Emergency Health Protocols Supporting Health Data Exchange, Cloud Storage, and Indexing

Konstantinos Koutsoukos[1,2], Chrysostomos Symvoulidis[1,2], Athanasios Kiourtis[1],
Argyro Mavrogiorgou[1], Stella Dimopoulou[1,2] and Dimosthenis Kyriazis[1]
[1]Department of Digital Systems, University of Piraeus, Piraeus, Greece
[2]BYTE S.A., Athens, Greece

Keywords: Emergency, Electronic Health Records, EHR Cloud, Remote-to-Device.

Abstract: The health industry has evolved significantly through the last years by adapting to the new technologies and exploiting them in order to upgrade the services that provides to the people. In this context, a lot of effort has been focused on converting medical documents to electronic health records and storing them online. However, taking into consideration the current innovations, it is doubtless that there are many limitations when these proposals are applied in a real-life scenario. For this reason, this paper proposes a system that combines electronic data storage and health record exchange between individuals and authenticated medical staff in a secure way. The specific recommendation is being evaluated through the corresponding applications and protocols that are developed and finally, the results exhibit the solutions over existing gaps.

1 INTRODUCTION

The Healthcare industry is increasingly adopting new technologies to enhance and facilitate citizens' care. Over the years, paper-based medical records have been replaced with Electronic Health Records (EHR). EHRs offer real-time updates of data and access from any authorized user all around the world. Healthcare organizations are taking advantage of modern technology and devices such as mobiles, wearables, sensors, etc., to gather more precise information about the citizens and eventually offer appropriate treatment (Zewe, 2021). The long-range scope of this initiative is to improve the quality of life by predicting deadly diseases, monitoring citizens' habits, and intervening when it is needed.

Even though almost every Health Organization uses EHR technologies, in most cases, it is implemented locally or in association with limited health centers. Therefore, when a citizen needs to get treatment and has to interact with multiple Healthcare Practitioners (HCP), the health information is not exchanged among them and needs to be done traditionally, since they are not connected to a central health network.

Consequently, a common mechanism that is used by every healthcare organization can enhance the HCPs' services and offer a better treatment service to the citizens. By exploiting two communication protocols that will be analyzed later in Section 3 of the paper, the EHR can be uploaded to any available cloud service and be safely stored. Additionally, whenever an HCP needs access to the citizen's health record, an intermediate mechanism will redirect her to the health record location where the information will be up to date. For example, in the case a citizen has multiple appointments to attend, the data will be immediately updated after treatment for the next HCP to use.

The vital importance of such a mechanism is becoming better understood by applying it to an emergency scenario. In the case a citizen needs immediate treatment, multiple stakeholders should be able to gain access without any delays and the information must be accurate and up to date. By assuming that the citizen has made some changes or has visited a doctor a short time before the accident, there is a high risk that the newly generated data will not be available to the HCPs. And in such cases, there is no room for unnecessary risks. In this context, this paper proposes the protocols that are responsible for the proper communication and data exchange between citizens, healthcare practitioners, and cloud providers. Moreover, it suggests a background service which facilitates the handling of urgent

Koutsoukos, K., Symvoulidis, C., Kiourtis, A., Mavrogiorgou, A., Dimopoulou, S. and Kyriazis, D.
Emergency Health Protocols Supporting Health Data Exchange, Cloud Storage, and Indexing.
DOI: 10.5220/0010878900003123
In *Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2022) - Volume 5: HEALTHINF*, pages 597-604
ISBN: 978-989-758-552-4; ISSN: 2184-4305

situations, when the citizen is not able to grant access to the uploaded data.

The rest of the paper is organized in the following sections. Section 2 introduces the related work and research that has been conducted regarding the communication between the involved entities, the techniques used to redirect users to the proper services, and the security aspect of the data exchange. It also highlights the deficiencies of these systems and recites the features that the proposed mechanism should cover. Afterwards, the overall methodology is presented in section 3 by analyzing the involved applications and by explaining the real-life scenario step by step. Section 4 includes a demonstration of the system's functionality and makes a thorough evaluation. Finally, section 5 introduces the research conclusions and results as well as future plans.

2 RELATED WORK

2.1 Remote-to-Device (R2D) Backup Protocol

The communication between user applications and cloud providers is rapidly becoming a common occurrence since it facilitates the storage of vital personal data and its fast and constant retrieval. To begin with, Dropbox (Dropbox for HTTP Developers, 2021) offers the possibility to connect an application with the cloud and interact with each other by exchanging data. This is achieved by a group of APIs that support the communication through a set of HTTP endpoints that are used to establish the communication between the two entities. In the same direction, DataVaults (DataVaults Empowering Secure Data Storage, Sharing and Monetisation, 2021) aims to give users the ability to fully manipulate their data and share it with other organizations or individuals by adopting adjustable sharing schemes. Meanwhile, it offers an innovative framework whose main scope is to gather information derived from several sources and finally provide them in a secure and interoperable manner to the users. As the overall purpose of the paper suggests, these technologies offer limited functionalities when it comes to time efficiency. Therefore, it makes sense that this kind of services should not be trusted with vital data such as EHR.

2.2 Remote-to-Device (R2D) Emergency Protocol

Many cloud providers offer the opportunity to handle emergencies and other situations where data access from third parties has a vital significance. Concerning this, some services provide APIs that are responsible for sharing the data with one or more stakeholders when needed. At the same time, several studies have proposed ways to cope with health-related incidents. In (Oliveira et al., 2020) the authors suggest a Red Alert Protocol (RAP) to address situations when the citizen is not conscious. In the emergency session, a central authority links the responsible treatment teams to the citizen's EHR which is stored in the cloud. Using an access token to download the data and an emergency key to decrypt it, the medical staff acquires access to the medical records. After the procedure, the access tokens are either removed or expired and the HCPs can no longer use the citizen's information. Although this approach offers an innovative way to deal with emergencies, it cannot be used in other occasions such as medical visits. In that way, a health organization should integrate more systems for different situations and create a complex procedure. In a similar manner, (Banerjee et al., 2013) talks about a centralized cloud database that will store every user's medical history in a single standard-formatted and interoperable document. By exploiting the multi-document summarization technique, the system creates a single summarised document that contains the complete medical history of that person. Using a graph-based ranking algorithm the system creates a summary for every single document and then a meta-document is produced to generate the result. The main concept is to authenticate the citizen with the use of biometric data and finally retrieve the appropriate data to use for the operation. Even though biometric authentication is an efficient way to access personal records, it should not be the only option since, in emergency cases the citizens' condition may not support this procedure.

2.3 Health Record Index

Health record indexing is a very crucial procedure since the quick response and retrieval of the requested data can be lifesaving. Especially when there are more than one sources that EHR can be stored to, this challenge is a lot more demanding. Several types of research and studies take into consideration that the needed information may be distributed in different sources and need to be gathered. Primarily, the authors of (Ehler et al., 2007) proposed an

Information Retrieval (IR) tool to index and retrieve citizens' EHR. The system creates a table for each document which contains a table with every word in the document along with its frequency rate. Taking into consideration the query, the system locates and retrieves the documents that contain the query keywords at a high-frequency rate. The authors in (Wan et al., 2019) dealt with geographic data collected from the real world through sensors. Real-time data creates a challenge since it can be unpredictable. Hence, they proposed a multidimensional data indexing scheme to handle large queries. The proposed methods are utilizing hierarchical indexing structures by running binary space partitioning (BSP) algorithms like kd-tree, quad-tree, k-means clustering, and Voronoi-based methods striving for better efficiency with less latency. After a set of detailed simulations, it resulted that the Voronoi diagram data index model is the most suitable since it minimizes the average query response time and energy consumption. These are the parameters that have stimulated the interest of the researchers. Finally, a recent study (Yao et al., 2018) demonstrates an indexing mechanism over EHRs. The overall concept is referring to citizens as data owners and they are responsible of their own data. Doctors, health sensors or any source that can generate data is referred as data provider. Given the owner's consent, they can upload EHR to the cloud along with an index which will be used for the retrieval. Coming from any source, the data is always encrypted before being uploaded to the cloud. The request for the health records is performed in the form of a query from an authorized health provider. The cloud service indexes the stored data according to the corresponding indexes and returns the proper medical data without decrypting it. Eventually, the provider can access the records with the use of a decryption key. The idea of uploading EHR to a publicly reachable location with the proper security has significantly enhanced the communication between medical personnel and citizens. However, these techniques have limited efficiency when it comes to emergencies. In most cases, the proposed way to identify the citizen is through credentials, which it will be a major obstacle when the data accessing is vital. Furthermore, the proposals are trying to deal with specific problems and circumstances and are not flexible enough to accommodate different conditions.

2.4 Encryption Mechanisms

When it comes to personal health data it is crucial to study thoroughly the security aspects of the proposed system. Therefore, encryption techniques are used to prevent internal attacks as long as secure data transfer. Since there is a large number of security techniques, there are studies that focus on choosing those that can be used in the health industry. According to (Madnani et al., 2013) these are symmetric-key cryptography, public-key cryptography, and attribute-based encryption. In (Abbas et al., 2014) the proposed system encrypts the data using an encryption key known by the cloud provider. However, this approach raises the concern of internal attacks considering that acquiring that key gives access to all the stored data connected to it. The proposal in (Yang et al., 2019) presents a system that combines attribute-based encryption and password-based break-glass (Scafuro et al., 2019) key to create a self-adaptive access control scheme. More recently, (Oliveira et al., 2020) suggests the involvement of ciphertext-policy ABE (CP-ABE) associated with emergency situations' policies.

2.5 Advancements beyond the Related Work

Resulting from the previous studies and works it has been obvious that the storage of medical records in cloud repositories has been rapidly evolved regarding the plurality of services, techniques, and consistency. Nevertheless, the ability to handle emergency situations is what challenges the researchers since it is very demanding to combine punctual reaction and security. Additionally, most of the proposals are restricted to a certain country's infrastructure or adjusted to a specific scenario with known and tested circumstances. As a result, this paper proposes a system that tries to eliminate these gaps. This is achieved by making the service centralized so that authenticated personnel can gain access regardless of the country where the citizen comes from. Moreover, it attempts to create a paradigm that HCPs can use to download the EHR even when the citizen is unconscious. It is important to propose a way to secure the data in every stage of the process. Finally, the recommended service should be applicable to any possible scenario while it complies with all the parameters.

3 METHODOLOGY

3.1 Involved Applications

To better understand the overall methodology, the involved terminologies should be presented and analyzed. All the following applications are developed in the context of the Interopehrate research project for this research.

3.1.1 S-EHR Application

The Smart-EHR application is a mobile application developed to be used by citizens. This application stores locally the user's EHR and data generated by sensors or after a medical visit. Additionally, the user can use the application in order to upload the EHR to a S-EHR Cloud of their choice. Finally, as will be thoroughly described in the following section, citizens may give their consent for the EHR to be accessed by authorized HCPs in emergency situations. When a citizen registers to the service, a Quick Response (QR) code is generated. This QR code contains crucial information such as the citizenId, an emergency token, an encryption key, and the Health Record Index (HRI) location (Kiourtis et al., 2021).

3.1.2 S-EHR Cloud

The Smart-EHR Cloud as presented in (Symvoulidis et al., 2021) is a cloud service that provides storage for EHRs. Taking into consideration that users have previously agreed to share this data when needed, authorized HCPs can access these records and use them to treat the citizen as will be depicted later. Furthermore, storing health data in the cloud can be used as a backup in case the citizen's device is damaged or unreachable. Lastly, the S-EHR Cloud stores audit information that keep track of every procedure made by clinicians or citizens and can be accessed through the citizen's S-EHR app.

3.1.3 HCP Application

HCP application is a software application, operated by medical staff and provides a way to access cloud storage and download citizens' health data assuming that it is encrypted, and authentication operations have been completed. More precisely, by exploiting a set of credentials that identify both the clinician and the healthcare organization, the system confirms that the request is originated from an eligible and authenticated source. Since the overall system needs to be supported across Europe, every HCP app uses an integrated translation system that converts the crucial information into the appropriate language (Bella et al., 2021).

3.2 Emergency Scenario Overview

This section demonstrates the precise procedure that every entity is going through by the time an emergency occurs. Moreover, the actions that need to be done prior to this incident are also analysed by examining the protocols.

3.2.1 R2D Backup Protocol

This protocol focuses on the preliminary actions that need to be done when a citizen starts using the S-EHR application. Its purpose is to allow users to safely backup their health records in a remote repository and correspondingly download them at any time (Symvoulidis et al., in press). Likewise, in this stage, the citizen may sign a consent that allows HCPs to have access to the stored data if it is necessary.

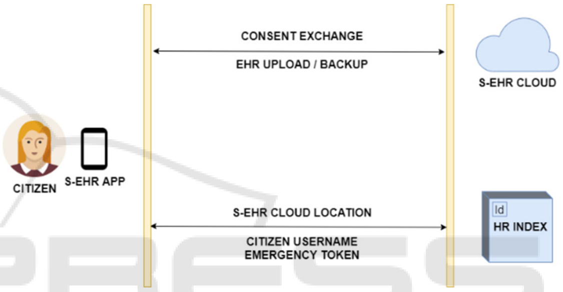


Figure 1: R2D Backup Protocol.

In Figure 1 the general idea of the protocol's functionality is depicted by presenting the main operations taking place between the entities. As detailed below, the complete procedure consists of the following stages. Formerly, the user registers to the preferred cloud service through the Smart-EHR application. Later, several consents need to be signed by the user to allow the S- EHR Cloud to store the data and agree with the sharing of the medical record with authorized medical staff. It is important to note that the latter is an optional consent. In the case the user accepts the first term, it results in generating an access token which is sent to the mobile device. As a result, the S-EHR application generates an encryption key which will encrypt the data before uploading it to the cloud. By the time the citizen agrees with the second term, there is a sequence of actions that are taking place. Firstly, an emergency token is generated and stored in the app. Secondly, Smart-EHR sends information to the HR Index, containing the cloud provider, the citizen's username, and the emergency token. Then a QR code is created, containing the encryption key, the emergency token and information regarding the user's HRI entry such as a citizen ID.

However, if the latter consent is not signed, the cloud will not be able to share the data with any third parties and the selected service will be only used as a backup. Taking into consideration that the first consent has been signed, the user is able to upload the EHR to the cloud. Using the encryption key, which is stored in the app, the health data is being encrypted and uploaded to the S-EHR Cloud. From now on, the uploaded records will be automatically updated if any changes are made to the local files. Finally, in case the citizen uses a different device, it is always possible to login to the S-EHR application using the credentials and download the health records from the cloud which will then be decrypted and accessible through the application. It is worth mentioning that the user can any time withdraw the consent and change the permissions to the data.

3.2.2 R2D Emergency Protocol

The R2D Emergency protocol is an internet-based protocol which defines the actions that are taking place between the S-EHR Cloud and the HCP application when an emergency occurs in order to allow the HCP to access the citizen's health data from the S-EHR Cloud (Symvoulidis et al., in press). Both protocols support Fast Healthcare Interoperability Resources (FHIR) for the exchange of EHRs (Kiourtis et al., 2018). Moreover, compliance checking is performed to the exchangeable files to assure advanced interoperability.

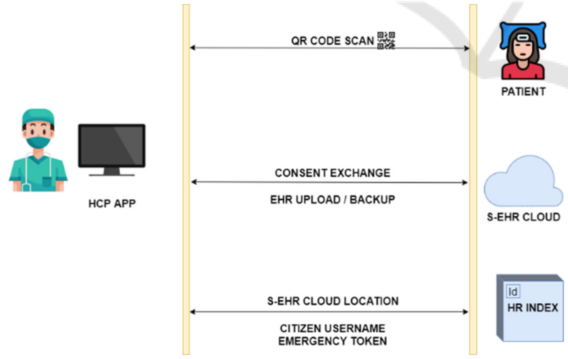


Figure 2: R2D Emergency Protocol.

Figure 2 shows the sequence of the performed operations when a citizen is admitted to the hospital due to an emergency. At the initial phase of the emergency, the HCP who is responsible for the patient's treatment needs to collect the QR code and scan it to acquire the necessary information for the operation. As described in section 3.2.1 the QR scanning provides the emergency token which will be used to make the request to the S-EHR Cloud, the encryption key that will decrypt the data as long as it is downloaded, and finally, information about the HR Index entry to retrieve the cloud location. Following the successful scanning, an automatic request is sent to the HRI, and the cloud provider used by the citizen is returned as a response. Hence, the HCP has everything that is needed to request the citizen's EHR from the cloud. With the use of the emergency token along with the HCP and healthcare center attributes, the S-EHR Cloud approves or declines the request. In the first case, the data is downloaded in an encrypted format and can then be decrypted locally using the encryption key. Otherwise, the connection is terminated and no interaction with the data is possible. It is worth mentioning that after the completed verification, the connection remains open so that the medical records on the cloud will be updated with the new encrypted data after the treatment is completed and the patient is discharged. All this time, the S-EHR application creates a notification to the citizen's mobile regarding the actions made by the HCP over their medical records.

3.2.3 Health Record Index

The role of the HR Index has been stated previously with the description of the protocols. To better understand its utility, the scenario needs to be tested on a situation with special parameters. As it was explained previously, the citizen chooses a cloud provider to upload the medical information and then acquires a QR code which will be printed also on a card for easier access. Without the HRI, the QR code would contain a direct link to the cloud service. On the assumption that the user decides to use a different cloud service, the records will be removed from the first cloud and be encrypted and uploaded to the new one. Supposing that an emergency occurs, and the citizen needs to be treated immediately, the HCP will scan the QR code as depicted earlier and will be redirected to the wrong cloud location which does not store the user's records. Health Record Index overcomes this issue since it is automatically updated when the cloud is changed and functions as a mediator between the HCP and the cloud. As a result, the scanning will always return real-time information to the health center and will prevent vital implications. It is worth mentioning that the HR Index is a background service and neither the S-EHR application user nor the HCP has direct interaction with it.

3.2.4 Encryption Mechanisms

Every stage of the overall process should be characterized by indisputable security. When it comes to personal health data, any risks should be eliminated on data storage and on data transit. Therefore, both protocols are using a set of encryption technologies to safely transfer the data and also to allow only certified entities to have access. R2D Backup protocol uses the Advanced Encryption Standard 256 (AES-256) which is a symmetric-key algorithm to encrypt the data locally in the S-EHR app. This means that a single key is used for both encryption and decryption. This key is exchanged between citizens and medical staff through the QR code after scanning. Additionally, when citizens use their credentials to log into the S-EHR Cloud, a JSON Web Token is returned to the mobile application. Then with the proper JWT authorization, the encrypted data can be uploaded to the cloud.

4 EXPERIMENTATION

4.1 Working Environment & Scenario

In this research, a set of services and libraries were developed to demonstrate and test the functionality. Specifically, the HCP application and the HR index have been developed in Java v.8.0 while the S-EHR application runs on Android v4.3.1 and above. Regarding the two protocols, a set of Java libraries were built to implement the communication of the components according to the protocols' specifications. Figure 3 demonstrates all the involved entities and the interactions between them, in the context of the evaluation scenario that has been implemented.

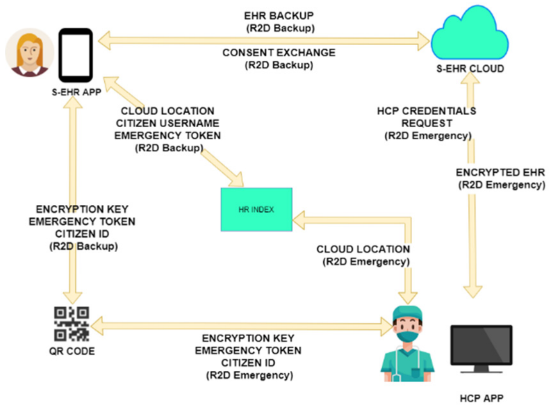
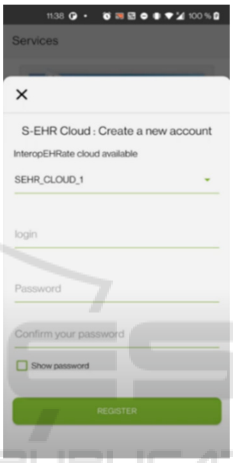


Figure 3: Overall scenario and interactions.

4.2 Preliminary Evaluation

To practically test the operational qualification of the system, the developed services were used to demonstrate the citizen's user experience. At the beginning, the citizen registers to one of the available S-EHR Cloud providers through the S-EHR application as shown in Figure 4. Later, two consents need to be signed regarding the health record storage on the cloud for backup purposes and then to allow authorized HCPs access the health data. The corresponding functionality is depicted in Figure 5, Given that the consents are signed, the citizen uploads the EHR to the S-EHR Cloud provider via the R2D Backup protocol.

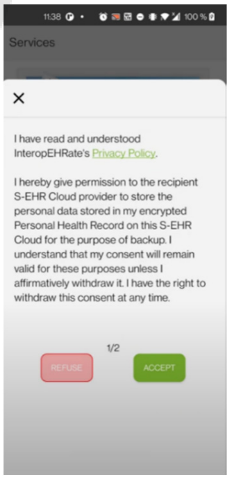


S-EHR Cloud : Create a new account

InteropEHRate cloud available

SEHR_CLOUD_1

Figure 4: S-EHR Cloud registration.



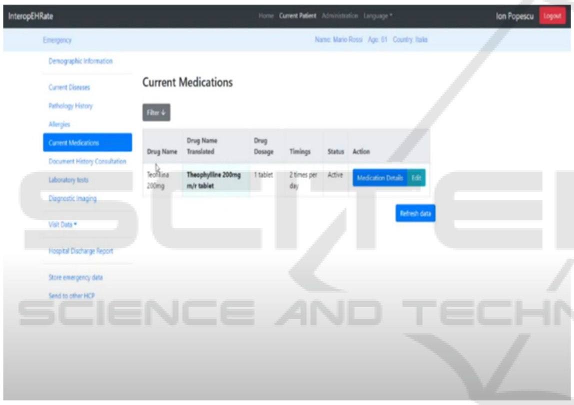
I have read and understood InteropEHRate's Privacy Policy.

I hereby give permission to the recipient S-EHR Cloud provider to store the personal data stored in my encrypted Personal Health Record on this S-EHR Cloud for the purpose of backup. I understand that my consent will remain valid for these purposes unless I affirmatively withdraw it. I have the right to withdraw this consent at any time.

Figure 5: Consent approval option.

After the successful registration, the encrypted data is uploaded to the cloud and the QR code is created and presented to the users along with options to change their preferences and optionally revoke their signed consents. From this time, the local files are periodically synchronized with the cloud to keep them up-to-date. This step summarizes the user interface regarding the Smart EHR application.

At a later time, an emergency occurs and the citizen is transferred to the Healthcare organisasation where HCPs need to address it in order to offer direct treatment. To do so, they must provide their attributed credentials to log into the HCP app. Since the citizen is unable to assist the clinicians with vital personal information, the unique QR code is scanned through the HCP app. Following the scanning, the involved information is presented encrypted in the application interface. At this point, the HCP can request access to the EHR. Providing the information is right and the credentials are validated by the S-EHR Cloud, a success message will inform the medical staff that the connection has been established and they can access all the citizen's data in a structured way, via the R2D Emergency protocol, as depicted in Figure 6.



Current Medications

Drug Name	Drug Name Translated	Drug Dosage	Timings	Status	Action
Teofilina 200mg	Theophylline 200mg m/r tablet	1 tablet	2 times per day	Active	Medication Details Edit

Figure 6: EHR through the HCP app.

After the treatment, the HCP compiles a Discharge Report with the procedure details along with therapy and future recommendations and uploads it with the updated data to the S-EHR Cloud.

5 CONCLUSIONS

The healthcare field has recently presented many advancments regarding the exchange of data between HCPs and citizens. However the limitations of the existing systems have created the need of a proposal that offers a functionality beyond these restrictions. This paper, proposed a system that can take these studies a step further. For this reason, two protocols were defined to facilitate the secure backup of medical data to EHR-based cloud providers and enhance the exchange of crucial data between Healthcare Professionals and citizens during emergency situations. Additionally, HRI is offered to deal with the case there are multiple cloud services and redirect the medical staff to the proper one.

During the evaluation process, some restrictions came up that did not comply with the initial scenario design. For example, there is no assurance that the citizen's QR code will always be reachable. Morever, the effort has been focused on handling emergency occasions. This approach could also be applied in other situations such as everyday medical visits but without the proper functionalities since this paper does not cover that view.

Therefore, concerning the following steps, the goal is to extend the area where the protocols function in order to be applicable in more scenarios with the same performance. Besides, the QR code accessing should be evaluated and saved in a way to be always available. For the time being, QR code is the main tool for data accessing in emergency scenarios, but the fact that its complexity is increased as more information is stored, it may create the need to examine other possibilities like Near-Field Communication (NFC) tags (Vidakis et al., 2020). Finally, it is important to constantly improve the performance of the protocols as far as efficiency and security is conserned, since the needs and the figures are always changing.

ACKNOWLEDGEMENTS

The research leading to this result has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106 (InteropEHRate project).

REFERENCES

Abbas, A., & Khan, S. U. (2014). A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds. IEEE Journal of Biomedical and Health Informatics, 1431–1441.

Banerjee, A., Agrawal, P., & Rajkumar, R. (2013). Design of a cloud based emergency healthcare service model. 2261–2264.

Bella, G., Bocca, S., Torelli, F., Dalmiani, S., & Duflot, P. (2021, February). Design of information extractor and natural language translator - v1. https://www.interopehrate.eu/wp-content/uploads/2021/04/InteropEHRate-D5.11-Design-of-information-extractor-and-natural-language-translator-v1.pdf

DataVaults Empowering Secure Data Storage, Sharing and

Monetisation. (2021). DataVaults. Retrieved 2021, from https://www.datavaults.eu/about/

Dropbox for HTTP Developers. (2021). Dropbox. Retrieved 2021, from https://www.dropbox.com/developers/documentation/http/overview

Ehler, F., Ruch, P., Geissbuhler, A., & Lovis, C. (2007). Challenges and methodology for indexing the computerized patient record. 129(Pt 1):417–21.

Kiourtis, A., Mavrogiorgou, A., Symvoulidis, C., Tsigkounis, C., & Kyriazis, D. (2021, January). Indexing of Cloud Stored Electronic Health Records for Consented Third Party Accessing. In 2021 28th Conference of Open Innovations Association (FRUCT) (pp. 158-166). IEEE.

Kiourtis, A., Mavrogiorgou, A., & Kyriazis, D. (2018, September). FHIR Ontology Mapper (FOM): Aggregating Structural and Semantic Similarities of Ontologies towards their Alignment to HL7 FHIR. 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom).

Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 89–106.

Madnani, B., & Sreedevi, N. (2013). Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation. 2320–9801.

Scafuro, A. (2019). Break-glass Encryption. IACR International Workshop on Public-Key Cryptography – PKC 2019, 34–62.

Symvoulidis, C., Kiourtis, A., Mavrogiorgou, A., & Kyriazis, D. (2021). Healthcare Provision in the Cloud: An EHR Object Store-based Cloud Used for Emergency. In HEALTHINF (pp. 435-442).

Symvoulidis, C., Mavrogiorgou, A., Kiourtis, A., Marinos G., Kyriazis D. (in press). Facilitating Health Information Exchange in Medical Emergencies. In 2021 E-Health and Bioengineering Conference (EHB). IEEE.

T. De Oliveira, M., Bakas, A., Frimpong, E., Groot, A. E. D., Marquering, H. A., Michalas, A., & Olabarriaga, S. D. (2020). A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud. Annals of Telecommunications, 103–119.

Vidakis, K., Mavrogiorgou, A., Kiourtis, A., & Kyriazis, D. (2020, June). A Comparative Study of Short-Range Wireless Communication Technologies for Health Information Exchange. 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE).

Wan, S., Zhao, Y., Wang, T., Gu, Z., Abbasi, Q. H., & Choo, K. K. R. (2019). Multi-dimensional data indexing and range query processing via Voronoi diagram for internet of things. Future Generation Computer Systems, 382–391.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences, 567–592.

Yao, X., Lin, Y., Liu, Q., & Zhang, J. (2018). Privacy-Preserving Search Over Encrypted Personal Health Record In Multi-Source Cloud. IEEE Access, 3809–3823.

Zewe, A. (2021, September 23). Toward a smarter electronic health record. MIT News. Retrieved 2021, from https://news.mit.edu/2021/medknowts-electronic-health-record-0923