National College of Ireland

Improving Security and Data Privacy of eHealth Application in the Cloud Using Federated and device-based authentication

MSc Research Project
Cyber Security

Oluseye Jerome Arinde
Student ID: X20121598

School of Computing
National College of Ireland

Supervisor: Rohith Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Oluseye Jerome Arinde
Student ID:	X20121598
Programme	Cybersecurity **Year:** 2021/2022
Module:	Internship
Supervisor:	Rohith Verma
Submission Due Date:	……
Project Title:	IMPROVING SECURITY AND DATA PRIVACY OF eHEALTH APPLICATION IN THE CLOUD USING FEDERATED AND DEVICE-BASED AUTHENTICATION.
Word Count:	5279…… **Page Count 20**……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Oluseye Jerome Arinde
Date:	9/19/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Improving Security and Data Privacy of eHealth Application in the Cloud Using Federated and device-based authentication

Oluseye Jerome Arinde
X20121598

Abstract

With the increase in patient influx and burdened health care system, healthcare providers architecting their infrastructure in cloud and faced with the big challenge of security of patient data as well as the privacy of this records, requires a well secured and architected infrastructure in the cloud to both handle capacity and the requirement of security.

This research implemented a federated authentication with device-based authentication using protocols such as Active directory federated services and oauth2 to design a highly secured authentication infrastructure, to improve the security and privacy of an eHealth application. The focus of this study is to build a well architected framework, that is not overly complicated to adopt in other to combat known cloud infrastructure and application vulnerabilities that might lead to breach in patient data

Keywords: Cloud Security, Federated Authentication, Privacy, Device-based Authentication, IdP, Service Providers, and Oauth2

1 Introduction

1.1 Background of study: eHealth is recently rated with great potential to improve health care management, especially in health records management. (Mamun and Rana, 2017)

There has been several studies and researches that buttresses around architecting a secured eHealth solution in the cloud (Thilakanathan et al., 2014) in their study suggested the cloud as the popular alternative for the analysis of health data; and they proposed a methodology that allows patients to authorize every access to their health data by doctors by clicking share in eHealth application for access to be granted to their health data.

Implementing security of an eHealth application in the cloud brings a lot of concerns about the following:

- Security of stored health records in the cloud
- Security in model adopted to share health records
- Privilege access management, and access revocation

The requirement of study in ensuring security and privacy of health record birth the creation of frameworks such as the ASCLEPIOS this is to tackle the numerous concerns on data privacy which is the pain point of architecting an eHealth solution in the cloud. (Reis et al., 2021).

This study adopts the NIST identity standards especially in federated authentication. NIST approach recognizes the establishment of trusts between an Identity provider and a service provider to use trusted tokens that supports biometrics and secret key-based authentication. (Garcia, 2017)

1.2 Justification of Study:

Architecting an eHealth-based application has transitioned from the on-premise infrastructure to the cloud, and this has been the new shift since the increase in demands for health services especially during the global pandemic.

Health care services was overwhelmed by the massive number of covid patients among other illness such as diabetics, heart problems, blood sugar issues and cancers. This reflect in the data collected by the European Centre for Disease Prevention and control (ECDC), that was analyzed in the later section of this research. (ECDC, 2022)

To handle this increase, and filter the number of people that actually need to be in the hospital; healthcare organizations innovate better approach to patient management including managing patients remotely, going paper-less and migrating eHealth applications to the cloud. These has reduced stress on the already burdened health facilities as well reduced the risk of patient exposure to viral diseases.

1.3 Research problems

This study identifies the following research problems:

- The security of eHealth cloud-based application newly architected in the cloud or migrated to the cloud.
- Risk of health data privacy and the consequences it might have on patients (Data subjects)
- Authentication problems which is the entry point of breaches or attacks to the security of data is saved in the cloud.

1.4 Research Question

This research will answer the following research questions

- How can an eHealth application be securely architected in the cloud
- How can a federated authentication solution improve security of cloud-based eHealth application
- How does the secure architected solution contribute to the privacy of patient records in the cloud.

2 Related Works

There are related studies and researches that have critically crafted algorithms that tackles security and privacy issues, bulk of which proposed solutions for cloud records at rest and in transit, with encryption, and key management largely discussed. This research takes a different angle at looking at authentication, as this is a big part to be considered if any cloud-based health application will be compromised.

2.1 Adopting Cloud for eHealth Applications

Software Solutions are recently architected in the cloud, which has been a paradigm or a shift from the traditional ways of deploying on-premises. According to (Mehrtak et al., 2021) cloud computing delivers services, applications and tools storage, database, compute, networking and security to support telemedicine, IoT, electronic health to mention just a few. He further stated that cloud takes precedence over traditional deployment on-premises.

There are a lot of cloud providers which also provide federated identity solutions. Such companies include but not limited to Amazon, Google, Facebook, IBM, Yahoo and so on. (Liang et al., 2009)

In a survey carried out in (Chalker et al., 2020) adopting the cloud helps organizations, to be able to get better control on their investment in infrastructure and help them save, among other benefits of scalability, accessibility, efficiency.

NIST describes the underlisted cloud models as it might applies to solutions architected in the cloud (Jared et al., 2012):

- Infrastructure as a Service (IaaS): an example entails deploying a computing resource such as Virtual Machine (VM) or the network. This breaks the barrier of purchasing hardware
- Software as a Service (SaaS): Some eHealth applications are offered as software as a service. This model leverage on the internet, and the consumer of this resource, need not to provision any virtual machine or install any application. They usually just subscribe to a SaaS to service for patient management. (Jared et al., 2012)
- Platform as a Service (PaaS): This model is less popular especially with eHealth solutions. It entails abstraction of platforms for specific services such as database for example. (Jared et al., 2012)

2.2 Risk of adopting the Cloud for eHealth Applications

The associated risks and concerns of migrating an eHealth application to the cloud cannot be over emphasized. Rodrigues et al (Rodrigues et al., 2013) stated a list of requirements to be considered before migrating health applications and its associated data to the cloud. Top of the concerns here are confidentiality of records, patient's consent in record use, as well as the legality of data access.

Regarding health records, the General Data Protection Regulation **GDPR** states the responsibilities and the legal bases of health managers in processing health data of subjects. The data controllers and processors in the health sector are legally liable to process data of subjects in emergency situations, or for the purpose of medical diagnosis, and in the interest of the data subject. (HSE, 2018)

Table 1 below shows attack classification based on Cloud architected eHealth system

Attacks on perception layer	Attacks that taget network layer	Attack that target application layer
•Tampering of devices •Side channel attack •Tag cloning •Sensor tracking •Insertion of forged nodes	•Denial of Service (DOS) •Distributed Denial of Service (DDOS) •Rogue access •Eavesdropping •Man in the Middle attack (MITM) •Sybil Attack •Sniffing Attack •Routing attacks	•Session hijacking •Cross-site scripting (XSS) •Cross-Site request forgery (CSRF) •SQL injection •Brute Force attack •Ransomware •Buffer Overflow •Phishing Attack

Table 1: Cloud attack surfaces and threats

Building an ideal electronic records system usually attracts tradeoffs between flexibility and security. Health records is highly regarded in GDPR and HIPAA regulatory requirements of securing personal data, while the cloud offers a great deal of flexibility, breach in patient confidentiality poses a great threat to health care manager, hospitals and any institutions that may hitherto be referred to as health data controllers or processors. (Yoon et al., 2020)

2.3 Cloud Authentication models and Security

In recent researches and implementations, there are has been several attempts to improve security and privacy of health records in the cloud. Deebak and Al-Turjman (Deebak and Al-Turjman, 2021) in their literature developed an SSA framework; known as Smart Service Authentication so as to verify common secret session keys, which is key among communication parties such as identity providers and service providers for example. This framework employs deeps mathematical processes only to proof its efficiency against threats

2.4 Securing Electronic Health records in Cloud.

Encryption is a major consideration to secure data at rest in the cloud. Access control and distinct encryption parameters will contribute to integrity and confidentiality of patient records. Effective key management that factors turnaround time in retrieval and access to records. (Alabdulatif et al., 2013). In implementation, this study took advantage of the java security libraries for preliminary authentication and bloom filters were used to search out hash values which are generated and stored in the database. This research shows the need to further implement access control model for the electronic health records, as its lacking in its design. The approach also poses performance concerns and intensive computing requirement.

2.5 Anonymization of health records in the cloud.

As stated earlier, achieving data privacy of health records requires maintaining anonymity of this records. According to (Jusak et al., 2022) an anonymization algorithm was employed to achieve the confidentiality of patient records. In his literature, the percentage residual difference was the methodology used, together with brute force and performance comparison.

Securing medical health records requires both cryptographic and non-cryptographic technique or methods (Jusak et al., 2022). As there's no single approach to security, achieving our objective of securing health data in the cloud requires a conglomerate of methods and systems. This means that, records are secured end to end all through its life cycle. That is, at the record creation, while the record is kept, while the record is in use and when the records are no longer in use. The weakness in this approach is the lacking of key management repository for storage and distribution of keys.

2.5.1 Achieving Anonymization with Federated and device-based authentication

Many web-based and mobile applications heavily rely on traditional password model for authentication; Papadamou et al (Papadamou et al., 2020) this study stresses the absence of attribute-based authentication in the traditional password model in allowing anonymity in access to cloud services.

One of the main concerns of achieving anonymization is the act of building cryptographic system that achieves state of art security without excessive use of computing resource. The goal of security is forfeited when cost of implementing security is invariably too high, and much more that the value of data it's meant to secure. This is why Yi Liu et al (Liu et al., 2018) in his literature proposed a fine grained access control approach in securing health data in mobile cloud computing by generating an offline cyphertext prior to knowing the electronic health data and access policies, that is responsible for computing overload.

Also, the European Commission's Horizon 2020 Research and Innovation supported the INCOGNITO project which is an acronym derived from the word "**IdeNtity verifiCatiOn with privacy-preservinG credeNtIals for anonymous access To Online services**" the project owner and author Vaios et al (Vaios and Nikos, 2019) in their research specifies the technique in achieving anonymous credential with federated entities; in achieving authentication and

authorization. This is achieved with a device-based authentication with solutions using federated authentication protocol with the FIDO2 protocol alongside with implementations such as the Keycloak. In their research Vaios et al (Vaios and Nikos, 2019) stated the use of tokens and certificates that ties to user attributes as a proof of identity to carry out designated tasks on secured cloud infrastructure that keeps patient's sensitive data.

The algorithm in use by the INGOGNITO project mitigates replay attacks and mitigates the likelihood of stolen or tampering of user credentials, as they are saved cryptographically on user devices and only accessible using a "user-to-device authentication protocol" like FIDO2. These credentials are encrypted in case of device loss or theft

This thesis will complement the INCOGNITO project by implementing active directory federations with device based multifactor authentication, before the authentication requests are made to the service provider through the identity provider like Facebook, Google and so on.

Though key management is lacking in the algorithm proposed by Jusak et al. This project will not buttress on encryption and key management as several researches has covered these areas as far as implementing privacy is concerned.

3 Methodology

After several reviews of literatures and past works on subjects of cloud security and authentication, data privacy, with peculiarity to eHealth applications, cloud infrastructure security and best practices. This research adopts the methodology of using federated authentication protocols and services in authenticating securely into eHealth secured network. It uses the Active directory federation service (AD FS) which extends the abilities of a single-sign authentication for security and privacy of interactions with internet facing eHealth applications. (billmath, 2021)

The model proposed by Papadamou (Papadamou et al., 2020) takes the burden of password management, which makes users susceptible to brute force attacks, replay attacks, SQL injection, eavesdropping, shoulder surfing to mention just a few; which is similar to the method adopted by Vaios and Nikos in the INCOGNITO project (Vaios and Nikos, 2019) and proposes a device-centric authentication.

The proposed method incorporating AD FS with IdP isn't common with eHealth applications; though some attempts has been made to adopt a portion of this in highly secured infrastructures, this method may be considered for highly sensitive environments especially where records in databases classified or highly sensitive.

3.1 Identity Management for eHealth Application

The concept of identity management became a necessity as there are disjointed platforms requesting for the same user credentials and authentication attributes. Social networks have seen substantial growth over the years, and has taken the responsibility to manage identities of users. According to (Ferdous et al., 2020) entities are formally recognized with digital identities which employs the use of an identity management system (IMS) to aid or transacts with parties such as:

- **Users:** This can be doctors, patient appointment scheduling agents, nurses, lab scientist, Health insurance administrators and other health management officers that needs to authenticate to an eHealth application
- **Service Providers:** This can be a hospital, clinic or health management organizations that provides services to individuals, and owns an eHealth application that requires authentication from health managers, that interacts with the system for the purpose of managing health related cases, of individuals and members of the public
- **Identity Provider:** They are also known as the IdP; they provide the technology for the storing and administration of digital identities of users and subscribers that uses the services of a service provider. (Ferdous et al., 2020)

Federated Identity Management (FIM): This is based on the idea of identity federation, meaning an aggregation of identities from trusted domain to access one hosted resource or another. (Ferdous et al., 2020) This requirement legal bindings between IdP and Service providers to facilitate the access of their users to this hosted resource, in ease and state of art security in mind. Here there are exchange of attributes between this providers as agreed and allowed by the users under the requirements to respect data privacy (GDPR, 2019)

One of the major challenges to the confidentiality of records is the poor management of identity. One of the suggested requirement in improving security according to (Thilakarathne,

2020) is the identification of users and the devices used to authenticate into eHealth applications. This entails state of the art user management and enrollment of devices.

3.2 Protocols and standards

Achieving Single-Sign-On simplifies authentication in an eHealth application, which might require integrations of different services, endpoints, and APIs in meeting with the requirement of servicing patients. To achieve Sing-Sign-On in a federated identity scenario, OpenID connect and OAuth 2.0 are commonly used. (Gonçalves et al., 2022)

OAuth 2.0: It's an authorization framework identified in the RFC6749 it retires its predecessor OAuth 1.0 with the sole objective to allow or authorize third-party access to highly protected application (Dodanduwa and Kaluthanthri, 2018)

OpenID Connect: One major difference in this protocol and OAuth 2.0 is the fact that the entity that authorizes to secured resource must be human. This is due to the requirement introduced by the identity layer, which transfers user details through JasonWeb tokens (JWT)

Health organizations globally has implemented diverse requirements in meeting their obligations in maintaining state of the art security and privacy of patient records. Rodrigues in his literature cited an example of the United States of America in her implementation of the HIPAA regulations, as a bench mark for all health institutions and relative service providers in the US (Rodrigues et al., 2013).

In Ireland the Health Services Executives HSE is responsible for health data privacy. (eHealth Ireland, 2020). In a bid to digitize health records, improve patient management, and cater for the already burdened health system, most health care providers and institutions have migrated their health applications to the cloud, with much obligation to meet capacity and legal requirement; and its implication should there be a leakage or breach; not neglecting their primary duty of managing patents.

A method was adopted to create a common interface for major cloud providers to break the barrier of interoperability and vendor dependence in easy migration of eHealth application from one cloud provider to another, without compromising on collective security baseline as

required by regulation and implemented by all cloud providers that are party to the hybrid cloud integrations. (Bahrami and Singhal, 2015).

Much work has already been done in encryption and anonymity of records, in solving the problem of security and data privacy, but this research will be focusing more on authentication, as it is assumed that, the first point of compromising a system is the application authentication system.

This research combines the advantage of federated identity with token-based multifactor authentication to step up security and privacy of patient records in a cloud hosted eHealth application

4 Design Specification

The diagram below shows the proposed architecture showing the accessibility to an eHealth application.

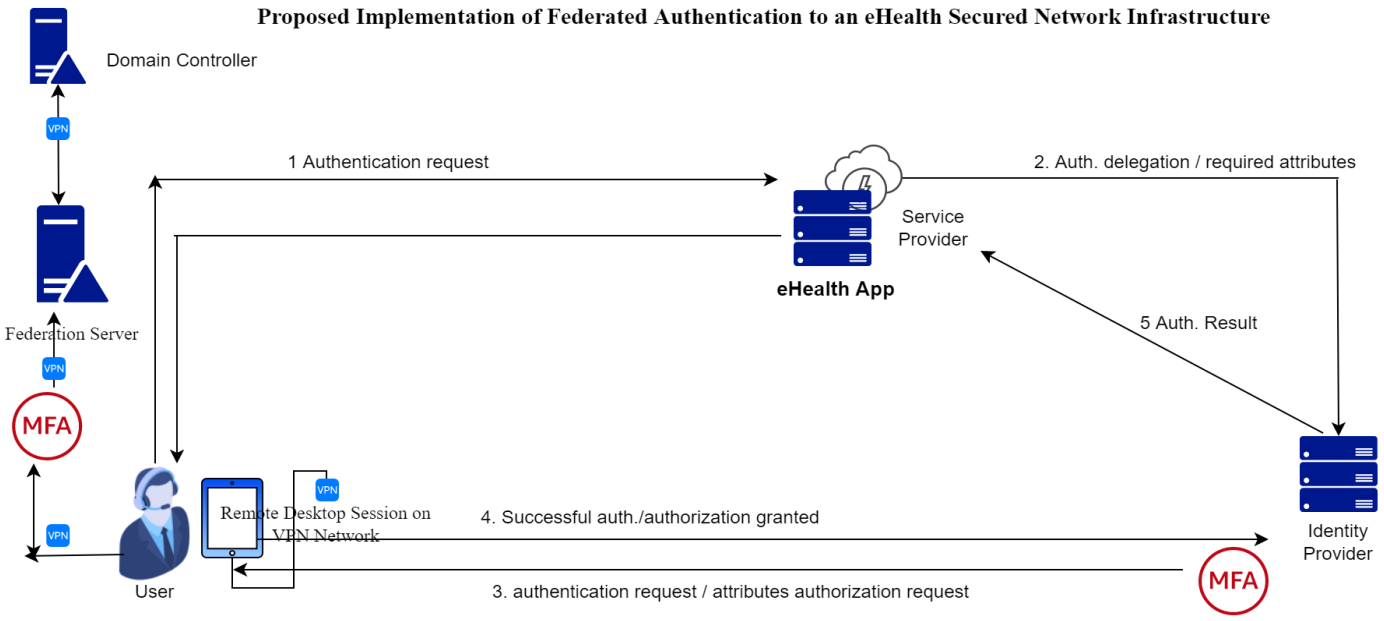

Figure 1 above depicting the proposed methodology in achieving a highly secured authentication system is described in the bulleted workflow below:

- Users are created in an active directory domain-controlled environment
- User roles are defined and pushed with the Active directory group policies
- Federated Services are provisioned from a federated server connected by VPN to the Active Directory
- Remote desktops are created and deployed on a VPN. Users authenticated to their local machines are signed into the Active directory and requested to authenticate to the Federated server using a device-based multi-factor authenticator (MFA) services that can be used for MFA include DUO, Keycloak, Google authenticator, F5 etc

Procedure to access the eHealth application

- On the VPN, Users makes a authentication request to the eHealth
- Users are directed to the IdP (like Facebook) to authenticate
- IdP request for MFA authentication
- IdP authenticates users to the eHealth Application (SP)
- Timeout sessions between authenticated remote desktops (on VPN) and the eHealth requires MFA to continue
- All devices and applications are managed devices that allows remote wipe incase of theft
- All devices are secured with endpoint protection with malware behavioral monitoring detections
- All servers and cloud networks plug into cloud security solutions that implements apt security baselines and regulatory recommendations. Products like trend micro's CloudOne can perform this function as well as other similar vendor products like Rapid 7.

This approach in security built around authentication will combat brute force attacks, replay attacks and SQL injection attacks.

5 Implementation

Data is collected on the ECDC portal for analysis to validate the variance in hospital visits between the years, 2020, 2021 and 2022. This was analyzed using the Jupiter notebook and excel worksheet to establish the claims of rapid change in hospital visits using Ireland as a case study.

The federated identity solution is implemented with Facebook as the IdP, and Microsoft providing hosting for the authentication app, Active directory, and federation services (AD FS)

The Python programming Language is used both for the development of a federated authentication service (Using Django Framework) and for the analysis of the records of hospital visits between year 2020, 2021 and 2022. The App is deployed on Azure with TLS certificates provisioned.

Django framework is highly secure and proven to be secured against known threats and vulnerabilities such as the Cross site scripting (XSS), Cross site request forgery (CSRF), SQL injection protection, session security, Clickjacking protection, SSL/HTTPS protection and other web security modules and frameworks as required in the published by OWASP top 10. (Django official, 2022)

Demo

Below is the authentication workflow

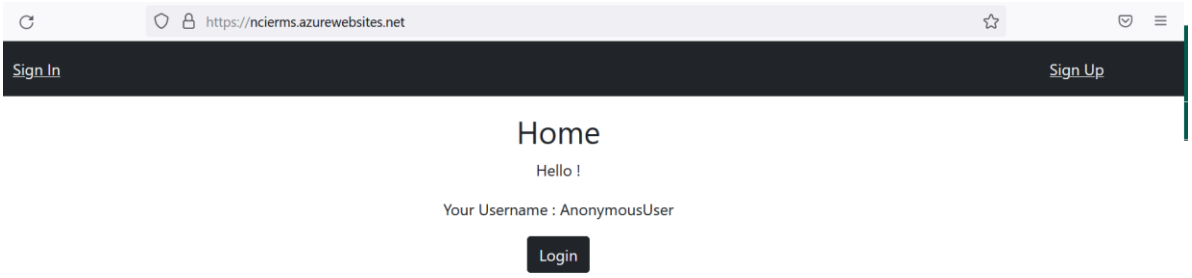

Figure 2: eHealth app Authentication page

The user is presented with the login screen. Prior to this, the healthcare cloud security Administrator will have created an active directory user credentials and applies the required privileges to the user. The Active directory federation service (ADFS) is used here to integrate active directory with the IdP in this instance “FACEBOOK”

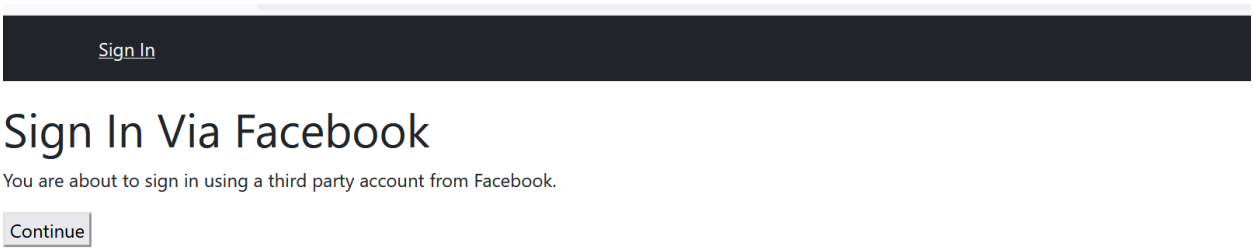

Figure 3: Landing page for the Facebook API

User click on "*sign in with Facebook*" as depicted in figure 3 above

User is presented with the Facebook login page as depicted in Figure 4 below.

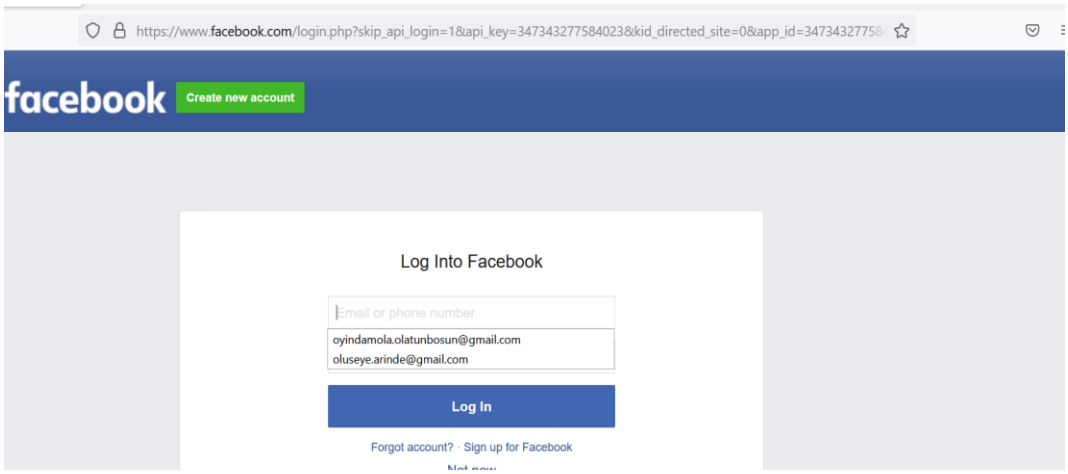

Figure 4: Facebook federated login page

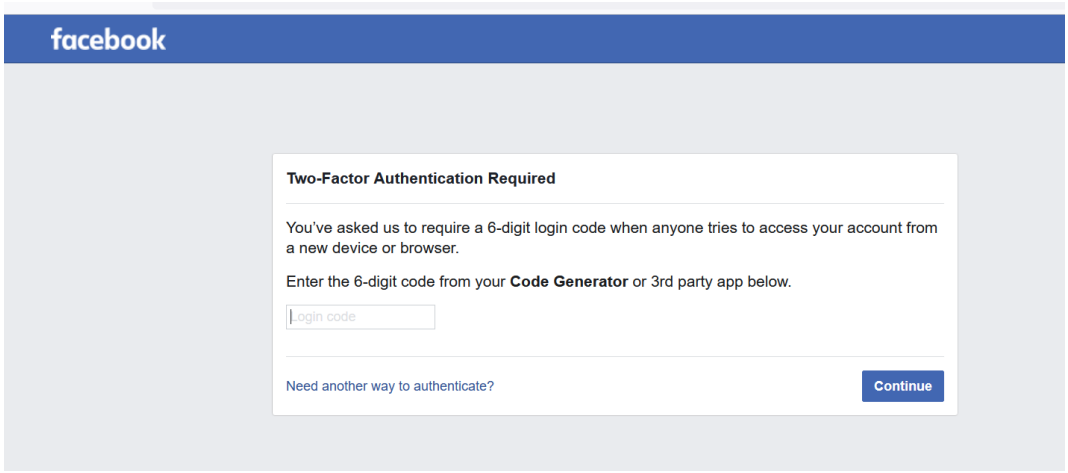

Figure 5: device based multifactor authentication request page

Multifactor authenticator page is displayed and a device authenticator is used to authorize the device trying to authenticate into the idP.

As the token is entered the VPN user is redirected to the eHealth application landing page. Here a trust is established between the User device and the hosted eHealth application.

6 Discussion

6.1 Evaluation

To test the vulnerability of the architected solution and infrastructure; the vulnerability assessment, tools used are the OWASP ZAP, Nessus and NMAP this scan was done both for the local app and remote application after deployment to Azure Cloud.

Below are the results.

OWASP ZAP Scanning report

Sites: https://ncierms.azurewebsites.net

Generated on Mon, 8 Aug 2022 11:59:30

Risk Level	Number of Alerts
High	0
Medium	0
Low	2
Informational	0
False Positives	0

Table 2: Risk level of artifact

Alerts

Name	Risk Level	Number of Instances
Cookie No HttpOnly Flag	Low	8
Cookie without SameSite Attribute	Low	15

Table 3: Low vulnerability alerts suggestions

Below is NMAP Scan Summary

Nmap 7.40 was initiated at Mon Aug 8 11:58:59 2022 with these arguments:

nmap -v -oX=- --host-timeout=28800s -Pn -T4 -sT --webxml --max-retries=1 --open -p0-65355 ncierms.azurewebsites.net

20.118.48.0 / ncierms.azurewebsites.net
Address
20.118.48.0 (ipv4)
Hostnames
ncierms.azurewebsites.net (user)
Ports
The 65349 ports scanned but not shown below are in state: filtered

65349 ports replied with: no-responses

Port		State	Service	Reason
80	Tcp	Open	http	Syn-ack
443	Tcp	Open	https	Syn-ack
454	Tcp	Open	contentserver	Syn-ack
1221	Tcp	Open	Sweetware-apps	Syn-ack
4022	Tcp	Open	dnox	Syn-ack
4024	Tcp	Open	Tnp1-port	Syn-ack
8172	Tcp	Open		Syn-ack

Table 4: Results of port scanning

On the local version of the app, a vulnerability scan was also carried out using the nessus application installed on Kali Linux below is the result of the analysis.

Nessus Scan

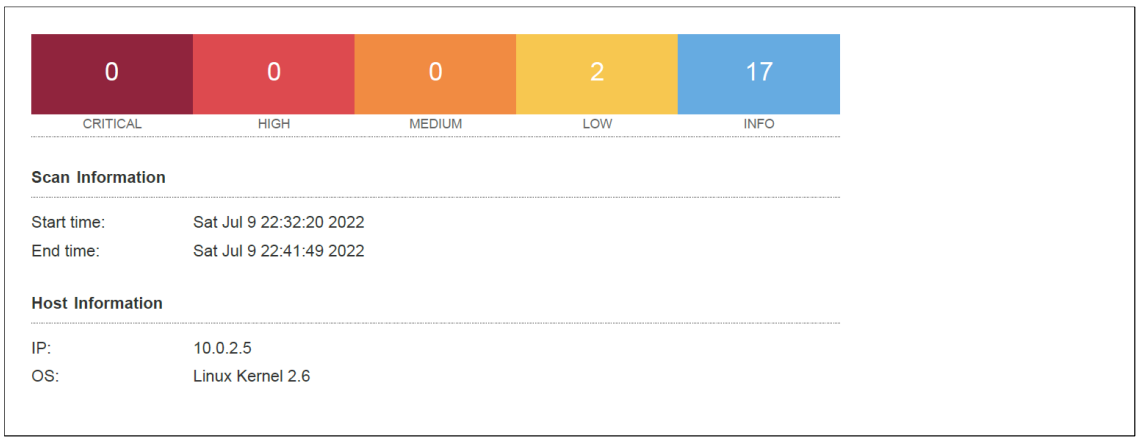

Table 5: Results of vulnerability scan using the Nessus tool

6.2 Discussion:

The ANOVA test was carried on the hospital visits report. And from this statistical analysis done, The analysis of the hospital visits shows that there is significant change in hospital visits between the year 2020 and the year 2022 in Ireland according to the data gathered across Europe. (ECDC, 2022)

H0: There is no significant difference in hospital visits between the year 2020, 2021 and 2022

H1: There is a significant difference in hospital visits between the year 2020, 2021 and 2022

The null hypothesis is rejected and the alternative hypothesis accepted as the Post-hoc Test confirms that there is significant change in hospital visits especially comparing the records between 2020 and 2022. These supports the statement in this research that shows that hospitals got overwhelmed during this period and here by sort to migrate their eHealth application to the cloud to handle the capacity of patients in the hospital and also to monitor patients' health remotely, hereby reducing the number of patients that actually need to come to the hospital.

With eHealth Application hosted securely in the cloud, health care providers employed patient appointment scheduling agents that can work remotely, and book hospital visits which filters the number of patients that come physically to the hospitals; as hospital visits are strictly appointment-based.

The vulnerability assessments done on the federated eHealth authentication application shows that the framework is relatively secured with no Alerts of vulnerabilities in the risk level bands "High" and "Medium" but with just two alerts of Low. One of which is "Cookie No HttpOnly Flag" that has been remediated with the application's migration to Azure cloud with TLS certificates provisioned.

The federated authentication system implemented in this research makes replay attacks, brute force attacks and other cloud security threats mentioned in the earlier sections impossible, and hereby preserve the confidentiality of patients records and achieves the healthcare provider's regulatory obligation of ensuring privacy of patient's records.

7 Conclusion and further research

Many Organizations and businesses; e-commerce, servicing, manufacturing and so on has replicated their on-premise infrastructure into cloud, but this shift has been slow with most health care providers. The advent of covid however forces several hospitals to follow suite and even though being faced with cloud security threats, the methodology in this research can take advantage of the federated authentication protocols, oauth2, VPN remote desktop protocols, and MFA to achieve a well architected cloud secured federated authentication system that prevents security threats like brute force attacks, replay attacks that could compromise the security of an eHealth system and the privacy of patient records.

For further studies, the limitations of oauth2 in maintaining the anonymity of users of an eHealth system can be done, an advancement in this protocol or a provision of another protocol that provides all the advantage of oauth2, and yet never shares user attributes by IdP to service providers, without users consenting to the attributes to be shared while a trust relationship is securely built between IdPs and Service providers.

References

Alabdulatif, A., Khalil, I., Mai, V., 2013. Protection of electronic health records (EHRs) in cloud, in: 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). pp. 4191–4194. https://doi.org/10.1109/EMBC.2013.6610469

Bahrami, M., Singhal, M., 2015. A dynamic cloud computing platform for eHealth systems, in: 2015 17th International Conference on E-Health Networking, Application & Services (HealthCom). pp. 435–438. https://doi.org/10.1109/HealthCom.2015.7454539

billmath, 2021. AD FS Overview [WWW Document]. AD FS Overv. URL https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview (accessed 8.13.22).

Chalker, A., Hillegas, C.W., Sill, A., Broude Geva, S., Stewart, C.A., 2020. Cloud and on-premises data center usage, expenditures, and approaches to return on investment: A survey of academic research computing organizations, in: Practice and Experience in Advanced Research Computing. ACM, Portland OR USA, pp. 26–33. https://doi.org/10.1145/3311790.3396642

Deebak, B.D., Al-Turjman, F., 2021. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. IEEE J. Sel. Areas Commun. 39, 346–360. https://doi.org/10.1109/JSAC.2020.3020599

Django official, 2022. Security in Django | Django documentation | Django [WWW Document]. Secur. Django. URL https://docs.djangoproject.com/en/4.1/topics/security/ (accessed 8.8.22).

Dodanduwa, K., Kaluthanthri, I., 2018. Role of Trust in OAuth 2.0 and OpenID Connect, in: 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS). pp. 1–4. https://doi.org/10.1109/ICIAFS.2018.8913384

ECDC, E., 2022. Data on hospital and ICU admission rates and current occupancy for COVID-19 [WWW Document]. Eur. Cent. Dis. Prev. Control. URL https://www.ecdc.europa.eu/en/publications-data/download-data-hospital-and-icu-admission-rates-and-current-occupancy-covid-19 (accessed 8.12.22).

eHealth Ireland, I., 2020. Privacy [WWW Document]. EHealth Irel. URL https://www.ehealthireland.ie/a2i-hids-programme/individual-health-identifier-ihi-/privacy/https:/www.ehealthireland.ie/a2i-hids-programme/individual-health-identifier-ihi-/privacy/privacy.html (accessed 7.19.22).

Elhoseny, M., Thilakarathne, N.N., Alghamdi, M.I., Mahendran, R.K., Gardezi, A.A., Weerasinghe, H., Welhenge, A., 2021. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability 13, 11645. https://doi.org/10.3390/su132111645

Ferdous, Md.S., Chowdhury, F., Alassafi, M.O., Alshdadi, A.A., Chang, V., 2020. Social Anchor: Privacy-Friendly Attribute Aggregation From Social Networks. IEEE Access 8, 61844–61871. https://doi.org/10.1109/ACCESS.2020.2981553

Garcia, R., 2017. Federated identity hybrid cloud security considerations supporting first responders, in: 2017 IEEE Conference on Dependable and Secure Computing. pp. 326–333. https://doi.org/10.1109/DESEC.2017.8073819

GDPR, 2019. Data Protection Commission [WWW Document]. Data Prot. Comm. URL https://www.dataprotection.ie/dpc-guidance/blogs/does-gdpr-really-say (accessed 4.9.22).

Gonçalves, C., Sousa, B., Antunes, N., 2022. BIANFE: Object identification and authentication in federated scenarios, in: 2022 IEEE 19th Annual Consumer Communications &

Networking Conference (CCNC). pp. 957–958. https://doi.org/10.1109/CCNC49033.2022.9700542
HSE, F., 2018. hse-gdpr-faqs-public.pdf [WWW Document]. URL https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf (accessed 6.22.22).
Jared, C., JP, M., Morgenthal, B.G., 2012. Cloud Computing : Assessing the Risks [WWW Document]. URL https://eds.p.ebscohost.com/eds/ebookviewer/ebook/ZTAyMG13d19fNTcxNTU0X19BTg2?sid=4ac1f6f2-a59f-49f0-9da2-393ba07323b0@redis&vid=5&format=EB&rid=5 (accessed 4.7.22).
Jusak, J., Mahmoud, S.S., Laurens, R., Alsulami, M., Fang, Q., 2022. A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Testbed. IEEE Access 10, 1082–1095. https://doi.org/10.1109/ACCESS.2021.3138135
Liang, Y., Chunming, R., Gansen, Z., 2009. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography 726.
Liu, Y., Zhang, Y., Ling, J., Liu, Z., 2018. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Gener. Comput. Syst. 78, 1020–1026. https://doi.org/10.1016/j.future.2016.12.027
Mamun, Q., Rana, M., 2017. A robust authentication model using multi-channel communication for eHealth systems to enhance privacy and security, in: 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). pp. 255–260. https://doi.org/10.1109/IEMCON.2017.8117210
Mehrtak, M., Alinaghi, S.A.S., Pour, M.M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., Dadras, O., 2021. Security challenges and solutions using healthcare cloud computing. J. Med. Life 14, 448–461. https://doi.org/10.25122/jml-2021-0100
Papadamou, K., Gevers, S., Xenakis, C., Sirivianos, M., Zannettou, S., Chifor, B., Teican, S., Gugulea, G., Caponi, A., Recupero, A., Pisa, C., Bianchi, G., 2020. Killing the Password and Preserving Privacy With Device-Centric and Attribute-Based Authentication. IEEE Trans. Inf. Forensics Secur. 15, 2183–2193. https://doi.org/10.1109/TIFS.2019.2958763
Reis, L.H.A., de Oliveira, M.T., Mattos, D.M.F., Olabarriaga, S.D., 2021. Private Data Sharing in a Secure Cloud-based Application for Acute Stroke Care, in: 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS). pp. 568–573. https://doi.org/10.1109/CBMS52027.2021.00039
Rodrigues, J.J., Torre, I. de la, Fernández, G., López-Coronado, M., 2013. Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. J. Med. Internet Res. 15, e2494. https://doi.org/10.2196/jmir.2494
Thilakanathan, D., Zhao, Y., Chen, S., Nepal, S., Calvo, R.A., Pardo, A., 2014. Protecting and Analysing Health Care Data on Cloud, in: 2014 Second International Conference on Advanced Cloud and Big Data. pp. 143–149. https://doi.org/10.1109/CBD.2014.25
Thilakarathne, N.N., 2020. Security and Privacy Issues in IoT Environment. Int. J. Eng. Manag. Res. 10, 26–29. https://doi.org/10.31033/ijemr.10.1.5
Vaios, B., Nikos, P., 2019. IdeNtity verifiCatiOn with privacy-preservinG credeNtIals for anonymous access To Online services - INCOGNITO Deliverable D3.1.
Yoon, J., Drumright, L.N., van der Schaar, M., 2020. Anonymization Through Data Synthesis Using Generative Adversarial Networks (ADS-GAN). IEEE J. Biomed. Health Inform. 24, 2378–2388. https://doi.org/10.1109/JBHI.2020.2980262