Full-Scale Evaluation of the Mental Healthcare Data Protection

Amani Bawaked
University of Denver
Denver, CO
Email: amani.bawaked@du.edu

Aishwarya Surani
University of Denver
Denver, CO
Email: aishwaryaumesh.surani@du.edu

Matthew Wheeler
University of Denver
Denver, CO
Email: matthew.wheeler@du.edu

Braden Kelsey
University of Denver
Denver, CO
Email: braden.kelsey@du.edu

Nikki Roberts
University of Denver
Denver, CO
Email: nicolette.roberts@du.edu

David Vincent
University of Denver
Denver, CO
Email: david.vincent@du.edu

***Abstract*—The adoption of digitization in every sector is accelerating. Online shopping, banking, food delivery services, healthcare and many other sectors are adopting digitization and providing services to the users online. One of the most booming sector is the healthcare where users are provided services in form of websites and web applications. These services not only include health checkups but also provide mental health support online. With pandemic there has been a surge in getting these services online like booking an appointment, to get information regarding physicians, get electronic health records, having mental health therapy sessions online and so on. Given the nature of these healthcare services especially when dealing with mental health, users share sensitive and personal information online through websites or web apps for consultation. This brings an additional risk of users privacy and security. To further understand this, the aim of this paper is to conduct a full scale evaluation of top 48 websites and 50 web applications in mental healthcare domain to analyse how these mental care services are accessing user data. Our study evaluated security and privacy policies of both mobile apps and websites to analyse how mental health services are designed and developed. While evaluating the security measures we also conducted a case study on how mental health services offered by the mobile application is different than the general healthcare applications.**

***Index Terms*—mental-healthcare, healthcare, data, security, web services, applications.**

I. Introduction

Mental Healthcare has been revolutionized by technological advances in recent years [1]. It is a highly data-intensive field, generating, disseminating, storing, and accessing a large volume of data each day [2]. The data generated by mental healthcare services has become one of the most valuable assets in the current digital age [4]. A great deal of data is generated by every digitalized industry. It is a challenging and complex task for any security expert to manage this big amount of data securely [4]. In addition, Mental healthcare data plays a significant role in people's lives. As can be seen from the current increase in cyber-attacks, the cybercriminals are concentrating their efforts on these repositories of data in order to take advantage of the money that can be made from data that has been tampered with or stolen [4]. There have never been more technological challenges in the healthcare domain [1]. Healthcare data is increasingly viewed as a valuable commodity by third parties. Medically and healthcare-infused data are scraped by big data brokers with the intention of supplying their predictive analytics services, while cybercriminals have long recognized the benefits of stealing health records, which can provide an abundance of financial opportunities using this information [4].

Within the next few years, there will be an increase in security breaches due to the rapid change in the risk environment and widespread disclosure of new vulnerabilities and threats. Additionally, due to the Affordable Care Act, more people will enroll in health insurance, which will present an appealing target for cybercriminals and lead to a proliferation of breaches in the healthcare industry [8]. Violation of patient data in electronic health records can jeopardize patient privacy and breach the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) law in the U.S. [9], [10]. In order to ensure patient safety, electronic health record security must be a top priority.

Since the turn of the century, there has been an exponential growth in the provision of online health interventions, as well as scientific evaluations of their effectiveness [43]. It is a common occurrence that security considerations are overlooked and underfunded when developing, delivering, and evaluating electronic mental health interventions, even though security is vital to the overall success of such projects [43]. In light of this, the technology that is used to store and transmit this kind of sensitive information must be evaluated for its security. In addition, ensure that the best security measures are being implemented, and that they are being continually reviewed.

In order to evaluate the security and privacy of a specific electronic service provided by any mental health care provider,

there are security measures should be evaluated. Also, there are many automatic tools that can be used to help in conducting such as evaluation. Examples of those tools are SSL lab and MobSF. These tools are providing a report about the security measure configurations which can be reviewed and evaluated to build a conclusion about the security level of the service; which is the method we followed throughout our paper.

In this paper, we describe a method for testing and analyzing the privacy and security of mental healthcare webs services and applications. In addition, we conduct a case study on mental health applications to compare general health care to the mental health care applications. Our results are showed that Mental healthcare websites adhere to strong security protocols and high overall security rates. On the other hand, mental health mobile applications should improve the way permissions are handled and certificate encryption algorithms used. In the case study we found that both general and mental health application having equal security level.

The following is a brief summary of how the paper is organized: Section II presents the related work, Section III outlines the overall methodology. Section IV shows the results of the analysis. Section V to cover a case study on general health data security. Section VI discusses the result. Section VII that illustrates the implications of the research findings. Section VIII depicts the limitation and provides future work. Section IX concludes this paper.

II. Related Work

There has been a rise in providing IT services online [46]. Veliz mention in their study that technology has played an important role in pandemic. With pandemic, majority of the services are online and are helping users with their needs [33]. There are various sectors like e-commerce, education, healthcare, food services etc. that are moving towards digital world. All of these services are provided to the users online where users use websites or applications to connect and avail these services. This has led to removal of manual paper work and storing digital records in the system. With digitization, the overall cost to the company is reduced as there is no need of maintaining any data manually and can be handled by the system [30].

Healthcare is one of the sectors that is increasing especially due to pandemic as patients do not have to travel and can avail the services online from anywhere and whenever they want [34]. Patients can schedule their appointment, get medical help, can query about different medicines and their use, and also get dietary plans and so on. All of these services do not require patients to be in person but can connect to the internet to get these services. These services are available to the users in the form of websites and mobile applications. Users can connect to the websites or install mobile application to connect to these services whenever they want [32].

Apart from general healthcare, mental healthcare services are also provided online. Earlier, all the counseling and mental health issues were provided by the medical professionals [38]. But now users can avail the mental health services online through various telehealth services. Due to pandemic, users had a hard time getting mental consultation and needed the mental support for well being and so there has been a surge in getting the mental healthcare online. Users can book an appointment for psychiatric consultation, schedule therapy sessions for themselves, group or family online, get other medical assistance whenever they need [47]. However all of these services require users to share their personal and sensitive information with the system which increases security risk. When these services are provided in person the medical professionals are required to have documents as per the state or country to practice it [39]. Also all of these professionals need to follow rules and regulations like maintaining confidentiality of the patients data and they are subject to action if disclosed the sensitive data [40]. But with these services moving online there is no law or regulation which is governing the way the users data should be used of stored in the system. If the patient data is disclosed without the consent then there can be loss of reputation for users and also a privacy breach [41]. There is a lack of transparency to the way the data is shared or used by the systems [42].

A. Mental Healthcare Websites

Mental healthcare is very crucial as it requires timely medical assistance whenever the the users need. There have been several research studies to understand if mental health services is effective when provided online or not. Kauer et al. in their research conducted qualitative and cross sectional experiments where they found that users availing the mental health service online as satisfactory [48]. Young et al. evaluated websites that offer mental health services for youth and shared the findings. The results showed that the information shared by the website was informative and accurate and users are using the services online [49]. Oh et el. compared the mental health services provided online vs in person and found youth were comfortable with both the ways of services. However there was a inclination of getting these services online as youth were more comfortable sharing their issues with the system rather than medical professionals [50]. Cavanaugh et al. conducted a study to evaluate mental health websites to see how parents can get help from these websites in terms of learning about mental health disease. The study showed that the content was useful and can be used by the users [51].

B. Mental Healthcare Mobile Applications

Apart from providing mental healthcare services through websites, they are also provided in the form of mobile applications that can help users connect to the medical professionals easily. Wang et al. in their study reviewed the mental health applications in times of covid-19 to study if the use had increased or not. The results show that use of these applications surged during pandemic as the psychological needs of the patients increased during this time [52]. Grist et al. conducted study to review mental healthcare applications for young generation and children. The study showed that the use of application by children was satisfactory. However there is a

need to do full proof research in understanding how effective the applications are for children [53]. Lui et el. focused on how effective mental health mobile applications are in terms of psychological help. The results show that users should use these applications carefully given the nature of the medical assistance needed [54].

The crucial aspect in using these services whether it is in the form of websites or applications is the security and privacy. To use these services users need to share the personal information with the system and there is no guarantee that the data is not disclosed to any third party services. It is important to analyse the security aspects from users perspective.

C. Security and Privacy Concerns in Mental Healthcare

When dealing with the healthcare data the most important concern is of security and privacy of user data. Trust also plays an important role from users perspective. When users communicate with the system, it is important for the websites and mobile application provider to ensure that the data is not compromised or shared as it has personal health-related information. It is necessary to have security and privacy laws and regulations between the users and the system for functioning [31]. In terms of mental health websites we need to study what protocols are used for communication over the internet and also how the data is stored in the back end because there are chances that the data might be stolen or disclosed. In terms of mental healthcare mobile applications we need to analyse the way permissions are granted to the users and also analyse the vulnerabilities in the application. With the rise of technology in these services it is important to analyse the security aspects for the users to communicate with the system without any hesitation.

III. Methodology

During our research we focused on the quality of healthcare sites that dealt with mental health. We defined a mental health service as any that would have access to; mental health appointment information, mental health insurance information, or mental health medication. We decided on this definition as having access to any of these pieces of information would give a person insight into the mental state of a subject. Security for mental health data is important as if an attacker is involved in the trauma of a victim, they could abuse the information and cause further trauma to the victim.

In order to conduct our evaluation of data confidently, we started by compiling a list of websites and mobile applications of mental and physical healthcare institutes in the United States. Following that, we automatically scanned the websites and applications of these institutions for security and privacy measures and analyzed their details. Lastly, we conducted quantitative analyses that allowed us to identify some of the privacy characteristics associated with these websites and applications. This section provides details of these steps.

A. Planning the Evaluation

The first step in this evaluation is identifying the need for this project to be conducted. As a starting point of our research, we defined the objective; our goal was to conduct a comprehensive assessment of the mental healthcare data protection requirements for the top 89 websites, web services, applications, and telehealth services. Furthermore, conduct a case study on 9 physical healthcare applications to compare the security level of the physical healthcare applications with that of the mental healthcare services, focusing on how data is accessed and stored by them. As a result, we designed an evaluation protocol that defined the criteria for selecting websites, web services, applications, and telehealth services, and analyzing each in order to reach the study's objective; this protocol is described in the following section.

B. Obtaining a Primary List of the Healthcare Services

As the first step, we aim to collect 98 mental and physical healthcare websites, web services, and applications in total to create a primary list. We made sure that we are covering in our primary list a combination of the following health services: general hospitals, private practices and physicians, outpatient facilities, pharmacies; and community health centers. Each individual service entity is operate in the English language and the providers of each service are based in the United States. In order to find and collect the entities of the primary list, we used Google's search engine. The primary list contains fifty web-based services in the form of websites, web services, or telehealth services. On top of that, it contains fifty mobile applications that work on the Apple operating system or Android operating system.

C. Web-services Evaluation and Security Measures

In this section, we will perform HTTP analysis by examining the configuration of the web server to check the integrity of the data transmission. A tool called SSL Labs is used to analyse the server of the application. SSL Labs is an online service that inspects a server's certificate and secure configuration and assesses the server's TLS security and assigns a letter grade. In this test, a certificate is examined to verify that it is legitimate and trustworthy. As well as examining protocol support, key exchange support, and cipher support, this examines server configuration. After examining these points, the areas scores are combined to produce an overall score and an academic letter grade (A+, A, A-, B, C or F). If exploitable vulnerabilities are found or if a specific patch has not been implemented, these letter grades are adjusted downward. As an example, a server that is not patched is given a letter grade of failure [22]. It is possible for the SSL Labs Server Test to not provide a letter grade of (A+ - F) in certain circumstances. For instance, if the site certificate has not trusted, the test will issue grade of T. The test will also issue grade of M if there is a certificate name mismatch. It is important to remember that if a trust certificate is not present or the certificate name is mismatched, the actual security grade is irrelevant since active network attackers can undermine the security of connections [22]. The SSL Labs website features a detailed description of handshake simulations using different platforms like Android, Chrome, and Firefox [22].

1) Security Measures: In this part, In order to determine the security level of the HTTP data transmission, we used SSL Labs to analyze the web server configuration and to evaluate the data transmission security. The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems and it is transferring data as plain text without being encrypted [11]. The Transport Layer Security protocol (TLS) ensures the security of data sent between applications over the Internet from end-to-end; TLS is a cryptographic protocol [12]. The Secure Socket Layer (SSL) protocol helps protect sensitive information such as credit card numbers, SSNs, and login credentials [12], [13]. Plain text is typically the format used to send data between browsers and servers. The information sent between a browser and a web server can be intercepted and exploited by an attacker who is able to intercept the data sent between them [13]. Both TLS and SSL are intended to ensure the authenticity and confidentiality of online communications, as well as the integrity of transmissions. SSL and TLS are available in different versions, and the oldest once had very serious vulnerabilities [14], [15].

This paper examines SSL version numbers and TLS version numbers due to SSL and TLS versions being available in different versions, and also to known vulnerabilities in the old versions. There are improvements made to more recent versions that are considered to be more secure. During the evaluation, we will look at the use of SSL/TLS as well as the oldest supported version. Due to the fact that SSL 2.0 had no functionality to prevent tampering with the Handshake message portion (data integrity isn't guaranteed), MITM attacks were possible, and the protocol itself was recognized as vulnerable [14]. In addition, the POODLE attack (Paddling Oracle On Downgraded Legacy Encryption) makes it possible to carry out a hacking activity against SSL 3.0 when it is used to encrypt messages using CBC ciphers, so SSL 3.0 is currently discouraged [14], [16]. By using POODLE, third parties will be able to extract plaintext from SSL 3.0-protected traffic, for example, by stealing "secure" HTTP cookies (or other bearer tokens such as those within HTTP Authorization headers) [16]. Other than SSL 2.0 and SSL 3.0, there are no known security problems with the new TLS versions, as long as the server and client are configured correctly; An improved POODLE attack and other vulnerabilities exist with older versions of TLS that lack proper configuration [16]. Clients alone can mitigate Browser Exploit Against SSL/TLS (BEAST) which is an additional TLS 1.0 vulnerability [17]. We focus our paper on these protocols, because SSL/TLS is certainly one of the most important protocols in the security field, since it is the backbone of our communication privacy and security. This makes it an attractive target for both attackers and security professionals [18] The examination and the use of these protocols will be shown in the Results section.

The authentication and exchange of key material are carried out by TLS using asymmetrical cryptography and public key infrastructure (PKI) [12]. As remote services become more common, PKI plays a crucial role in ensuring security and reliability. The modern PKIs rely on public key certificates, which are issued by certification authorities (CAs), which can be exchanged publicly online. Certificates are used to authenticate servers [20]. During this certificate interactive process, the server transmits a certificate containing its public-key, thereby increasing the Message Digest of the server certificate. Upon receiving the server's certificate, the client validates its legality and effectiveness, computes the certificate's value, then compares that value with the value that is calculated by the server; if the value between them is different, the message has been modified in progress, so the server should be disconnected [20]. Whenever the client confirms the validity of a server certificate, it traces the chain of trust from the server certificate [20]. As part of this study, we researched certificate concerns.

In our work, we also focus on providing an evaluation of HTTP Strict Transport Security (HSTS). One of the most widely used techniques was described by Moxie Marlinspike [18], in which old HTTP connections were stripped, HTTPS links were rewritten to HTTP, cookie properties were changed and other similar changes were made. Users usually type only the name of the website into their browsers instead of the full URL, which results in the first connection being an HTTP connection, which is vulnerable to being intercepted and tampered with. The HSTS came about in response to Moxie's stripping attacks. In order to use HSTS, a special header must be sent by the server; this instructs the client to only communicate via secure HTTPS connections. Clients and servers must both support HSTS in order for it to work. While HSTS is primarily a concern for browser-based Web applications, a large number of apps include Web components that rely on the browser platform [19]. In the Results section, HSTS headers will be displayed if they are present in the server responses.

Simulation of the handshake process occurs in data communication when the hardware and software need to agree on the state of the operation mode before exchanging any information. A communications parameter is a set of communication parameters that defines the exchange of data between a sending station and a receiving station. In the TLS Internet Standard, the clients and servers are able to choose among a variety of cryptographic algorithms and constructions for each handshake. Through the TLS protocol, confidential internet communication is maintained. A client/server application can communicate using this protocol in a way that is designed to prevent eavesdropping, message forgery, and tampering. TLS Handshake Protocol generates the cryptographic parameters for the session state, which is built upon TLS Record Layer. TLS clients and servers first establish communication by agreeing on a protocol version, determining the cryptographic algorithm, performing authentication if necessary, and setting shared secrets via public-key encryption. In this paper, we are doing automatic handshake simulation to know the used cryptographic algorithm types.

D. Mobile Applications Evaluation and Security Measures

In this section, we use MobSF which is an open source security assessment tool to perform static analysis of mobile healthcare web applications. With the help of this tool we analysed 50 Android based web apps to identify various security algorithm and vulnerabilities used by each of them.

1) MobSF: MobSF is an open source tool is used to perform static and dynamic analysis of mobile software including android, ios. This tool runs to analyse the different parts of the application, and validates the certificates if present, and does code analysis [25]. It can be used to check for malwares. It requires Python 3.6 or above and JDK 1.8 or above [27]. Using MobSF, the Android manifest files can be analyzed to check permissions and identify potential risks.Code analysis can also be done to check for any hardcoded data, cryptographic keys, errors in SQL query parsing which might lead to SQL injections [28]. MobSF has an interactive Graphical User Interface (GUI) to help security researchers better visualize the results. Once a file is uploaded, a dashboard displays basic information, permissions, Android API's used, Browsable Activities, Security Analysis, Malware Analysis [25].

2) Steps followed for analysis: After the tool was installed, the name of the app to be analysed was typed in the url part of the browser and the apk file was uploaded to the mobsf page. After the installation, the "Start Static Analysis" was selected and the analysis started. The dashboard of MobSF tool is shown in Figure 1. Once the analysis got completed the tool generated a pdf report for each mobile application. The report provided app security score, grade, file and app information in terms of md5, sha-1 algorithm, services and activities. It also provides certificate information in detail and permission settings of the app along with status that mentions if the permission could be dangerous or normal.It also highlights issues in the app with severity level and also provides malware check.

3) Security Measures: We need to evaluate security measures of Mental healthcare applications to understand how the applications are performing in terms of permissions, certificates, vulnerabilities, libraries and code analysis.

In terms of vulnerabilities, it is considered a threat to the application and need to be resolved as soon as possible if found. MobSF tool highlights two types of vulnerabilities in the report. First being Janus vulnerability, it is a vulnerability that infects the code without modifying the signature. The attackers can add some bytes to the APK andf DEX files in mobile application. APK file is a package in android used by the operating system in mobile phones. DEX is kind of virtual machine which is used by Android operating system for interpretation of the compile code. So janus vulnerability is when the attacker modifies the apk files in such a way that the signature verification part is bypassed. The authenticity is compromised and not checked. MobSF highlights the mental and general healthcare applications that can be susceptible to this vulnerability in terms of high, warning and low [55]. Hash Collision is

In our work, we also tried to evaluate the way mental healthcare applications are dealing with the permissions. Permissions are an important aspect in the mobile application as they drive who can access what. Sharing location, camera, audio can be dangerous and needs to be implemented securely. Certificates are another aspect that needs to be taken care of when working mobile applications. We analysed the different encryption algorithm used by the mental healthcare applications like SHA1, SHA256 with RSA and MD5 hash. SHA1 is hash function that is used to for signing he message to be sent and is used with RSA for better security. RSA is public key algorithm which is used for encrypting and decyrpting the data. We also analysed if applications used SHA256 RSA algorithm which is more effective than SHA1 as the key length bits is of size 256. SHA256 is used to create hash value from the input then apply RSA encryption to encrypt the data with the help of private key [57].

We also evaluated the signature schemes and key bit size to analyse how effective security measures are taken by the mental health applications. While developing android applications the developers need to sign the APK to ensure that authenticity of the application. For this purpose there are various signature schemes used to ensure that safety of the applications.V1 signature is the traditional one and has been used since the beginning of the android applications. It is based on signing the jar but it has some security issues as it cannot protect certain parts of the code. V2 and V3 are more effective and secure than V1. In V2 it can help find all the updates in the apk file that are not possible in V1. This ensures more security and verification of the application. V3 is similar to V2 but it add more information related to SDK versions [58].

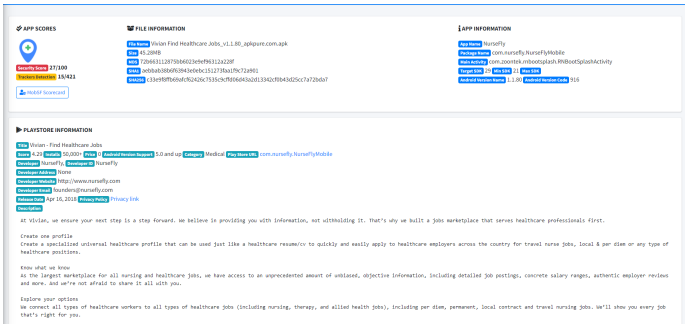

Fig. 1. Dashboard of MobSF tool

IV. Results

The aim of this section is to present the findings of the analysis of web services and mobile applications that are related to a list of mental healthcare services to know the level of data safety and protection. We will begin this section with a description of the results of a set of security measures that are the result of examining the server configuration of 48 mental health providers' web applications. Following that, demonstrate the results of the security examination of 40 apple and android mobile applications that are provided by different mental healthcare organizations

A. Web-services Security Examination Results

The first measure we focused on to examine the security of the server is the total letter grade of the server. Grading is based on several factors that are evaluated with the help of the SSL Labs tool to determine if the SSL protocol is configured properly in the server. The evaluation process includes the following steps [56]:

- Verifying the validity and trustworthiness of a certificate
- Examined the server configuration in three different categories, which are Protocol support, Key exchange support, and Cipher support.
- Adding each category score to an overall score that is determined by a number between 0 and 100. A score of zero in any category will result in a score of zero for the overall score. After that, the letter grade is determined, as shown in the Table I.Mention should be made that there are some characteristics of server configuration that cannot be summed up numerically. As a reward for the exceptional configurations on the servers, the grade was raised to A+. This grade means the server with good configuration, no warnings, and HTTP Strict Transport Security support with a minimum age of 6 months.

TABLE I
THE LETTER GRADE TRANSLATION

Numerical Score	Grade
A score of 80 or higher	A
A score of 65 or higher	B
A score of 50 or higher	C
A score of 35 or higher	D
A score of 20 or higher	E
less than 20	F

After examining the servers of each web service of our primary list of mental healthcare providers, and get its calculated grade rating, Figure 2 shows a bar chart of the SSL Labs service test grades and its percentage. In the chart, its show that most of the servers tested (19) were rated A+, while (17) of them rated B, and the rest (12) rated A.

Also, the examination of the web services showed that all the servers (100%) are certificated with with 91.67% utilizing RSA 2048-bit encryption, 2.08% using RSA 4096-bit encryption, and 6.25% using EC 256-bit encryption. In addition, 14.58% of those servers are having DNS Certification Authority Authorization (CAA), that mean domain name owners of these servers can be trusted to issue digital certificates to their hostnames; nevertheless 85.42% are not allowed to do that.

As part of our analysis, we looked at the security issue of public key cryptography, which is a stronger encryption method. Public key technology is sometimes called certificate authentication, even though certificates are only one of the applications of public key technology. A key size decision is one of the most important considerations in this area. After doing the automatic handshake simulation using SSL lab tool to know the used cryptographic algorithm types.

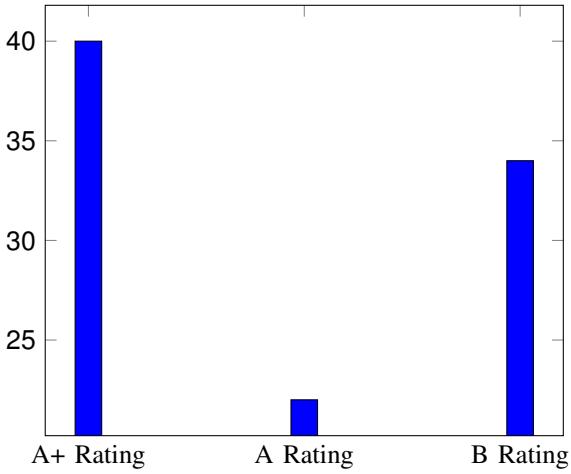

Fig. 2. SSL Labs Service Test Grades

The results showed that 93.75% of the servers are using the cryptography algorithm SHA256 with RSA, and 6.25% are using SHA256 with ECDSA. Additionally, we found that there was a difference in the size of cryptographic keys between the servers as shown in the pie chart in Figure 3; 91.67% are using RSA 2048 bits, 6.25% are using EC 256 Bits, and 2.08% are using RSA 4096 bits. In addition, We found that 8% of the servers showed weak in the key exchange.

In our results we investigate the session resumption; an adaptive, performance-optimized technique that saves the results of costly cryptographic operations and makes them available for reuse. When the session resumption mechanism is disabled or nonfunctional, a significant performance hit may be experienced. We found that 77.08% of the mental healthcare servers are support session resumption through caching.

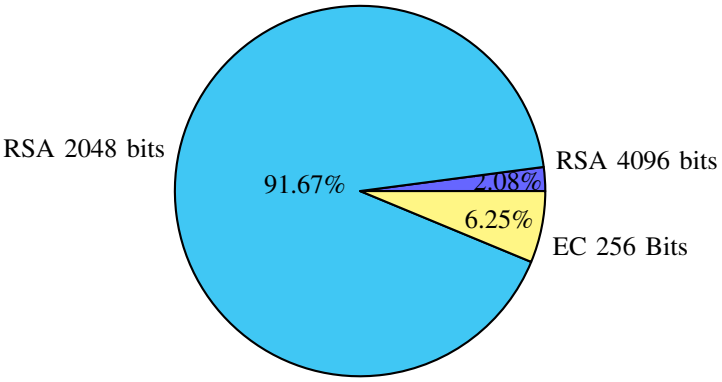

Fig. 3. Public key cryptography sizes

In order to maintain security on the web server, the web server configuration should be updated so that the proper certificate file, private key file, and certificate chain file generated by the certificate authority are used. We found that 68.75% of the servers don't had any certificate chain issues while 27.08%

faced issues on the contains anchor, and 4.17% contained issues related to incorrect order and extra certs.

The following Table II shows the scores SSL Labs assigns to each supported protocol version as of the writing of this paper. The percentage refer the amount of the server that we found support for the specific protocol version. Based on the results and as positive observations, TLS 1.3 support has been observed in 37.5% of the web servers when communicating with their functional servers.

TABLE II
PROTOCOL SUPPORT

Protocol	Percentage	Notes if any
SSL 2.0	0 %	-
SSL 3.0	0 %	-
TLS 1.0	8.33%	-
TLS 1.1	20.83 %	2.08% Supported in a weak way
TLS 1.2	100 %	6.25% Experimental: Server negotiated using No-SNI
TLS 1.3	37.5 %	-

Our results showed that HSTS support was observed in 64.58% of the servers, however, 6.25% is observed too short (less than 180 days). Furthermore, using the downgrade attack, the client is forced to connect to the server through an unprotected HTTP connection. By doing so, a malicious third party can perform a MitM attack and, as a result, access sensitive user information. As a positive result, we determined that 56.25% of the servers support the prevention of the downgrade attack with TLS_FALLBACK SCSV. For the other 43.75% of websites SSL labs was unable to determine the presence or lack-there-of of a downgrade attack prevention method.

Forward secrecy, sometimes referred to as perfect forward secrecy, is a protocol feature that allows for secure communications independent from the private keys of the server. Because forward secrecy is not provided by cipher suites, anyone who manages to recover a server's key can decrypt all the encrypted conversations the server has previously recorded. For modern browsers to enable forward secrecy, the server must support and prefer ECDHE suites. Our results showed that 79.17% of the mental healthcare servers of our primary list are support forward secrecy protocol with most browsers, while 8.33% support the protocol only with the modern browsers.

B. Mobile Applications Security Examination Results

We evaluated total 40 mental healthcare mobile applications to analyse the current security and privacy aspects. MobSF tool was used to access the applications in below different categories:

- Analysing the security score which of all the mobile applications.
- Analysing the scores given to each app by the tool along with tracker' detection.
- Analysing the different signature algorithms used along with signed information.
- Accessing different type of vulnerabilities with severity and identifying the encryption algorithm used by the app.
- A detailed description of the permission issues in the overall app design and use.

1) Security Score and Trackers Detection Analysis: After studying the individual report from mobSF tool for each mobile application. MobSf calculates the overall security score out of 100 based on the permissions, vulnerabilities, weak algorithms identified in the applications. From the report, we have analysed that 16 applications received score less than 40 whereas only two applications got security score greater than 60. The remaining applications have medium score overall.The overall lowest score is 20 which is given to three applications and are considered as high risk security applications. In terms of Tracker Detection, it allows users to scan an AirTag to check if there are any items with them without their knowledge. The MobSF tool also provides a score for tracker detection for each app in the report. The average score for all the 40 mental health applications is 5.425. This is an important feature which can be used to check how well the app is designed.

2) Grading of the application: MobSF provides rating to the apps from A to F depending on the security score. From the analysis of the all the applications, only 5% of the apps got an A rating. Fig 4 shows number of applications with the grades provided by the tool. 55% of the total mental health applications received B rating. The average percentage score of the 40 mental mobile applications is 41.6%. Majority of the applications got B and C rating respectively. 12.50% of the applications got F rating. Majority of the apps have B rating which is good from security standpoint. However there are 5 apps which have a F rating because of the poor security score. The general trend of all the apps with F rating have very high severity risks and moderate medium severity risks. However 27.5% of the apps received C rating. After analysing the reports of the apps receiving B rating it can be derived that majority of the applications are tagged as medium risk overall. They also have less high severity issues in the application and very few medium severity issues.

3) Certificate Analysis: Every website and mobile application needs certificate for maintaining the security and privacy and for identifying the traffic over the internet. MobSF report provides certificate information like the key size, encryption algorithm used, who is the issuer, validity, different hash used and fingerprint.From the analysis report, 23 applications are using SHA 256 with RSA to encrypt and decrypt the certificates. All of them are signed and the key bit size for 11 applications are RSA 2048 and the 12 applications are using key bit size of 4096. 11 applications are using key bit size of RSA 1024. One more important information that the report provides is whether the applications are using v1,v2 or v3 signatures. So v1 and v2 signatures are used in the android applications which is used to protect the APK and the integrity by verifying the changes made in the APK. So only the authorized one can update the APK. There is also another version v3 which allows to rotate the old key with the new one.It is more secure than previous one. Out of 40 mental

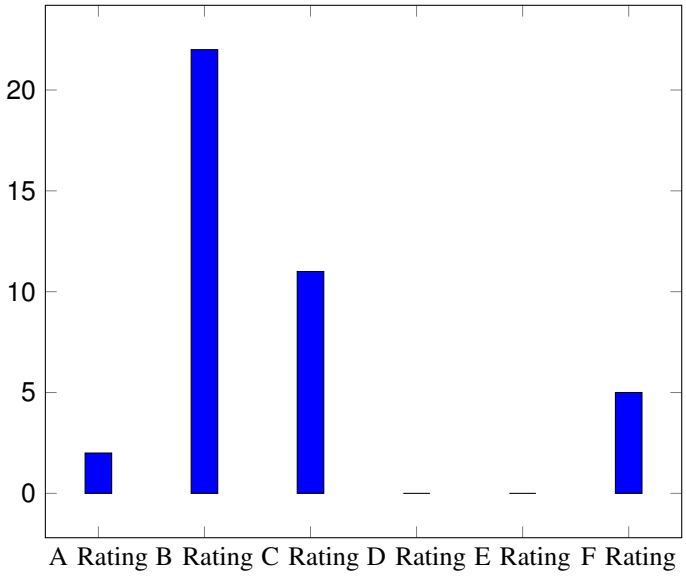

Fig. 4. MobSF Application Grades

health applications, 8 use all the three signature versions to ensure security and integrity of the APK code. 2 application do not use v3 signatures and 6 applications do not use v1 signatures but use v2 and v3. Fig 5 gives a snapshot of the percentages of applications using SHA1 and SHA256 with RSA algorithm.

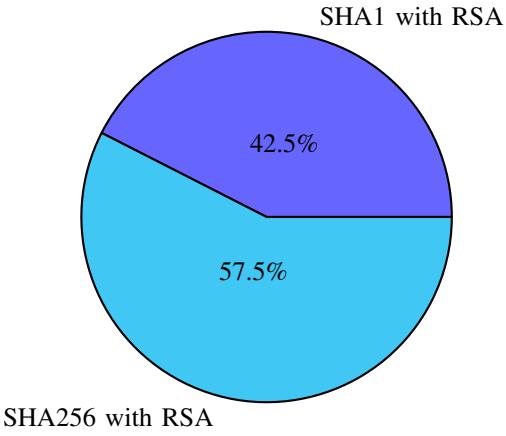

Fig. 5. Snapshot of Signature Algorithm

4) Analysis of Permissions: This section describes the various issues or good practices that mobile applications are using in terms of permissions. This is an important security aspect overall as it drives who can access what based on the levels decided. There are many softwares installed in the mobile that play an important role in defining the permissions. From the analysis of the report, we identified that there are different kind of software,hardware, tools in the mobile application that needs permission. Internet access, network access, wifi, boot startup access, read/write access to external storage, location access through maps, and many others. MobSF assigns the permission status levels- Normal, Dangerous, Unknown, Signature. Normal, unknown status permissions are not vulnerable to the application and can be treated secure as they denote that the apps do not access private data. Signature status is for the devices to communicate with the third parties. The most severe one is Dangerous as it implies that there are permissions which cannot be termed secure, can access to private and sensitive data and needs re-validation. Table 3 shows the ranking of different dangerous permissions used by the mobile applications overall. The highest is storage permission where majority of the apps have given full access to external or internal storage. This poses a risk and a threat to the CIA triad of cyber security. Camera is the second largest permission that needs to be validated as accessing camera can give the attackers to steal the data. Use Credentials is also one of the most important permission but that comprises of only 10% of the apps which is better than giving location access comprising of 50% which is alarming.

TABLE III
RANKING OF DANGEROUS PERMISSIONS IN MOBSF

Rank	Dangerous Permissions
1	Storage (80%)
2	Camera (70%)
3	Location (50%)
4	Phone State (40%)
5	Audio Recording (32.5%)
6	Account Related (17.5%)
7	Contact Access (15%)
8	System Alert Window (17.5%)
9	Activity Recognition (12.5%)
10	Use Credentials (10%)
11	Body Sensors (2.50%)
12	SMS (2%)

5) Manifest and Shared Library Binary Analysis: This section provides overview of the issues found in code, at network level, vulnerabilities in detail, issues in shared libraries and code. Manifest analysis report the issues in the code by providing severity and description of the issue. The different severity levels are- low, high and warning. Low and warnings can be ignored by the applications if there are lot of issues in high severity level. The issue gives the services names, activity names and network issue along with detailed description for the users to fix them. Overall if the issues are of high severity level then the security score drops of the particular app. There is also a section mentioned in the reports which is shared libraries in the code. The report provides full detailed information like name of the library causing issue, rpath and runpath of the library, whether the app has fortified functions that can cause buffer overflow attacks.

6) Vulnerability Analysis: Vulnerabilities are threats to the system, code and data. It is important to find the weaknesses in the system before the attackers so that the CIA is maintained. MobSF provides vulnerabilities by analysing the apps and also provide severity level alongwith detailed description.During

TABLE IV
SNAPSHOT OF MAJOR VULNERABILITIES WITH SEVERITY LEVEL IN PERCENTAGE.

Janus Vulnerability	**Percentage**
None	15%
Warning	82.5%
High	2.5%
Hash Collision Vulnerability	**Percentage**
None	57.5%
Warning	37.5%
High	5%

our analysis, the two vulnerabilities found in majority of the apps is Janus and Hash Collision.Janus is a kind of vulnerability that can inject code into the application and can run any malware in the system. Analysis from the report suggest that 15% of the apps do not have Janus vulnerability but 82.5% of the applications have received a warning about the vulnerability and there are still 2% who are vulnerable to attacks. Another critical vulnerability is Hash Collision where we get the same hash value for two different inputs. It leads to a collision and attackers can enter the system. Results show 57.5% of the apps do not have this vulnerability but it is still vulnerable to 5% of the apps. Table 4 gives an overview of the major vulnerabilities found in the apps.

7) Other Analysis: Apart from the above mentioned analysis themes, the report also provides information if there is domain malware or issue in database or emails and lists all the hard coded secrets. It does not always report issues or vulnerabilities, some are just mentioned for information purposes.For the malware check, it provides the domain name along with geographical location specifying the IP Address, country, region city and etc.

V. CASE STUDY: MENTAL HEALTHCARE VS GENERAL HEALTHCARE SECURITY IN MOBILE APPLICATION

Our first step in conducting the case study is to identify the providers that offer physical health services through their applications. We found from our primary list 11 out of 51 applications are providing general healthcare services whereas 40 are provide mental health services. After we shortlisted the applications list we performed a detailed analysis of each of them and conducted a case study focusing on comparing the security measures used to protect user privacy and security in the general health services to the mental health services security. Lastly, we provide our recommendations based on the results in each section.

1) Analysis on Application Score and Grading: From the MobSF results, we noticed that general healthcare applications and mental healthcare applications average score was similar. In terms of ratings no general healthcare application received A rating and 40% of the general applications received B rating. Both the mental and general healthcare service applications fall under B rating. The highest application security score in general healthcare service is 51 whereas in mental healthcare the score is 73. However the average tracker detection score of general healthcare service is slightly greater than the mental healthcare services. The number of mental healthcare applications receiving F rating is double than the number of general healthcare services. Also majority of the overall 50 applications fall in the category of B rating which shows moderate amount of security in the applications.

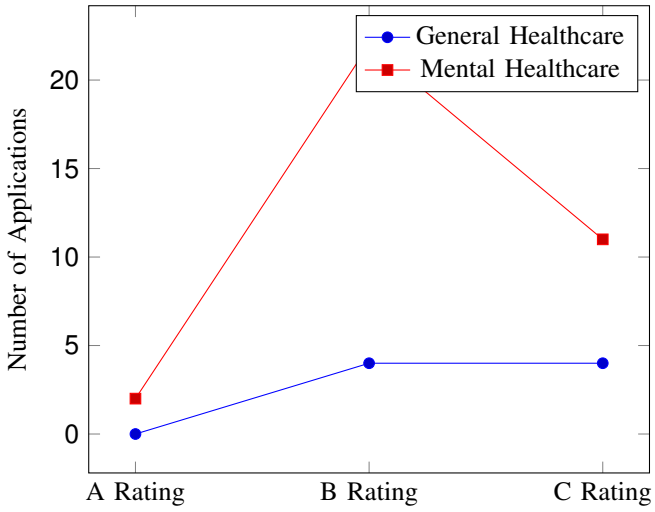

Fig. 6. Snapshot of Ratings for General and Mental Healthcare applications

2) Analysis on use of Certificates: Certificates are used for securing the applications and from the attackers. From the MobSF reports, all the applications including both general and mental health use signed keys for certificates. The signature algorithms used is similar in both mental health and general only 40% of the general application use SHA1 with RSA whereas 42.5% use SHA1 with RSA in mental health applications. None of the mental health applications use MD5 with RSA algorithm but 10% of the general healthcare applications use MD5. 57.5% of the mental health applications use SHA256 with RSA and 50% of the general healthcare applications use SHA256. There is difference in the key bits sizes in both mental and general healthcare. 40% of general healthcare use RSA 1024 key bits whereas only 27.5% of mental healthcare applications use RSA 1024. 2.5% of the mental health applications have the key bits in N/A category. General healthcare applications have equal split in using RSA 2048 and RSA 4096 key bits. Both general and mental healthcare applications have 30% using RSA 2048 key bits. Table V gives an overview of the signature algorithm used by the general and mental healthcare applications.

3) Signature Schemes: Both the mental and general healthcare applications use v1,v2 and v3 signature schemes. Table V provides key size used by the general and mental healthcare applications.All the general healthcare applications use v2 signatures but in case of mental healthcare, 97.5% of the applications use v2 signatures and 2.5% do not use this scheme. The number of applications using v3 is similar in both general and mental healthcare.The ratio of both the applications is 7:3. Majority of the applications are using v1

TABLE V
THE LETTER GRADE TRANSLATION

	General Healthcare	Mental Healthcare
Key		
RSA 1024	40.0%	27.5%
RSA 2048	30.0%	40.0%
RSA 4096	30.0%	30.0%
N/A	0.0%	2.5%
Signature Algorithm		
SHA1 with RSA	40.0%	42.5%
SHA256 with RSA	50.0%	57.5%
MD5 with RSA	10.0%	0.0%

in both the cases. 85% of the applications use v1 scheme in mental healthcare and 70% of general healthcare use v1 signature scheme.

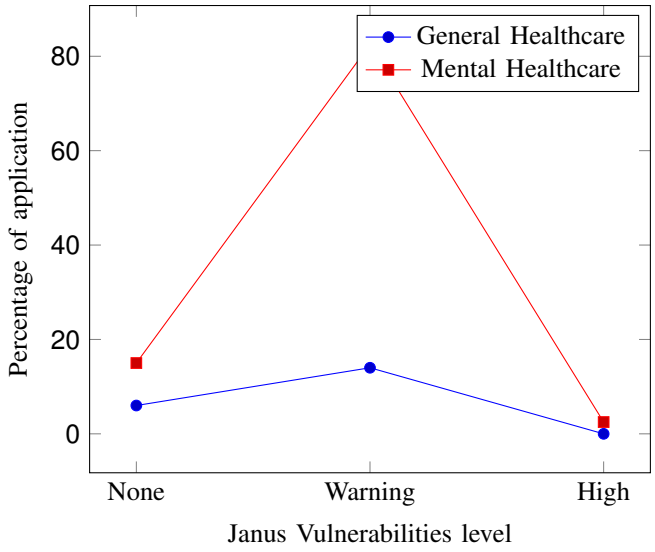

Fig. 7. Snapshot of Janus vulnerability for General and Mental Healthcare applications

4) Analysis of Vulnerabilities: Vulnerabilities are threats to the system and need to be identified, studies and resolved as soon as possible. MobSF provides vulnerabilities with the impact so that the applications can classify between high, warning and low. From the analysis of the report, there are two vulnerabilities highlighted which is Janus and High Collision. There are no high Janus vulnerabilities found in the general healthcare applications whereas 2.5% of the mental healthcare applications have high Janus vulnerability. 14% of the general healthcare applications are under the warning category for Janus whereas 82.5% of mental healthcare applications are issued warning for the vulnerability. The other vulnerability reported in the report is Hash Collision where 4% of the general healthcare applications come under high category and 5% of the mental healthcare applications are tagged as high for the vulnerability. More than 50% of the mental healthcare application do not have this vulnerability and 37.5% are issued warning. 12% of the general healthcare applications do not have hash collision reported in the report and only 4% are issued warning.

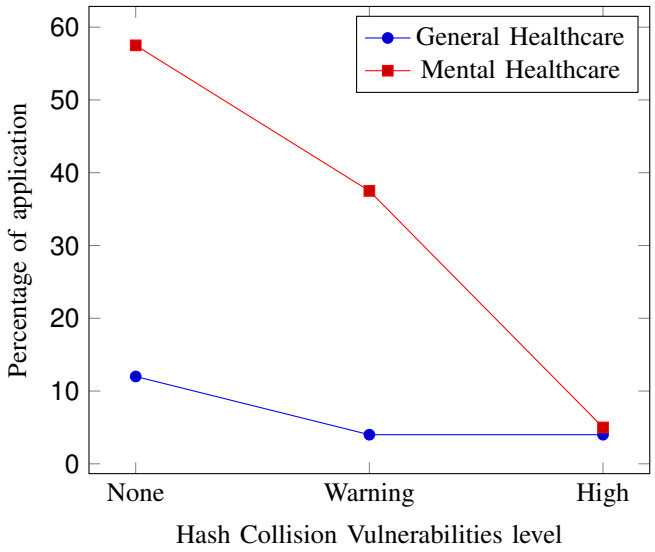

Fig. 8. Snapshot of Hash Collision vulnerability for General and Mental Healthcare applications

5) Analysis of Permissions: Permissions in the mobile application drives the access control of who can access what. MobSF provides a detailed analysis of the permissions that can be dangerous, normal to the users in terms of security. From the report, top three dangerous permissions in both general and mental healthcare applications is Storage, Camera and Location access respectively. Storage tops the chart with 80% in mental healthcare and 90% in general healthcare. Camera access for both the applications is at second position with 70%. 50% of the mental healthcare applications and 60% of the general healthcare applications have location access enabled. Recording Audio permission in mental healthcare application is double the percentage in general healthcare. Accessing phone state is similar in both general and mental healthcare applications and is at fifth position in terms of ranking. 40% of the applications have account and contact related access in general healthcare applications but in mental healthcare it is 17.5% and 15% respectively. There are no applications in general category have SMS and body sensor permissions activated whereas 2.5% of mental health applications provide these permissions. Activity recognition, use credentials, system alerts, phone calls permission used by the applications is less than 20% in both general and mental healthcare.

6) Shared Library Binary Analysis: Apart from the permissions, certificates and vulnerabilities we also need to focus on the code of the application. MobSF provides a detailed analysis of the libraries and code used to identify any weaknesses in the application. There are 4 applications who have received B rating in the general healthcare application category. All of these applications have less high severity risks and have decent amount of medium severity risks.In case of mental

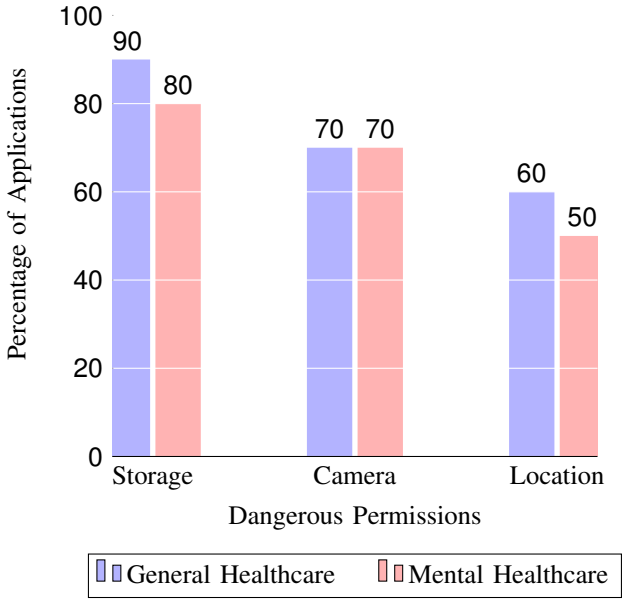

Fig. 9. Top three Dangerous Permissions from MobSF tool

healthcare applications, 22 applications have received B rating and there are few high risks identified overall. The shared library binary analysis section provides issues identified in the code of the application. From mental health application perspective there are warnings issued in the code but very few critical changes are highlighted by the tool. After analysing the F rating applications, it is observed that mental healthcare applications and general healthcare applications have high severity risks in the code and there are network security issues also that need to be fixed.

VI. Discussion

1) Mental Healthcare Websites: The results from the SSL labs analysis showed very promising results in terms of security. With the lowest score being a B, and 64.58% of sites scoring an A or A+, we were able to conclude that popular healthcare websites followed overall strong security protocols. All of the websites we analyzed were HIPAA compliant from a web security standpoint. We did notice that 52.94% of those that scored B had their grade capped to such due to the usage of TLS 1.1 or 1.0, due to the known vulnerabilities of these two versions.

Every site we analyzed took precautions against some of the most known website attacks such as; BEAST, POODLE (SSLv3 and TLS versions) Zombie POODLE, GOLDENDOODLE, OpenSSL 0-Length, and Sleeping POODLE. This is a very good sign as it showed companies taking at least the most basic prevention was commonplace. The most common issue outside of TLS protocols was the fact that 8.33% of sites had weak key exchange for forward secrecy, and 4.17% only supported forward secrecy with some browsers. Additionally, we found that 10.42% of sites reused the same DH key value for multiple handshakes. We also found that 22.92% of sites did not support strict transport security whereas 2.08% of sites had HSTS disabled. While all of these vulnerabilities are widespread and should be addressed, they are not dire threats to the security of a site. Overall, we found that sites who did not score an A or A+ either used TLS 1.1, 1.0, or had one of the above vulnerabilities.

The most concerning vulnerability found was on the DU HCC site which utilized RC4. This is concerning because the stream cipher's vulnerabilities are well known and have been known for several years. This poses a serious threat to the security and confidential of information that is being accessed and transferred from the site. RC4 should never be used in the general healthcare environment. Considering the site is used for all of the DU students' physical and mental healthcare means this issue affects a large group of people and contains extremely sensitive information.

2) Mental Healthcare Mobile Applications: Mental healthcare is an important aspect for users because they use the service to get mental health support. With pandemic there has been a surge to get these services online through mobile applications. There are many mental healthcare applications in the market that are used to assist patients. However the important aspect here is the way these applications have been designed with respect to privacy and security. Users share their personal and sensitive information which can be dangerous if the applications do not implement stringent security measures.

The average application security score of all the 40 applications is 41.6 which is relatively low as compared to websites. There are some known vulnerabilities that are still prevalent in applications that can cause attacks and loss of data.The overall security score of the mental health application is moderate as the highest score received is 73. Only 2 application got A rating which is concerning as mental healthcare application is being used by the users who need mental health support. There are 5 applications who got F rating which is alarming in terms of security and privacy. The lowest score is 20 for few applications that needs review thoroughly to understand the issues in depth and fix them.

Additionally, 80% of the applications give access to internal and external storage that can result in compromising the CIA of cyber security. The top three permissions which appeared in the applications is storage, camera and location access respectively. 50% of the apps give location access resulting in users of the application getting tracked. Even accessing the accounts can be dangerous as attackers can enter the system as an authorized user and perform malicious activities. But in case of using credentials, 10% of the applications are allowing this which is a high risk scenario as allowing the credentials to be stored so that the user does not have to sign in can cause severe repercussions.

Apart from all the above, the applications are using SHA1 and SHA256 with RSA algorithm for certificates alongwith v1, v2 and v3 signatures. Also the key bit size used by the applications is between RSA 1024 to RSA 4096. All of the mental healthcare applications use signed certificates for authentication which ensures security of the application. In terms

of vulnerability, almost all the mental healthcare applications have resolved the vulnerability or are given warning. There are only few of them who are placed in high category for the janus and hash collision vulnerability. More than 50% of the applications have removed hash collision and and 37.5% have issued warning.

From the results mentioned above, MobSF analysis tool gives a decent picture of mental healthcare mobile applications in terms of security and privacy. There is still a long way in implementing stringent security measures to safeguard the applications. After analysing the results it is advised that mental healthcare application need to implement strict security measures to protect the users data. There is a need for these applications to implement safe techniques and algorithm so that the CIA triad of security is maintained.

3) Case Study- Mental and General Healthcare Applications: Telehealth services are being used widely today as digitization of services is growing. In healthcare domain, general healthcare services are provided for assisting users with their queries. With pandemic users are not only demanding general healthcare services but also need mental support service online. Getting mental help online requires users to share their personal data with the application which raises security and privacy risks. So we conducted a case study to understand the differences in terms of security and privacy in mental healthcare and general healthcare applications.

After analysing the results, there are few significant differences between general and mental healthcare applications in terms of security and privacy aspects:

- There is no application who have received A rating in the general healthcare whereas there are 2 applications in mental healthcare that are following security and privacy measures. It is alarming because the security score of the general healthcare applications is not more than 51. In case of mental healthcare application the highest score is 73 which is still concerning.
- Trackers detection is one of the aspect that MobSF tool provides to see if there is any airtag that can monitor the users. The average score is less in both general and mental healthcare which is the good part.
- In terms of vulnerabilities, MobSF detects two vulnerabilities- Janus and Hash Collision. Both of them are severe and needs to be resolved as soon as possible. For mental healthcare applications, only 2% of the applications have high threat whereas more than 80% are issued warning which is considered normal. Mental healthcare overall are good in handling vulnerabilities than the general healthcare services.
- After analysing the permissions, top three dangerous permissions are same for both general and mental healthcare applications. Storage tops the list which is alarming because providing access to storage other than the users can lead to malicious activities. Another permission which is concerning and is ranked high in both the application is providing camera and location access which can be harmful to users as sharing personal content from the phone and getting tracked could lead to attackers getting personal information. The overall ranking of dangerous permissions is similar in both general and mental healthcare so it is very much important to analyse these and rectify it as soon as possible.
- Certificates is one of the aspect that need to be checked while developing the applications. MobSF provides all the details of the certificate including the key size, encryption algorithm, signature scheme used, whether it is signed or unsigned. From the report, we can say that both general and mental healthcare applications use SHA1 and SHA256 RSA algorithm for encryption. However, 10% of the general healthcare applications use MD5 with rsa algorithm. One more similarity is that all the applications are signed and use the same signature schemes.

VII. Implication

According to our findings there are number of security concerns about the security and data protection in the websites and mobile apps that are used in the mental and general health care services. In this sections we are giving our recommendations for those concerns.

- First, one of our mainly concerns is about The DU HCC's use of the RC4 cipher which is major security flaw we found in our analysis. An improvement can be seen in some SSL protocols that have been upgraded to TLS1.2, which do not use the stream cipher RC4 algorithm [44]. However, they continue to use RC4 with TLS1.0 and TLS1.1, which is extremely dangerous. Because RC4 stream ciphers are known to be weak ciphers in SSL. RC4 should be disabled for all SSL and TLS versions if an organization isn't using TLS1.2 or higher [44]. We recommend that DU HCC disable them in all SSL and TLS versions if it does not upgrade all protocols to use TLS1.2 or higher.
- Second, According to our findings, about quarter of the mental health care websites are using TLS versions older than 1.2. These versions lack the cryptographic protocols and algorithms current and recommended by the industry [45]. Considering the sensitive nature of the data being utilized in the mental healthcare field, it is highly recommended that websites upgrade to TLS 1.2 at least, and drop support for older version. Additionally, we would recommend that site administrators pay close attention to which version of web security protocols to update to, so as to stay ahead of the majority of cyber attacks.
- Third, we would highly recommend a wider support for forward secrecy. With 8.33% of browsers supporting forward secrecy with only modern browsers, 8.33% supporting forward secrecy with a weak key exchange, and 4.17% only supporting it with some browsers, this gives some concern for users who utilize uncommon browsers. Healthcare organizations need to account for a very diverse group of users as health issues of varying degrees affect every human at some point in their life.

As a result of diverse users, there will likely be diverse browsers being utilized, and thus support for security with these browsers from the server-end is necessary.

- Fourth, in terms of general and mental healthcare applications the permission need to be analysed. The ranking provided by the MobSF tool is alarming and the applications need to look into the access control of the application. Access to storage, camera, location, accounts, phone contacts or body sensors need to be minimized and given only to the authorized users.
- Fifth, we would recommend the applications who have been detected with hash collision and janus vulnerabilities to look into the application and resolve them as soon as possible. Janus vulnerability is severe as it updates the APK file and can insert malicious code into the application. Hash Collision is also severe where hash table has the exact same value for input.
- Sixth, we noticed that 42.5% of the mental healthcare applications and 40% of general healthcare applications are using SHA1 with RSA which is a risk and increases the chances of hash collision attacks. It is recommended to use SHA256 with RSA which is much more safe than SHA1.
- Seventh, 40% of the general healthcare applications and 27.5% of the mental healthcare applications are using key bit size of 1024 which can help attackers easily attack the application in case the encryption algorithm is SHA1 with RSA. It is advised that the key bitz size used should be RSA 2048 or RSA 4096 as it increases security overall.

VIII. Limitation and Future work

During this research, the researchers faced a tight time frame, since we needed to complete all steps of the research and compile the findings within a certain amount of time. It is a heavy workload and time-consuming process to review all the websites, web services, and mobile applications and analyze each one of them individually and write the findings, and then analyze everything that was done. To resolve this issue during the process of extracting the data, we performed a critical analysis only on those most important and critical security measures on the servers of the primary list of the health care services. The other limitations will be expanded upon in future research pertaining to this research area. We would be able to collect more comprehensive information regarding the security vulnerabilities of healthcare services if we investigated a wider selection of testing into the applications and web services. Whenever it comes to conducting research, there is no question that having enough data is essential for a quality study. As a consequence, one of our major goals in our future work will be to expand the list of our primary health services to analyze them.

Various wireless devices and IoT devices are coming onto the market for various diseases, and these devices contain algorithms that analyze the data to identify challenges and countermeasures for each disease [24]. The data generated by sensors and devices of this type can be used for a wide range of purposes by a variety of participants, such as medical professionals, patients, relatives, and health care facilities, allowing them to provide remote assistance. Nevertheless, the major challenges lie primarily in being able to find a secure channel to facilitate data exchange between different types of devices produced by different providers. One of our goals in the future work is study the communication channels in addition to investigating the vulnerabilities of sensors and hardware devices incorporated into healthcare services and connected to different web-servers and mobile application in the health industry.

IX. Conclusion

The use of websites, web services, and mobile applications has gained momentum in the mental and general health care industry and it is now widely used by healthcare providers and patients alike. Although these electronic services have been well received by users, privacy concerns have been raised about their management of personal data. In fact, the websites, web services, and mobile applications that used in mental health care dealing with mental health-related information, which are considered extremely confidential and strictly protected by national and international laws. There has been a greater emphasis on these concerns when it comes to mental health data.

In this paper, we conduct a full scale evaluation of the mental and general healthcare data protection required by a list of 98 websites, web services, and mobile applications services in total. These services were thoroughly tested and their behavior analyzed. Additionally, we conducted a case study to compare 10 general health services, these that specifically examined how the general health care data in these services is accessed. we analyzed each electronic service individually then combined the results together to build our findings and then write our recommendations. We used automated online tools to evaluate each of the electronic health services according to their type; we used the SSL lab tool to evaluate the websites and web services, and MobSF to evaluate the mobile applications. We focused on specific security measures to evaluate the security and data protection in each of the electronic health services of our primary list. As a result of our research, mental healthcare websites adhere to strong security protocols. Moreover, we verified that all the sites we tested took precautions against the most well-known website vulnerabilities. Mental healthcare mobile applications need to work on the way permissions are handled and encryption algorithm used for certificates. Furthermore, the findings of our case study on mental and general healthcare services indicate that both general and mental health service applications demonstrate satisfactory security.

X. Acknowledgments

The authors would like to express their gratitude to our primary supervisor and teacher, Dr. Sanchari Das, for her assistance with this document. We would also like to thank

the University of Denver for giving us the opportunity to study this topic.

REFERENCES

[1] C. K. Reddy en C. C. Aggarwal, Healthcare data analytics, vol 36. CRC Press, 2015.

[2] C. Esposito, A. De Santis, G. Tortora, H. Chang, en K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?", IEEE Cloud Computing, vol 5, no 1, bll 31–37, 2018.

[3] H. K. Patil en R. Seshadri, "Big data security and privacy issues in healthcare", in 2014 IEEE international congress on big data, 2014, bll 762–765.

[4] N. Terry, "Existential challenges for healthcare data protection in the United States", Ethics, Medicine and Public Health, vol 3, no 1, bll 19–27, 2017.

[5] E. McCann, "Kaiser reports second fall data breach," Healthcare IT News, 2013.

[6] Verizon, "Data breach investigation report," Verizon, 2013.

[7] P. Institute, "Third Annual Benchmark Study on Patient Privacy and Data Security," Ponemon Institute LLC, 2012.

[8] "Public Law 111 - 148 - Patient Protection and Affordable Care Act," U.S. Government Printing Office (GPO) , 2013.

[9] "Health Insurance Portability and Accountability Act,"U.S. Government Printing Office, 1996. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW104publ11/html/PLAW-104publ191.htm.

[10] "Health Information Technology for Economic and Clinical Health Act," 2009. [Online]. Available: http://www.gpo.gov/fdsys/pkg/BILLS111hr1enr/pdf/BILLS-111hr1enr.pdf.

[11] R. Fielding et al., "Hypertext transfer protocol–HTTP/1.1". RFC 2616, june, 1999.

[12] T. Dierks, C. Allen, en Others, "The TLS protocol version 1.0". Citeseer, 1999.

[13] T. Sontakke, A. Kesharwani, en D. Mallappa, "Study of SSL/TLS Attacks".

[14] Y. Suga, "Status Survey of SSL/TLS Sites in 2018 After Pointing Out About "Search form" Issues," 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), 2018, pp. 483-485, doi: 10.1109/CANDARW.2018.00093.

[15] D. Özden, "Analysis of recent attacks on SSL/TLS protocols", Uygulamalı Matematik Enstitüsü, 2016.

[16] B. Möller, T. Duong, en K. Kotowicz, "This POODLE bites: exploiting the SSL 3.0 fallback", Security Advisory, vol 21, bll 34–58, 2014.

[17] A. Satapathy en J. Livingston, "A Comprehensive Survey on SSL/TLS and their Vulnerabilities", International Journal of Computer Applications, vol 153, no 5, bll 31–38, 2016.

[18] J. Selvi, "Bypassing HTTP strict transport security", Black Hat Europe, vol 54, 2014.

[19] J. Hodges, C. Jackson, en A. Barth, "Http strict transport security (hsts)", URL: http://tools. ietf. org/html/draft-ietf-websec-strict-transport-sec-04, 2012.

[20] M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni, en L. Spalazzi, "Certificate Validation Through Public Ledgers and Blockchains", in ITASEC, 2017, bll 156–165.

[21] J. Du, X. Li and H. Huang, "A Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction," 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2011, pp. 445-448, doi: 10.1109/IMCCC.2011.117.

[22] Ristić,, I., 2022. Qualys SSL Labs. [online] Ssllabs.com. Available at: ¡https://www.ssllabs.com/¿ [Accessed 21 February 2022].

[23] S. P. Kumar en R. Subramanian, "An efficient and secure protocol for ensuring data storage security in cloud computing", International Journal of Computer Science Issues (IJCSI), vol 8, no 6, bl 261, 2011.

[24] I. Jayatilleka en M. N. Halgamuge, "Internet of things in healthcare: Smart devices, sensors, and systems related to diseases and health conditions", in Real-time data analytics for large scale sensor data, Elsevier, 2020, bll 1–35.

[25] G. LaMalva en S. Schmeelk, "MobSF: Mobile Health Care Android Applications Through The Lens of Open Source Static Analysis", in 2020 IEEE MIT Undergraduate Research Technology Conference (URTC), 2020, bll 1–4.

[26] D. Gökçeoğlu en Ş. Doğan, "Malware Analysis on Android Devices-Dynamic Analysis", PROCEEDINGS BOOKS, bl 45.

[27] M. M. H. Henchiri, "Handles for Pentesting Modern Secure Coding: bypassing mobile security", International Journal of Engineering and Information Systems (IJEAIS), vol 3, no 4, 2019.

[28] N. Kohli en M. Mohaghegh, "Security Testing Of Android Based Covid Tracer Applications", in 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, bll 1–6.

[29] S. Arzt et al., "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps", Acm Sigplan Notices, vol 49, no 6, bll 259–269, 2014.

[30] I. de la Torre Díez, M. Antón-Rodríguez, en F. J. Díaz-Pernas, "Mobile Web Application Development to Access to Psychiatric Electronic Health Records", in Telemedicine Techniques and Applications, IntechOpen, 2011.

[31] B. Mahapatra, R. Krishnamurthi, en A. Nayyar, "Healthcare models and algorithms for privacy and security in healthcare records", Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions, bl 183, 2019.

[32] M. Anwar, J. Joshi, en J. Tan, "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges", Health Policy and Technology, vol 4, no 4, bll 299–311, 2015.

[33] C. Véliz, "Privacy and digital ethics after the pandemic", Nature Electronics, vol 4, no 1, bll 10–11, 2021.

[34] H. K. Patil en R. Seshadri, "Big data security and privacy issues in healthcare", in 2014 IEEE international congress on big data, 2014, bll 762–765.

[35] E. P. Morera, I. de la Torre Díez, B. Garcia-Zapirain, M. López-Coronado, en J. Arambarri, "Security recommendations for mHealth apps: Elaboration of a developer's guide", Journal of medical systems, vol 40, no 6, bll 1–13, 2016.

[36] W. Wang en K. Siau, "Trust in health chatbots", 2018.

[37] L. Nurgalieva, D. O'Callaghan, en G. Doherty, "Security and privacy of mHealth applications: a scoping review", IEEE Access, vol 8, bll 104247–104268, 2020.

[38] S. F. Jacoby, J. A. Rich, J. L. Webster, en T. S. Richmond, "'Sharing things with people that I don't even know': help-seeking for psychological symptoms in injured black men in Philadelphia", Ethnicity & health, vol 25, no 6, bll 777–795, 2020.

[39] A. N. Winnike en B. J. Dale III, "Rewiring mental health: Legal and regulatory Solutions for the effective implementation of Telepsychiatry and Telemental health care", Hous. J. Health L. & Pol'y, vol 17, bl 21, 2017.

[40] W. J. Winslade en J. W. Ross, "Privacy, confidentiality, and autonomy in psychotherapy", Neb. L. Rev., vol 64, bl 578, 1985.

[41] L. Parker, V. Halter, T. Karliychuk, en Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices", International journal of law and psychiatry, vol 64, bll 198–204, 2019.

[42] A. Razaghpanah et al., "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem", in The 25th Annual Network and Distributed System Security Symposium (NDSS 2018), 2018.

[43] K. Bennett, A. J. Bennett, en K. M. Griffiths, "Security considerations for e-mental health interventions", Journal of medical Internet research, vol 12, no 5, bl e1468, 2010.

[44] T. D. B. Weerasinghe en C. Disanayake, "A research study: usage of RC4 stream cipher in SSL configurations of web servers used by Sri Lankan Financial Institutes", Int J Cyber Secur Digit Forensics, vol 7, no 2, bll 111–119, 2018.

[45] K. Moriarty en S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", Internet Engineering Task Force, RFC, vol 8996, 2021.

[46] S. Khan, S. Khan, en M. Aftab, "Digitization and its impact on economy", International Journal of Digital Library Services, vol 5, no 2, bll 138–149, 2015.

[47] M. Feijt, Y. De Kort, I. Bongers, J. Bierbooms, J. Westerink, en W. IJsselsteijn, "Mental health care goes online: Practitioners' experiences of providing mental health care during the COVID-19 pandemic", Cyberpsychology, Behavior, and Social Networking, vol 23, no 12, bll 860–864, 2020.

[48] S. D. Kauer, C. Mangan, en L. Sanci, "Do online mental health services improve help-seeking for young people? A systematic review", Journal of medical Internet research, vol 16, no 3, bl e3103, 2014.

[49] M. Young, C. Richards, en M. Gunning, "Online mental health resources for teenagers: an evaluation of two websites developed for adolescents",

Advances in School Mental Health Promotion, vol 5, no 4, bll 277–289, 2012.
[50] E. Oh, A. F. Jorm, en A. Wright, “Perceived helpfulness of websites for mental health information”, Social psychiatry and psychiatric epidemiology, vol 44, no 4, bll 293–299, 2009.
[51] D. L. Cavanaugh, J. Riebschleger, en J. M. Tanis, “Mental health literacy websites for children of parents with a mental illness”, Clinical Child Psychology and Psychiatry, vol 26, no 3, bll 720–733, 2021.
[52] X. Wang, C. Markert, en F. Sasangohar, “Investigating popular mental health mobile application downloads and activity during the COVID-19 pandemic”, Human Factors, bl 0018720821998110, 2021.
[53] R. Grist, J. Porter, P. Stallard, en Others, “Mental health mobile apps for preadolescents and adolescents: a systematic review”, Journal of medical internet research, vol 19, no 5, bl e7332, 2017.
[54] J. H. L. Lui, D. K. Marcus, en C. T. Barry, “Evidence-based apps? A review of mental health mobile applications in a psychotherapy context”, Professional Psychology: Research and Practice, vol 48, no 3, bl 199, 2017.
[55] J. De La Cruz en M. Bradley, “Philips Hue Bulb & IoT App Security ”.
[56] . Müthing, R. Brüngel, C. M. Friedrich, en Others, “Server-focused security assessment of mobile health apps for popular mobile platforms”, Journal of medical Internet research, vol 21, no 1, bl e9818, 2019.
[57] H. E. Michail, G. S. Athanasiou, G. Theodoridis, A. Gregoriades, en C. E. Goutis, “Design and implementation of totally-self checking SHA-1 and SHA-256 hash functions’ architectures”, Microprocessors and Microsystems, vol 45, bll 227–240, 2016.
[58] @inproceedingscamenisch1997efficient, title=Efficient group signature schemes for large groups, author=Camenisch, Jan and Stadler, Markus, booktitle=Annual International Cryptology Conference, pages=410–424, year=1997, organization=Springer