19] David Lobach et al. (2012), Enabling health care decision making through clinical decision support and knowledge management, Evidence Report/ Technology Assessment. 2012 Apr; (203): 1–784
[20] Christo El Morr, Julien Subercaze, (2010).Chapter 23: Knowledge Management in Healthcare, In book: Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives. Publisher: IGI Global. DOI: 10.4018/978-1-61520-670 4.ch023. https://www.researchgate.net/publication/230682282_K nowledge_Management_in_Healthcare[accessed Jun 22 2019]
[21] Abidi, S. S. R., (2008),"Healthcare knowledge management: The art of the possible," in In Proceeding of K4CARE, LNAI 4924, pp. 1–20
[22] Evans J.M., Brown A. and Baker G.R.,. (2017). Organizational knowledge and capabilities in healthcare: Deconstructing and integrating diverse perspectives, SAGE Open Medicine. Published online 2017 Jun 6.doi: 10.1177/2050312117712655
[23] Abidi, S. S. R. (2001). Knowledge management in healthcare: towards 'knowledge-driven' decisionsupport services. International Journal of Medical Informatics, 63(1-2), 5–18. doi:10.1016/S13865056(01)00167-8
[24] Elliott, S., & O'Dell, C. (1999). Sharing knowledge & best practices: The hows and whys of tapping your organization have hidden reservoirs of knowledge. Health Forum Journal, 42(3), 34.
[25] Bertino et al. (2006).Secure Knowledge Management: Confidentiality, trust, and privacy. IEEE Transactions on systems, man, and cybernetics—part a: systems and humans. Vol. 36, Np. 3, Mat 2006
[26] Darren Mundy D. and Chadwick D.W.,. Secure Knowledge Management for Healthcare Organizations Chapter In book: Creating Knowledge-Based Healthcare Organizations (January 2004)DOI: 10.4018/9781591404590.ch023
[27] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. and Saadi, M., 2017. Big Data security and privacy in healthcare: a review. Procedia Computer Science, 113, pp.73-80.
[28] Baig, M.M., Gholam-Hosseini, H. and Connolly, M.J., 2015. Mobile healthcare applications: system design review, critical issues and challenges. Australasian physical & engineering sciences in medicine, 38(1), pp.23-38.

About the authors:

Savoska Snezana, "St. Kliment Ohridski" University – Bitola, Faculty of Information and Communication Technologies- Bitola, Associate professor, PhD, Local coordinator of Cross4all IPA2 project for UKLO-FIKT Bitola.
Jolevski Ilija, "St. Kliment Ohridski" University – Bitola, Faculty of Information and Communication Technologies- Bitola, Professor, PhD. Technical coordinator of Cross4all project for UKLO-FIKT Bitola.
Ristevski Blagoj, "St. Kliment Ohridski" University – Bitola, Faculty of Information and Communication Technologies- Bitola, Associate professor, PhD.
Blazeska-Tabakovska Natasha, "St. Kliment Ohridski" University – Bitola, Faculty of Information and Communication Technologies- Bitola, Associate professor, PhD.

Bocevska Andrijana, “St. Kliment Ohridski” University – Bitola, Faculty of Information and Communication Technologies- Bitola, Associate professor, PhD.
Jakimovski Boro, Ss Cyril and Methodius University in Skopje, Faculty of Computer Science and Engineering, Associate professor, PhD.
Chorbev Ivan, Ss Cyril and Methodius University in Skopje, Faculty of Computer Science and Engineering, Associate professor, Professor, PhD.
Kilintzis Vassilis, Lab of computing, Medical and Computing Informatics and Biomedical Imaging Technologies, Aristotle University of Thessaloniki, Greec