Healthcare Provision in the Cloud: An EHR Object Store-based Cloud Used for Emergency

Chrysostomos Symvoulidis[1,2], Athanasios Kiourtis[1], Argyro Mavrogiorgou[1] and Dimosthenis Kyriazis[1]

[1]*Department of Digital Systems, University of Piraeus, Piraeus, Greece*

[2]*BYTE S.A., Athens, Greece*

Keywords: EHR Cloud, Object Storage, Emergency, Storage Clouds.

Abstract: EHR Cloud architectures have come a long way within the last years, giving the ability to individuals to store their healthcare data in the cloud, thus being accessible at all times. Though Electronic Health Records (EHR) and Personal Health Records (PHR) sharing technologies have been developed over the last decades, and a lot of the attention is given on the exchange of healthcare data between organizations and healthcare institutions, less emphasis has been put in the services regarding the exchange of such data between individuals and healthcare professionals and the issues that this gap creates are yet to be answered. To this end, in this paper, we introduce an EHR Cloud-based system that utilizes an Object Storage architecture to store healthcare data, and provides the ability to authenticated healthcare professionals to gain access if needed during an emergency, in an automated yet secure way, for accelerated health services provision. The proposed approach is evaluated and the results are presented in order to justify the rationale behind its design.

1 INTRODUCTION

Cloud computing has come a long way during the last two decades, becoming a state of the art solution for the provision of services across all areas; from finance and banking systems, to hosting the elections of a country. Let alone, the healthcare industry where the cloud can play a huge role.

The adoption of cloud in the healthcare leads to great changes that impact highly the way the healthcare professionals work (Vinati Kamani, 2019), making their job easier, faster, and more efficient. For instance, there has been a major impact on the way the produced health-related data are managed and analyzed. Healthcare data regard a significant asset that without cloud computing could not be exploited in its full potential. Powerful cloud-hosted services that utilize techniques like Big Data analytics and Artificial Intelligence (AI), can now analyze tons of newcoming data at a glance, making the process not only easier, but faster too, while expanding several possibilities (Martin, N., 2019; Davenport and Kalakota, 2019).

Interoperability issues over healthcare systems across different organizations regards a great concern that until now is not entirely dealt with. But, big steps are taken towards that direction, and cloud computing assists considerably. A typical example, regards the report by West Monroe Partners (Cohen, 2018), stating that 35% of the questioned organizations store more than 50% of their healthcare data in the cloud. This brings new potential to solving the interoperability issues, by allowing inter-institutional data exchange.

Nevertheless, the impact that cloud computing leaves on the healthcare sector is mostly related on evolving the systems and procedures in healthcare institutions, something crucial and of high importance. But small, or rather less attention is given on the creation of services that could give the ability to individuals to collect and manage their own healthcare data, as well as exchanging their data with professionals when needed.

As indicated in Section 2 as well, there exist solutions that complement such requirements but their main focus is concentrated on the security aspects rather than trying to agile and speed up the whole data exchange process. For this reason, in this paper we propose a novel EHR Cloud architecture that allows its users to safely store their healthcare data,and more precisely their Electronic Health Record (EHR) in the Cloud, while giving the possibility to healthcare professionals to gain access to this data when needed, without supplanting the serious security and privacy

Symvoulidis, C., Kiourtis, A., Mavrogiorgou, A. and Kyriazis, D.
Healthcare Provision in the Cloud: An EHR Object Store-based Cloud Used for Emergency.
DOI: 10.5220/0010247004350442
In *Proceedings of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2021) - Volume 5: HEALTHINF*, pages 435-442
ISBN: 978-989-758-490-9

issues that should also be taken under consideration.

The remaining of the paper is constructed as follows. Section 2 provides a description regarding the study of the state of the art in the fields of EHR Storage Cloud and Secure EHR Management in the Cloud. Section 3 provides a detailed description of an emergency scenario where the proposed EHR Cloud architecture can be exploited in its full potential. Section 4 describes the EHR Cloud architecture in detail. Section 5 analyzes the experiments performed in order to evaluate the proposed EHR Cloud. In Section 6, the requirements of an EHR-related Cloud with respect to security and privacy are introduced, along with the way these are fulfilled by the proposed EHR Cloud. Finally, Section 7 concludes the paper.

2 RELATED WORK

This section summarizes the work achieved in the area of EHR Storage Clouds and EHR Management in the Cloud. There exist several storage cloud services solutions for the secure collection of EHRs and healthcare data in general. In (Cai et al., 2017), the authors propose an EHR sharing scheme deployed in the cloud where the owner of the healthcare data can generate EHR ciphertexts, for a user to be able to decrypt them based on transformed ciphertexts from the EHR Cloud.

Moreover, the authors in (Cao et al., 2019) propose a secure cloud-assisted e-Health system, where the medical institutions that generate and own a patient's EHR ensure that only authorized individuals may have access and be able to modify those EHR data, without the involvement of a trusted entity. The latter is achieved with the exploitation of the blockchain technology, providing a tamper-proofing way to operate actions including the exchange of EHRs, since no transaction can be accepted unless documented into the blockchain.

In a relevant manner, in (Seol et al., 2018) a cloud-based EHR model, utilizing Attribute-based access control techniques is proposed. In this research, the main focus is given on securing the transactions between the owner of the EHR and its requestor. All transactions are digitally signed prior to their execution, while partial encryption of the EHRs is performed as well. In addition, in (Joshi et al., 2018), a centralized attribute-based authorization mechanism is introduced. In this study, Attribute Based Encryption is used allowing medical organizations to delegate authority to healthcare providers in accessing EHRs stored in cloud-based systems. Finally, the authors of (Manoj et al., 2017) suggest the use of two encryption methods in a hybrid EHR system, aiming at achieving protection of data privacy and access control upon the health data.

Based on the research work described above, it is made clear that a lot of work has been achieved in the area of secure transaction of EHRs and health data between two or more entities and storage of such data in Cloud-based infrastructures. What can be identified based on the above-mentioned research work it that the attention is mainly focused on the security and privacy risks that arise when the exchange of health data between healthcare organizations. However less attention has been given on how EHR exchange can be achieved between an individual and healthcare organizations, with respect to the efficiency of such systems.

With that in mind, in this paper we introduce a novel EHR Cloud system utilizing the Object Storage architecture (Factor et al., 2005) whose purpose will be two-fold. To give the user the ability to safely store and backup their healthcare data in the Cloud, and allow Healthcare Professionals to gain access to this data if needed in an automated yet secure way, for accelerated health services provision.

3 EMERGENCY SCENARIO

This section describes the scenario that worked as a thriving force in order to design the EHR Cloud architecture which will be described in section 4.

3.1 Preliminaries

In order to better comprehend the scenario it is very important to define the entities that constitute the overall system.

- **Electronic Health Record Application (EHR App):** A smartphone application that is used by the user. Through this application a user is able to access their EHR that is stored locally on the phone and visualized through this application. In addition, using the same application the user uploads their health data (e.g. EHR, Medical Images, etc.) to the EHR Cloud.
- **Healthcare Professional Application (HCP App):** The Healthcare Professional's (HCP) application through which an HCP gains access to the user's health data that is stored in the EHR Cloud. Using the same application, the HCP may also visualize this data, modify it and upload it to the EHR Cloud. The HCP App in the current

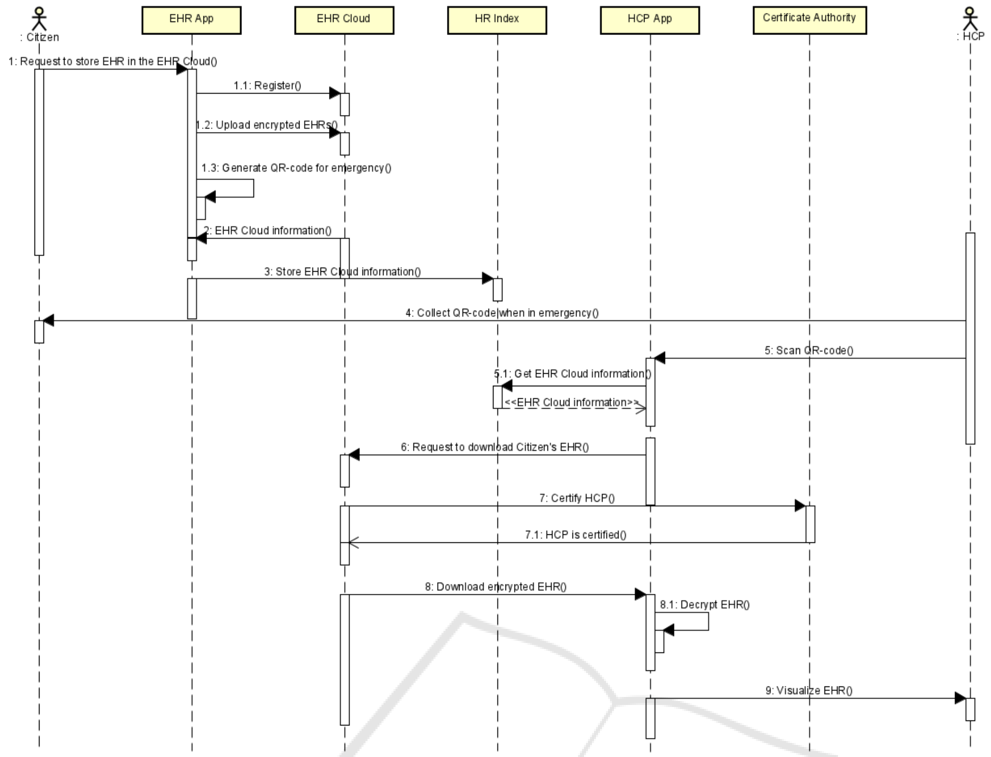
: Citizen
EHR App
EHR Cloud
HR Index
HCP App
Certificate Authority
: HCP
1: Request to store EHR in the EHR Cloud()
1.1: Register()
1.2: Upload encrypted EHRs()
1.3: Generate QR-code for emergency()
2: EHR Cloud information()
3: Store EHR Cloud information()
4: Collect QR-code when in emergency()
5: Scan QR-code()
5.1: Get EHR Cloud information()
<<EHR Cloud information>>
6: Request to download Citizen's EHR()
7: Certify HCP()
7.1: HCP is certified()
8: Download encrypted EHR()
8.1: Decrypt EHR()
9: Visualize EHR()

Figure 1: Emergency scenario.

emergency scenario replicates the system used in Hospitals and other Healthcare institutions.

- **Health Record Index (HRI):** A health record indexing methodology as proposed by (Kiourtis et al., 2020) through which HCPs may access a user's EHR that is stored in a Storage Cloud similar to the proposed EHR Cloud in emergency cases. In cases where several EHR Cloud providers exist, the HRI holds information about each user's preferred EHR Cloud.
- **EHR Cloud:** The proposed EHR Cloud architecture as proposed in Section 4. A user utilizing the EHR App on their phone uploads their health data in the EHR Cloud.
- **Certification Authority:** An entity that can certify an individual as HCP. This is a mandatory entity in order to assure that only certified individuals can gain access to the EHR Cloud in emergency situations.

3.2 Scenario Description

The emergency scenario, also visually depicted in Figure 1, is split into two time periods. The first includes the steps prior to the emergency, while the second starts at the moment the emergency occurs and can be further divided into the following steps.

1. **Pre-emergency:**
   (a) **Upload EHR:** The first step of this emergency regards the upload of the user's EHR to the EHR Cloud, through the EHR App. An important note, is that the EHR is encrypted on the smartphone side prior to its upload to the EHR Cloud.
   (b) **QR-code Creation:** As soon as the upload is complete, a QR-code is created in the smartphone application. This QR-code contains the information needed by the HCP in order to contact the HRI, gain access to the user's EHR that is stored in the EHR Cloud and decrypt the EHR. This QR-code is printed by the user and kept with them at all times.
2. **An Emergency Occurs:**
   (a) **User in Medical Need:** An EHR Cloud user is in need for medical assistance and is transferred to the nearest medical centre.
   (b) **QR-code Scan:** The HCP collects the above-mentioned QR-code from the user and scans it through the HCP application.
   (c) **HRI Mapping:** As mentioned earlier, the QR-code holds information about the citizen. This information is queried to the HRI service which returns the EHR Cloud that the user used to upload their EHR.

(d) **Download EHR Request:** The HCP requests to download the EHR from the user's preferred EHR Cloud. This cannot be achieved unless the HCP is already certified by a Certification Authority.

(e) **HCP Certification:** The HCP provides the EHR Cloud the necessary information in order to certify themselves as HCPs. The EHR Cloud then contacts this service in order to verify the identify of the HCP. If the process of certifying is unsuccessful, the request to grant access to the EHR is aborted.

(f) **Download EHR to the HCP App:** This steps can only happen, when an HCP is in fact certified as HCP. If the HCP is certified, the download of the EHR begins.

(g) **EHR Decryption:** The EHR is now downloaded in the HCP App. Using the above-mentioned information collected from the QR-code the EHR is decrypted and visualized.

4 CLOUD-BASED EHR ARCHITECTURE

This section describes the proposed EHR Cloud architecture. In Figure 2 the proposed EHR Cloud's architecture is presented. There, four main components are identified. The (i) **Object Store** where the users' encrypted EHR are stored, (ii) the **Identity manager** whose purpose is two-fold; to hold information related to the user's account and create temporary accounts for the HCPs in order to access the EHR Cloud. The remaining components of the proposed EHR Cloud are (iii) the **Access Auditing** component that keeps records of who and when accessed the EHR Cloud along with the files that were added, deleted or modified, while (iv) the **HCP Certification checking** mechanism ensures that only someone certified as HCP by a trusted certification authority HCP can access the EHR Cloud in case of an emergency. Note that for simplicity reasons the HR Index and the acknowledgement messages after each action are not shown in Figure 2.

4.1 The Object Store

The primary component of the proposed architecture is the **Object Store** where the users' EHRs are kept. The implemented EHR Cloud solution exploits MinIO (MinIO Inc., 2020), a high performance object storage developed especially for building cloud-native applications and service, as the EHR Cloud. Not only that, an object storage is preferred, instead of a NoSQL-based architecture that is commonly used for similar projects (Sreekanth et al., 2015) for the following reasons:

- The files stored in an object storage are by definition as objects. These objects contain the data along with its metadata and a unique identifier, thus making object stores highly customizable and powerful.
- Object stores can be deployed in commodity, less expensive hardware making them easier and less costly to manage and upgrade.
- Scalability is relatively easy to accomplish as well, something crucial for systems that require efficiency and low response time, as the proposed EHR Cloud.
- Object stores also ensure high availability for the stored data. For this reason, storing unstructured data, photos and videos (e.g. Medical Images, etc.) regard an optimal use case for using Object stores.

The objects (i.e. the user's EHR) stored in the EHR Cloud are encrypted prior their upload to the EHR Cloud on the phone side. This policy is set in order to ensure that even if in the worst-case scenario where an unauthorized entity manages to access the EHR Cloud, they will not be able to gain access to the health record itself.

4.2 The Identity Manager

The **Identity Manager** is another crucial component of the proposed architecture, since it is responsible for the account management of the users of the EHR Cloud. When a user is registered their information is stored in the Identity manager. Keycloak (Keycloak, 2020) is used as the Identity manager, an Identity and Access management service which is integrated with the MinIO object store. The Identity Manager is also responsible for providing a temporary account to an HCP during an emergency, in order to access the user's EHR. The policy under which the temporary account is created allows the HCP to only download the objects that are stored to the EHR Cloud, but cannot modify them.

The HCP has the ability to add new information to the EHR of the user, but these additions are kept in a separate bucket in the EHR Cloud. The content added by the HCP is only merged with the user's EHR after the user reviews and accepts it.

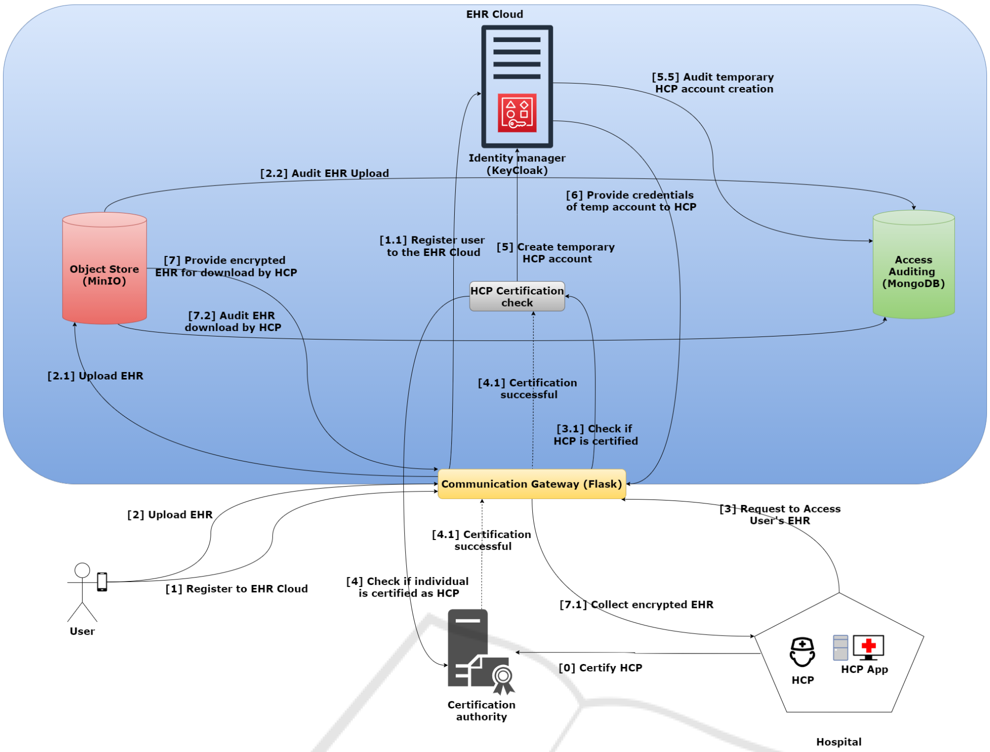
EHR Cloud
Identity manager (KeyCloak)
[5.5] Audit temporary HCP account creation
[2.2] Audit EHR Upload
[6] Provide credentials of temp account to HCP
[1.1] Register user to the EHR Cloud
[5] Create temporary HCP account
Object Store (MinIO)
[7] Provide encrypted EHR for download by HCP
Access Auditing (MongoDB)
HCP Certification check
[7.2] Audit EHR download by HCP
[2.1] Upload EHR
[4.1] Certification successful
[3.1] Check if HCP is certified
Communication Gateway (Flask)
[2] Upload EHR
[3] Request to Access User's EHR
[4.1] Certification successful
[1] Register to EHR Cloud
[4] Check if individual is certified as HCP
[7.1] Collect encrypted EHR
User
[0] Certify HCP
HCP
HCP App
Certification authority
Hospital

Figure 2: EHR Cloud architecture.

4.3 The HCP Certification Checker

The **HCP Certification checker** mechanism regards a service that is only triggered in emergency situations and specifically when an HCP requests access to the EHR Cloud. In order to ensure that the individuals that are certified as HCPs (doctors, nurses, etc.), this component requests from the HCP the provision of the credentials that can be used to verify their occupation from a trusted authentication authority. As soon as these credentials are received, the HCP certification checker verifies that the individual is indeed an HCP and the access to the EHR Cloud is granted.

4.4 The Auditing Mechanism

Finally, the **Access Auditing** component is a MongoDB (MongoDB Inc., 2020) database that keeps logs of all actions performed in an EHR by the user themselves or an HCP during an emergency. In more detail, what is stored in the Auditing component has to do with the registration of the user, the time that content is uploaded to the EHR Cloud, and changes that are made to the EHR by the user. In addition, logs concerning the HCPs that access the EHR Cloud are also kept, including the list of the EHR data objects they download, and the list of the healthcare data created during an emergency that are uploaded to the EHR Cloud.

4.5 Communication Gateway

For the communication between the users and the healthcare professionals with the EHR Cloud a gateway is implemented, using Flask (The Pallet Projects, 2020). This gateway implements the functionalities that a user (either an individual or an HCP during an emergency) may perform on the EHR Cloud.

These functionalities can be split into two main categories: the functionalities performed by a user of the EHR Cloud and the functionalities performed by an HCP during or after an emergency. Regarding the user, using this gateway they may register, login to and deactivate their account from the EHR Cloud. In addition they may use it to upload, download and update their EHR to the EHR Cloud. Regarding the HCP, they may request access to an EHR stored in the EHR Cloud, as well as upload new content once the emergency is over.

5 EVALUATION OUTCOMES

This section describes the preliminary tests executed while deploying the above-mentioned architecture.

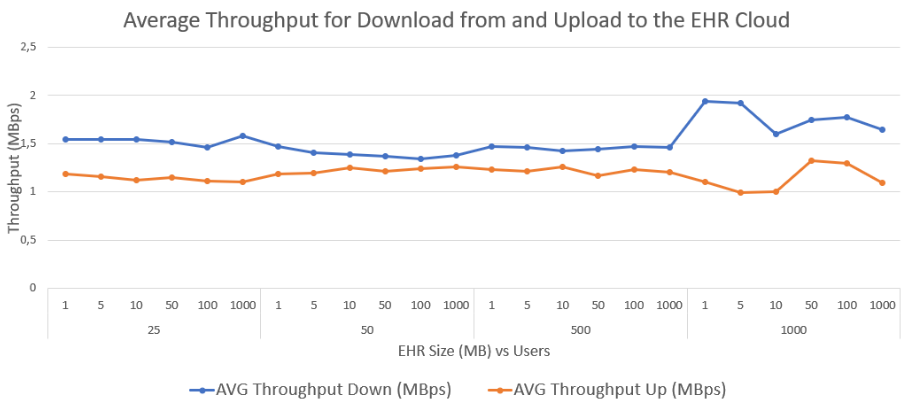

Figure 3: Average Throughput (download/upload) of the EHR Cloud.

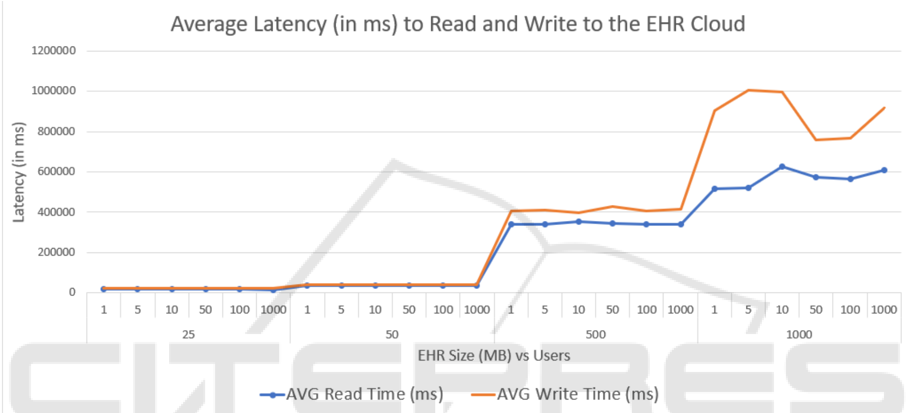

Figure 4: Average latency (in ms) to perform read / write operations to the EHR Cloud.

5.1 Evaluation Environment

In order to evaluate the proposed EHR Cloud, a setup that consists of 3 Virtual Machines (VM) is created. Each VM is comprised of 4 vCPU cores, 32GB of memory and 1TB of storage and static IPs. All VMs run CentOS 7 and have Docker installed. In each VM a containerized application is deployed. More precisely, on the first VM a MinIO container along with a containerized Flask service that handles all incoming requests is deployed. In the second VM, runs the KeyCloak container along with the containerized HCP certification checker service, while in the third VM runs the MongoDB Auditing service.

5.2 Results

This section describes the results that were derived after completing the experimental evaluation over the deployed EHR Cloud.

For this evaluation the main testing point was the performance of the deployed system with respect to the latency in order to perform Read / Write operations taking under consideration also the file size. It is particularly important to be able to download EHR content fast, especially large files (i.e. medical images), from the Cloud especially when in emergency, since in such cases even a few seconds can make a difference.

For the evaluation of the deployed EHR Cloud several use cases where designed each one with different numbers of simultaneous users and file sizes. More precisely, we tested the behavior of the EHR Cloud for 1, 5, 10, and 50 simultaneous users and simulated the behavior for 100 and 1000 simultaneous users that perform either Read or Write operations in order to measure how the number of the users impact on the performance of the EHR Cloud. The size of the files that were used were either 25, 50, 500 or 1000 MB.

Figures 3 and 4 present the results after running experiments on the deployed EHR Cloud. In these experiments the upload and download of EHR was simulated with files of different sizes in order to observe the behaviour of the deployed system. As seen in Figure 4 the latency for the execution of Read / Write operation to the EHR Cloud is irrelevant to the number of simultaneous users, when this is number is

Table 1: Average Throughput (MBps) (Up/Down) with respect to simultaneous users and encrypted EHR size (MB).

		EHR Size (MB)							
		25	**50**	**500**	**1000**	**25**	**50**	**500**	**100**
		Throughput Down (MBps)				**Throughput Up (MBps)**			
Users	**1**	1.558	1.470	1.470	1.919	1.190	1.190	1.234	1.104
	5	1.543	1.408	1.466	1.937	1.162	1.196	1.213	0.995
	10	1.548	1.399	1.424	1.921	1.126	1.254	1.264	1.002
	50	1.515	1.370	1.445	1.601	1.146	1.212	1.166	1.322
	100	1.462	1.355	1.470	1.745	1.116	1.244	1.231	1.301
	1000	1.582	1.336	1.466	1.773	1.100	1.257	1.205	1.092

low. This number of the other side increases when the number of simultaneous users increases. But given the fact that the current infrastructure did not have the ability to scale the system, the results show no issues regarding the functionality of the Cloud.

Figure 3 on the other side depicts the throughput when performing the experiments that are described previously. No significant changes on the throughput can be observed. More detailed information are depicted in Table 1.

6 DISCUSSION

The evaluation outcomes which are presented in section 5 shows that the deployed EHR Cloud's performance is not affected by the number of the users that are using it simultaneously or by the different-sized data that is uploaded. In addition, no service failures were identified during the tests that were executed. These results however, are related solely to the performance of the service and not to the security requirements that should be met by an EHR storing cloud-based service.

As described in the previous sections the main purpose of the proposed EHR Cloud architecture is to automate and accelerate the EHR exchange during emergency situations. Regardless, the privacy and security risks should not be undermined. For this reason, in this section the requirements that every EHR Cloud should meet, as identified by (Chen et al., 2012) are presented, in combination with how those requirements are addressed in the proposed EHR Cloud. An important note is that the analysis of these requirements was done prior to the design of the proposed EHR Cloud architecture.

- **Ownership of Information:** In the proposed EHR Cloud architecture the owner and managing entity of an EHR is the user (i.e. the patient). Therefore, any changes performed by HCPs on the content stored in the EHR Cloud must be approved by the owner. As mentioned earlier, new EHR content created by HCPs is uploaded in the Cloud and stored in a separate bucket and only if the user approves this content, is it then permanently moved to the main bucket.
- **Authenticity and Authentication:** Only authenticated HCPs can access the content of the EHR Cloud. An HCP should be authenticated by a trusted Authentication authority before requesting access to the EHR Cloud.
- **Non-repudiation:** Non-repudiation is achieved in the proposed EHR Cloud architecture, since only digitally signed transactions and modifications on the content stored in the EHR Cloud are allowed.
- **Patient Consent and Authorization:** In the proposed EHR Cloud two consents are accepted by the user. The first one regards the use of the EHR Cloud as a backup service where the user's healthcare data is stored in the EHR Cloud. The second one regards the authorization to the EHR Cloud provider to authorize authenticated HCPs to access the user's EHR when an emergency occurs. If the second consent is not accepted the user may use the EHR Cloud solely as a Storage Cloud service. In addition both consents are digitally signed by both parties (i.e. the user and the EHR Cloud provider).
- **Availability:** High availability is crucial to Cloud systems, especially when concerning emergency situations. The system should be available at all times, even when power outages, hardware failures or denial-of-service attacks are made. During the evaluation we put the EHR Cloud under, no timeouts or failures were identified, thus leading to the conclusion that the 99.9% availability requirement was met. Of course, additional measures should be taken when in production in order to meet this requirement.
- **Data Integrity and Confidentiality:** Confidentiality and data integrity is achieved through the encryption of the healthcare data before its upload the EHR Cloud.
- **Auditing:** A component dedicated to recording

any transactions and every access in the content stored in the EHR Cloud is included in the proposed architecture in order to ensure that auditing is done properly.

7 CONCLUSIONS

This paper proposed a Cloud-based EHR approach used for safely storing EHRs in the Cloud, while authorizing healthcare professionals to have access to this content when an emergency situation occurs. The proposed architecture automates the procedure of authentication and access to the EHR Cloud, thus accelerating the process of healthcare services provision. In order to evaluate the performance of the proposed EHR Cloud, experiments were executed and the preliminary results are presented. In addition, the requirements that every EHR Cloud should meet are presented, along with the way those are addressed in the proposed architecture.

It is within our future goals to perform additional evaluation to the proposed EHR Cloud-based approach. Moreover, we plan on researching on the integration of the edge cloud to the current architecture in order to reduce latency issues that may arise.

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

Cai, Z., Yan, H., Li, P., Huang, Z.-a., and Gao, C. (2017). Towards secure and flexible ehr sharing in mobile health cloud under static assumptions. *Cluster Computing*, 20(3):2415–2422.

Cao, S., Zhang, G., Liu, P., Zhang, X., and Neri, F. (2019). Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain. *Information Sciences*, 485:427–440.

Chen, Y.-Y., Lu, J.-C., and Jan, J.-K. (2012). A secure ehr system based on hybrid clouds. *Journal of Medical Systems*, 36(5):3375–3384.

Cohen, J. K. (2018). Report: Healthcare industry leads in cloud adoption. The healthcare industry is the furthest along in cloud adoption, compared to the financial services industry and the energy and utilities industry, according to a West Monroe Partners report. https://www.beckershospitalreview.com/healthcare-information-technology/report-healthcare-industry-leads-in-cloud-adoption.html. Last checked on Sep 23, 2020.

Davenport, T. and Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future healthcare journal*, 6(2):94.

Factor, M., Meth, K., Naor, D., Rodeh, O., and Satran, J. (2005). Object storage: The future building block for storage systems. In *2005 IEEE International Symposium on Mass Storage Systems and Technology*, pages 119–123. IEEE.

Joshi, M., Joshi, K., and Finin, T. (2018). Attribute based encryption for secure access to cloud based ehr systems. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 932–935. IEEE.

Keycloak (2020). Keycloak. https://www.keycloak.org/. Last checked on Sep 15, 2020.

Kiourtis, A., Mavrogiorgou, A., Vidakis, K., and Kyriazis, D. (2020). Health record index: Secure access of cloud-stored healthcare data. *Studies in Health Technology and Informatics*, 272:221–224.

Manoj, R., Alsadoon, A., Prasad, P. W. C., Costadopoulos, N., and Ali, S. (2017). Hybrid secure and scalable electronic health record sharing in hybrid cloud. In *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pages 185–190.

Martin, N. (2019). How healthcare is using big data and ai to cure disease. https://www.forbes.com/sites/nicolemartin1/2019/08/30/how-healthcare-is-using-big-data-and-ai-to-cure-disease/#17e97ef45cfc. Last checked on Sep 15, 2020.

MinIO Inc. (2020). High performance, kubernetes native object storage. https://min.io/. Last checked on Sep 15, 2020.

MongoDB Inc. (2020). The most popular database for modern apps — mongodb. https://www.mongodb.com/. Last checked on Sep 15, 2020.

Seol, K., Kim, Y., Lee, E., Seo, Y., and Baik, D. (2018). Privacy-preserving attribute-based access control model for xml-based electronic health record system. *IEEE Access*, 6:9114–9128.

Sreekanth, R., Rao, G. V. M., and Nanduri, S. (2015). Big data electronic health records data management and analysis on cloud with mongodb: A nosql database. *International Journal of Advanced Engineering and Global Technology*, 3(7):943–949.

The Pallet Projects (2020). Flask | The Pallets Projects. https://palletsprojects.com/p/flask/. Last checked on Sep 15, 2020.

Vinati Kamani, A. (2019). 5 ways cloud computing is impacting healthcare. https://www.healthitoutcomes.com/doc/ways-cloud-computing-is-impacting-healthcare-0001. Last checked on Sep 15, 2020.