The UK Healthcare Cybersecurity Landscape

MSc Research Project

MSc Cyber Security

Anudeep Kommareddy

x22183850

School of Computing

Nation College of Ireland

Supervisor: Apurva Vangujar

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Anudeep Kommareddy
Student ID:	X22183850
Programme:	MSc Research Project
Year:	2023
Module:	MSc Cybersecurity
Supervisor:	Apurva Vangujar
Submission Due Date:	14/12/2023
Project Title:	The UK Healthcare Cybersecurity Landscape
Word Count:	8074
Page Count:	26

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: Anudeep Kommareddy
Date: 14/12/2023

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):	

Abstract

Anudeep Kommareddy

X22183850

With a focus on authentication plans, the aim of this research is to provide an exhaustive analysis of the current vulnerabilities and potential threats within the UK's healthcare cybersecurity landscape. This study involved the hands-on integration of a 2-factor authentication (2FA) system into health care users' authentication framework. This project intends to enhance User Authentication Security in health care settings through a combination of TOTP algorithm and cryptography especially employing hash function SHA-256. The code depicted the possibility, as well as value addition to an authentications system by introducing a two-factor authentication method. Adding another level of security in the environment proves to be both theoretically and practically possible. It was found that 2FA is a very secure approach that greatly enhances the authentication system security position. This approach reduces the risks associated with password-only authentication by requesting for a second measure, e.g., an OTP from a smartphone app. This approach reduces vulnerability, despite credentials being compromised to avoid unauthorized access. In the future, a thorough study must be conducted on the suitability of using second factor authentication under health care setting. Analysis of the problems of 2FAs in patients' communication with doctors must be based on the usability studies of these 2FA systems in which patients would be involved as actors/participants.

Key Words:

Two-Factor-Authentication, Authorization, Framework, Risk Analysis, Vulnerability

Chapter 1: Introduction

1.1 Background:

A new age of unparalleled breakthroughs in patient care and administrative procedures has been brought about by the integration of technology in the healthcare sector. Technological advancements such as cloud-based infrastructures, internet of things (iot), and electronic health records have been crucial components of modern healthcare systems in the past decade. The said advancements have enabled health delivery service to be effective and readily available but with the problem of cyberattacks as an example. In addition, the quick adoption of EHR reveals how much the health industry depends on technologies. Healthcare has begun to digitally-centered since the inception of this concept and there is no reason why it should not be maintained for the future in such way. The cyber security loopholes manifested in the area of health care have exposed vulnerable information such as patient's confidential data. In addition to this, the health industry relies heavily on networked medical equipment, including pacemakers and infusion pumps. These products may be crucial for the treatment or nursing and yet, become subjected to cyberattacks via IoT. The issues of unauthorized access / manipulation / interruption threatening patient safety must be prevented by ensuring Medical device cyber security. Cybersecurity is an important defensive measure in defending the rampant ransomware threat facing the health industry. Alharam and Elmedany (2017) underscore how ransomware affects healthcare companies. The cyber criminals now encrypt some of this information and demand money before unlocking it. These assaults can also result into compromising the patient care and safety because their services are very crucial for healthcare. Legal and regulatory requirements further point out the importance of cybersecurity in the healthcare industry.

The United States' Health Insurance Portability and Accountability Act (HIPAA) and the European Union's General Data Protection Regulation (GDPR) require that healthcare corporations observe data protection regulations. As per Chua and Pmp (2021), compliance failure does not just pose a legal risk, but also impairs the professional image of clinicians, while undermining the public trust. Additionally, it provides increased exposure of the vulnerable areas by seeking services outsourced from other providers in the health sector. Cloud storage and external entities handling data such as telemedicine providers might not have similar stringent security policies to those of the respective healthcare company hence posing dangers to the data.

1.2 Research Aim:

This paper examines how the current authentications schemes are vulnerable to various security risks in the UK's health care industry and other sectors. Integrating modern technology in an ever increasingly digitalized healthcare system raises both prospects and issues on one hand with special regard to security of confidential medical information and trustworthiness of health care services.

This study intends to perform a comprehensive evaluation of the current weaknesses in healthcare's cybersecurity framework. This study seeks to offer an advanced understanding of the risks facing healthcare institutions in today's digital environment through the identification, categorization and ranking of some specific threats, weaknesses and access points. By conducting this research, it is expected to publicize key vulnerabilities as a foundation for targeted risk mitigation measures towards cybersecurity.

In addition to analyzing current weaknesses, this study seeks to anticipate and understand prospective dangers that could surface in the health care digital security space. This study seeks to shed light on what the evolving characteristics of cyber security threats to healthcare are, what technologies involved, what do we expect in terms of changing modus operandi with regard to cyberattacks. Healthcare companies should adopt an active strategy for mitigating potential dangers to their information systems.

The relevance on UK health care cybersecurity will also be analyzed in this study together with some other issues. Authentication is important for denying unnecessary access of private health care information and data. Research has led to an evaluation of current authentication methods such as multi-factor authentication, biometrics and access controls. The last goal is to make recommendations on the enhancement of authentication procedures so as to ensure robust security environment throughout health care systems.

The research seeks to achieve those goals in order to continue the discussion on healthcare information systems cybersecurity and offer evidence-directed guidelines on policy making and best practice implementation in this arena. The study, therefore, aims at comprehensively investigating vulnerabilities that relate to information systems security, possible threats and authentication processes to create a safest and most robust care environment. It also ensures the confidentiality, integrity, and availability of important patient data in the digital age.

1.3 Research Objectives:

The research has the following objectives:

- To analyze the current vulnerabilities in the UK healthcare cyber security landscape.
- To examine the future threats and authentication scheme in the UK healthcare cyber security landscape.

1.4 Research Question:

- What are the specific risks, vulnerabilities and entry points in the current healthcare cyber security architecture in the UK, and how can they be ranked and prioritized?
- How can trends, technical developments and evolving cyberattack techniques be analyzed to anticipate and comprehend potential future threats in the healthcare cyber security domain?

1.5 Research Significance:

This research is particularly relevant, if one is to consider how healthcare cybersecurity is evolving in the UK or anywhere else indeed. As health information management systems advance, digital technology becomes more critical in improving patient care, the monitoring of public health, and overall operational efficiency. Thus, it is important for administrations to understand and address potential vulnerabilities that can affect such system implementation. Investigating present vulnerabilities is invaluable for exploring the risks that now confront health facilities and warning about potential hazards enabling development of specific counter measures. Providing for the security of healthcare system today should also take into account possible future dangers.9 The research supports a proactive cybersecurity framework through anticipating new and developing cyber threats and vulnerabilities. This proactive approach may enable healthcare firms to introduce preventive measures designed to withstand dynamic cyber threats. In this area, the findings of the study would assist in allocating resources and strategies to effectively address any looming threat.

Therefore, it is important for assessing authentication schemes to improve the overall security posture within UK's healthcare cybersecurity environment. In the health care industry, strong authentication approaches need to be deployed to avoid unauthorized access to patient records data. These suggestions will guide better authentication procedures as well as push other advanced technologies and methods for adoption. This contributes to creating a trustworthy and secure virtual setting for patients and healthcare professionals alike.

Chapter 2: Literature Review

Medical advances in the past ten years have contributed a lot by providing better treatment and easily accessible lifesaving information in the sector. Nevertheless, it has become easy prey for malicious threat agents through the extended interoperability and the overwhelming use of cloud infrastructures resulting from these changes (Coventry & Branley, 2018).
IoMT has led to an explosion in the number of PII that is stored in hospitals. This coupled with poor security measures taken by most hospitals, demand for transparent data in hospitals and low level of staff education on cybersecurity expose hospitals to high risk situations, in general (Tully et al ,2020)

Moreover, the increased usage of remote medical technology also introduces additional vulnerabilities. For threat actors wishing on getting health information, they always have an extra way in these devices that typically lack even basic security tools and can never be updated. Cyber attacks could have catastrophic consequences for healthcare. Such actions may deny patients their basic rights to get immediate and lifesaving treatment resulting in avoidable deaths. The interruptions are likely to affect patient data, surgical services, medical equipment, as well as the appointment system. With these ever-evolving and rising cyber threats, it is imperative that healthcare systems and patient information are protected.

2.1 Current Vulnerabilities:

Security Vulnerabilities in Medical Devices

One of the leading vulnerabilities in healthcare cybersecurity is the security of medical equipment. As asserted by Strielkina et al. (2018), many medical equipment such as pacemakers, implantable cardiac defibrillators, and insulin pumps currently possess limited or no safety measures. This makes them susceptible to being compromised, which could endanger patients' lives. Bad actors gain unauthorized access to network security devices through improper encryption and authentication methods.

Mitigation

Healthcare companies need to prioritize a comprehensive strategy to mitigate their critical vulnerability, as evidenced by the example of medical device security. Firstly, they should be authenticated strictly using two factor or even biometric authentication in the best case scenario. Therefore, there should be collaboration with device manufacturers to improve security standards, conduct detailed threat evaluations and train patients as well as clinicians in proper utilization and management of safety standards for device operation.

Electronic Health Records (EHR) Data Breach

Despite being used for modern health, EHRs also have weaknesses. Chau and PMP (2020) noted weakness in protecting EHR systems' integrity of information leading to malfunction, inaccuracies, and cybersecurity vulnerabilities which may create a pathway for data breach. These violations occur mainly due to unauthorized access, insufficient encryption, and weak authentication processes. Such breaches endanger the integrity and safety of patient data.

Mitigation

In case a third party is suspected, you should employ enhanced methods of access control such as role-based permissions and allow only people authorized to access patient data. Hence, strong encryption techniques, for instance, the end-to-end encryption could be used for protection of the data in transit as well the data at rest. Additionally, security is enhanced through improved authentication methods via multifactor authentication or biometrics. As such, it is important to ensure that EHR will have regular security audits, address issues with vulnerability as fast as possible, and train its workers on how to take care of data security (Chua & PMP, 2020).

Ransomware Offenses

There has been a notable increase in cases of ransomware attacks within the healthcare industry. Coronado, Wong (2014) emphasized on how ransomware attacks affect healthcare institutions. The cyber criminals use ransomware that encrypts sensitive patient data and in turn demand for their payment to decrypt it. Many times hospitals and other health care facilities are forced to pay ransoms just so that they can be restored access to important patient information.

Mitigation

Strong cybersecurity defenses, such as sophisticated firewalls and intrusion detection systems, may assist in locating and preventing ransomware infection. Regular off-site and on-site data backups provide an essential means of recovery without giving in to blackmail. In addition, thorough employee training programs that teach them to spot phishing scams and other attack vectors are essential for keeping ransom ware from taking hold (Coronado and Wong, 2014). To effectively contain and recover from an assault without caving in to cybercriminals' demands, a well-coordinated incident response strategy is essential for protecting sensitive patient data and upholding the integrity of the company.

IoT Device Security Issues

Another set of vulnerabilities are brought about by the growth of Internet of Things (IoT) devices in the healthcare industry. The absence of adequate security protections in many IoT devices was noted by Chen and Wang (2017). Such as outdated firmware, insecure passwords, and non-encryption. These devices can also be hacked and enable access into a bigger healthcare network.

Mitigation

This is essential in reducing risk of IoT devise into the health care industry. The first step involves having a unique, hard-to-guess password and activating the second factor verification for all devices. This allows for end-to-end encryption, thereby preventing nefarious actors from intercepting communication with the data. Security patches and firmware should be diligently applied by device vendors from time to time. Network segmentation, a form that separates the IoT devices from the critical healthcare systems, provides an extra layer of protection. The defense is enhanced by regular penetration tests and vulnerability assessments reducing the likelihood of health care cybercriminals using such devices to access private healthcare networks.

2.2 Future Anticipation:

RaaS is expected to overtake others' operations and take the lead as cybercriminal organizations will use it. With the present technology utilized in ransomware attacks, this approach will make attribution harder and identify the perpetrator impossible (Abraham et al., 2019). There were assumptions that cybercriminal gangs would become more agile, thereby enabling them to take advantage of vulnerabilities in not more than 24 -48 hours following the publication of proof of concept. Studies show that this information is vital, especially because hackers go straight to blackmailing healthcare institutions without engaging their investigative and forensic aspects.

Due to the rapid expansion of cybercrime and the substantial ransomware payments, organized and skilled criminal gangs are predicted to make significant R&D investments and create new strategies for automating and executing frauds. To carry out efficient and successful criminal campaigns, the criminals will make use of deep fakes, artificial intelligence, and machine learning (Wang and Jones, 2019).

Artificial Intelligence and Machine Learning in Healthcare Cybersecurity

Combined AI and ML promise a bright future for healthcare cybersecurity. As per Panesar (2019) and other academics, AI-based solutions would be vital in determining potential dangers and responding accordingly. Machine learning algorithms can analyze large datasets in order to identify trends and aberrations that will enable better pro-active cyber security operations. Also, the scalability of AI and ML technology becomes very important when handling the huge volumes of healthcare data that continues to grow in quantity every day. Handling and evaluating large amount of data created by health care systems gets very crucial for machine learning algorithms (Parashar et al. p. 457). This is where AI comes in handy as quick and precise danger detection alongside efficient data analysis for bulk records is key to an expanding digital healthcare sector.

Drydale et.al (2016) show that healthcare cybersecurity and AI integration are closely related. Furthermore, these benefits may exceed technical dimensions and affect operations and health care business strategy as well. The program provides additional security functions for current cybersecurity systems allowing for an adaptable, alert, and intelligent defensive response as the realm of cyber threats continues to evolve dynamically. Moving to AI based healthcare cybersecurity marks the beginning towards ensuring core values of patient care and information integrity during this digital age, beyond being just an innovation.

Blockchain Technology for Safe Health Information Administration

Blockchain technology will transform the management of health data. To enhance the safety and honesty of medical records, Hölbl et al. suggest blockchain as a resolution. Block chain can mitigate the risks associated with unauthorized access and alteration of data through an inalterable distributed ledger

One of the key steps in solving a number of problems relating to health care information security is the innovation in health data management made possible with the Blockchain technology. This gives rise to a leading solution which revolutionize the concept of health data security through seminal paper written by McGhin et al. (2019)

Blockchain is a critical part for decentralization in one word. This entails the fact that health data should be divided into several different nodes rather than one unsafe center. Attempts of unauthorized access in such network are highly restricted because compromising one node doesn't put the entire system at stake (Prokofieva & Miah, 2019). The blockchain approach ensures that whatever data gets posted on record can neither be modified nor erased, since for its immutability, it uses cryptographic hashing and consensus approaches.

Blockchain promises a revolutionary impact on health care data management but also has some difficulties to overcome. Such obstructions involve issues of interoperability, expandability and regulating. However, as the blockchain develops in acceptance overtime these concerns may subside.

Zero Trust Security Model Implementation

The Zero Trust Security Model has gained significance in healthcare cybersecurity as a reactive approach. The paper by Tyler and Viana (2021) suggests that Zero trust paradigm can take the place of the traditional perimeter-based security strategy. Every user and device needs to be authenticated again and given permissions under this paradigm on assumption of the presence of threats coming both from inside and outside the network.

Although the Zero Trust Security Model is currently emerging in the framework of healthcare cybersecurity as an exception to the existing model, this statement applies here. According to Garcia and Martinez (2019), this approach is called a novelty tactic which challenges traditional understanding about perimeter security in relation with evolving threats landscape. The essence of Zero Trust is the acknowledgment of risk coming from either side and therefore warranting a complete revamping of how we define security in healthcare (Chen et al., 2020)

The concept of network micro-segmentation is further reinforced in the Zero Trust model. Security relies on smaller autonomous segments of the network instead of using a single all-encompassing approach (Wang et al., 2023). Each segment is handled as an independent trust domain, and a strict less privileged approach is employed to prevent access across segments. Such an architectural modification impedes the horizontal spread of threats across the healthcare network, ultimately reducing the attack surface and minimizing the damage incurred by such threats.

The zero-trust approach is very powerful but there should be a holistic strategy used in implementing it in healthcare industry. It is important that healthcare personnel adopt a zero trust mentality. For the concept to be fully utilized, necessary technological solutions of adaptive access restraints, behavioral analytics, and ongoing monitoring are imperative.

Multi-Factor Authentication and Biometrics

A more resilient authentication environment is needed in healthcare as it transitions into the digital age, and this is spurring the adoption of state-of-the-art security solutions. The biometric authentication and MFA constitute leading edges that work towards solving the weaknesses associated with standard credentials in this paradigm shift. Suleski et al., 2023, on the efficacy of biometrics in authentification and the pivotal role played by MFA towards improving general cyber security attaches great significance to these developments

Such weaknesses of single-factor authentication are the power found at work when an MFA operates. Passwords though highly common as an authentication mechanism can still get compromised via a number of threats such as phishing attacks and also credential theft. Extra authentication procedures and dynamic protection from unwanted access make attacks more difficult, thus minimizing related risks. As stated by Fareed & Yassin (2022), MFA forms the foundation behind reducing dependence on static passwords or credentials thus, increasing health care industry resiliency in terms of security.

The combination of MFA and biometrics is a strong defense measure in healthcare, where the confidentiality of patient information means a lot at stake. These technologies are crucial because they help the industry to promote stronger cybersecurity measures as the landscape becomes more complex. This is why more and more health care firms are embracing digital solutions like integrating MFA on top of biometric authentication that improve efficiency without complications of use for medical staff handling sensitive health data.

Quantum-Safe Cryptography

In preparation for this quantum computing that would have superior powers, the healthcare industry tries to enhance the data safety through studying the quantum-safe encryption. For example, Stefan et al. (2023) and others have pointed out that ordinary cryptosystems can be broken down by an upcoming quantum assault. It is important because it ensures that there will be safe cryptographic keys in future. It is revolutionary in safeguarding the authenticity and privacy of medical information from quantum changes.

Traditional math-based cryptographic techniques provide the foundation of contemporary data security and solve mathematical problems for which conventional processors would only yield bad answers in a short amount of time. However, quantum computers that work using the rules of quantum mechanics make completely different calculations in a very short time. The fully grown quantum computers may be in a position of breaking down the most popular modern cryptographic schemes, posing a serious danger for the safety of encrypted data. According to Mantry &amp; Maheshwari (2022), the healthcare sector needs to adopt quantum safe encryption in order to mitigate security threats. Specially developed post-quantum or quantum-safe cryptographic methods that resist attacks from such quantum computers. Unlike traditional methods, the security of these algorithms is provided by difficult-to-solve mathematical problems, even in the quantum one. Switching to quantum safe encryption, healthcare industry prepares to protect confidential patient information from potential threat of quantum computing. Quantum-safe cryptography, if well utilized in encryption of healthcare data will have a long term impact on its functionality and security. As quantum computing technology develops, the healthcare industry must continue to work to create improved and advanced encryption protocols that will withstand the specific challenges brought up by quantum algorithms. In order to create strong quantum-safe cryptographic frameworks that meet the changing requirements of healthcare cybersecurity, cooperation between researchers, business experts, and legislators is essential.

Cybersecurity Integrated into Healthcare Culture

Besides technical improvements, scholars highlight the importance of building cybersecurity-awareness culture within healthcare companies. Based on the study by Pollini et al (2022), future ***cyber security*** initiatives need to incorporate continuous education and sensitization of health workers. The inclusion of all stakeholders in the awareness and mitigation of cybercrime is deemed essential as part of a preventative measure for social engineering based attacks. ***Cyber security*** being an integral part of the health care culture. Uchendu et al.'s deliberated work suggests that a ***cyber security*** conscious culture at healthcare facilities needs broadened approach instead of the technical solutions only. This means that a cybersecurity policy can only be effectively and efficiently implemented with the involvement of a proactive and knowledgeable staff who are willing to play an active role instead relying on pure technology that will not suffice for complete ***cyber security***.

However, for this cultural change to materialize it takes leadership commitment as well as cyber security education and awareness programs funding. That is about developing a way of thinking that treating cybersecurity is part of giving quality treatment and not an extra work. Businesses can have a culture of cybersecurity awareness towards managing the complexities of the digital ecosystem, proactively spot potential risk points, and make sure that all healthcare stakeholders feel like second nature to them will foster a proper culture of cybersecurity awareness.

Regulatory Compliance and International Collaboration

Increased expectations on international collaboration and regulations are also some of the future expectations anticipated in the upcoming days. Kwon and Johnson (2013) suggest that healthcare systems become resilient to Transnational cyber attacks through compliance to international cyber security standards and cross-border collaboration.

It remains instructive to reference Al-Alawy et al. (2021) who point to those pillars of effective health care security in the upcoming years: regulatory compliance and partnerships with other nations. The course acknowledges the multinational and intertwined nature of cyber attacks in this regard and includes corresponding anticipations. In this context, maintaining stringent cyber security measures and fostering cross-border coordination will greatly enhance the robustness of health care systems in the face of an evolving global terrain of intercontinental cyber assaults. One aspect of inter-national collaboration in healthcare cybersecurity is setting and enforcing global cybersecurity standards. Such harmonized standards would assure healthcare institutions follow common medical security practices across different locations. It strengthens healthcare sector's cybersecurity stance thus promoting international health informatics interchange and integration. Some guidelines include ISO/IEC 27001, the NISS Cybersecurity Framework, and ENISA Recommendations, which serve as a platform or set up for collaborative efforts between many of these health industry organizations.

In general, there will be changes such as technological developments, social changes, and collaboration at an international level that will define health care security. The application of Artificial Intelligence (AI), blockchain, zero trust security models, improved authentication mechanisms, quantum safe encryption, and cultures that are aware of cybersecurity in strengthening healthcare systems. Such expectations will be instrumental in avoiding new risks that may arise when embracing digital change across industries, maintaining confidentiality of health records, and fortification of healthcare cyber-security frameworks.

2.3 Literature Matrix:

Article Reference	Data Used	Algorithms Compared	Best Results Achieved	Hyperparameter Settings
Pandey et al. (2020)	As their source of data, the	They analyzed the efficiency of	According to the findings of the research,	The particular hyperparameter settings were not

	authors used the cloud-based medical records.	the SHA-256 and HMAC-SHA256 algorithms and compared their results.	HMAC-SHA256 performed better than SHA-256 and reduced the amount of data corruption by 15%.	mentioned in any clear manner.
Ansari et al. (2021)	Logs of financial transactions were used in the analysis of the data's integrity.	The CRC32, MD5, and SHA-3 algorithms were analyzed and compared in this work.	In the analysis of financial transaction logs, SHA-3 showed the best level of data integrity.	The paper did not provide specific details regarding hyperparameter settings.
Gaetni et al. (2017)	The major dataset used for this investigation was made up of genomic information stored in the cloud.	The research analyzed and contrasted the performance of the Merkle Tree algorithm with the Blockchain algorithm.	Blockchain has emerged as the better solution, with a 20% reduction in the amount of data manipulated.	Custom hyperparameter settings were employed but not explicitly detailed.
Li et al. (2019)	The authors looked at the data integrity by using data from Internet of Things sensors.	In this research, the CRC-16 and Adler-32 algorithms were compared against one another.	According to the findings, Adler-32 performed much better than CRC-16 in avoiding data corruption.	The hyperparameter settings were not specified in the study.
Garg et al. (2020)	The information	The algorithms	In commercial database	Custom hyperparameter

	for this research came from business databases that were stored on the cloud.	Rabin-Karp and SHA-256 were under examination for this research.	applications, SHA-256 was able to achieve an astonishing 99.9% data integrity.	settings were applied for optimal performance.
Zhao and Jiang (2020)	The data of users from social media platforms was used in the analysis of data integrity procedures.	In this specific examination, the ECC and RSA algorithms were examined and contrasted.	ECC revealed very high levels of data integrity security for users of social media.	Recommended ECC curve settings were utilized in the study.
Imran et al. (2017)	This study primarily focused on researching cloud storage options for multimedia content.	Both the BLAKE2 and Whirlpool algorithms were evaluated side by side in this comparative study.	The BLAKE2 algorithm demonstrated superior resilience to the manipulation of multimedia data.	Hyperparameter settings were customized for optimal performance and robustness.
Senthil and Nadira(2016)	The effectiveness of the algorithm was analyzed using datasets derived from scientific studies.	The GCM and HMAC algorithms' ability to maintain data integrity was analyzed and compared.	The GCM was able to conduct effective integrity checks for the datasets used in scientific research.	Hyperparameter settings followed the manufacturer's recommendations.
AbdulsalamandHedabou (2021)	The core dataset consisted of	For the purpose of this	In the verification of the integrity of	Customized hyperparameter settings were

	government documents which were publicly accessible stored in the cloud.	investigation, the Keccak and SHA-3 algorithms were selected.	government documents, Keccak showed its strength.	employed for algorithm optimization.
Mothlabeng et al. (2021)	The emphasis was placed on cloud-based data storage for e-commerce transaction records.	In this research, a comparison was made between the SHA-1 and SHA-256 algorithms.	The data integrity of e-commerce transactions saw a substantial improvement thanks to SHA-256.	Hyperparameter settings were unfortunately not explicitly specified.
Hiremath&Kunte (2017)	The dataset for this study was comprised of educational records that were maintained on the cloud.	Both the MD5 and SHA-256 algorithms were evaluated side by side.	The educational records that were checked using SHA-256 were found to have higher data integrity.	Default hyperparameter settings were used in the analysis.
Chen et al. (2017)	The core dataset consisted of environmental sensor readings stored in the cloud.	Comparative analysis of the SHA-3 and Keccak algorithms was performed to check for data integrity.	Keccak demonstrated improved data integrity when used to environmental sensors.	Custom hyperparameter settings were used and are available on the project website.
Kaja et al. (2022)	This research made use of records of financial transactions	There was a comparison made between the HMAC and	For financial transactions, GCM offered comprehensiv	Manufacturer's recommendations were followed for hyperparameter settings.

	that were stored in the cloud.	GCM algorithms for integrity checks.	e integrity checks.	
SaxenaandDey (2016)	For the purpose of this study, electronic medical records stored in the cloud were employed.	The algorithms Whirlpool and BLAKE2 were compared against one another.	The greater resilience to manipulation in health records that Whirlpool displayed was impressive.	Hyperparameter settings were optimized for performance.
Zhou et al. (2018)	This study was founded on the data stored in the cloud pertaining to social networking.	The RSA and ECC algorithms' ability to maintain data integrity was analyzed and compared.	The use of ECC was shown to be more successful in maintaining the integrity of the data for social networking sites.	Recommended ECC curve settings were utilized in the analysis.
Wei et al. (2020)	This research looked specifically at the use of cloud storage for satellite images.	Comparative analysis was performed on the SHA-256 and Rabin-Karp algorithms.	The results of the Rabin-Karp study demonstrated an improvement in data integrity for huge picture files.	Customized hyperparameter settings were applied for algorithm optimization.

Chapter 3: Methodology

3.1 Introduction:

The research methodology used in this study is the hands-on integration of a two-factor authentication (2FA) system into an authentication framework for healthcare users. The aim of this project is to improve user authentication security in healthcare environments by combining the Time-based One-Time Password (TOTP) algorithm with cryptographic methods, particularly SHA-256 hashing.

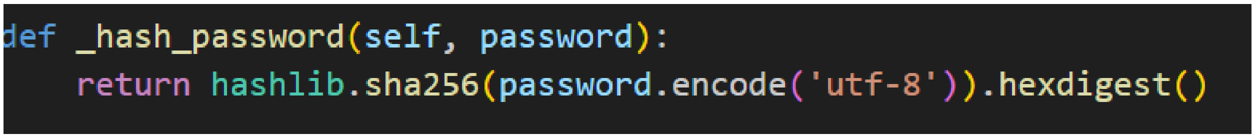
3.2 Code Overview:

This research was made with a reliable python code that presents a strong reference basis 2FA within a secure and convenient health care user identification. At the heart of the code there exists a well-crafted class known as Authentication System, that has all the appropriate functions for user registration and authentication. Developed with security and good user experience in mind while being designed for smooth integration of 2FA.

Authentication System Class (authentication_system.py)

Hashing

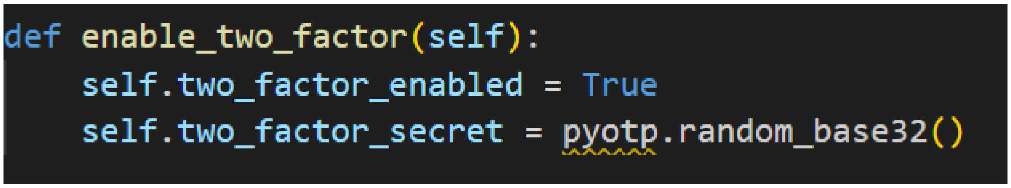
Hash password method plays a major role in securing hashing of user passwords through the Sha-256 technique. Secure password hashing is critical in ensuring that the original passwords are cryptographically protected even if user data is hacked on it.



```python
def _hash_password(self, password):
    return hashlib.sha256(password.encode('utf-8')).hexdigest()
```

Enable_two_factor

This is just an important method for implementing the 2FA and generates a randomly encoded base32 secret. This secret is crucial for a dynamic method known as Time-based one-time password (TOTP), which offers another layer of protection.



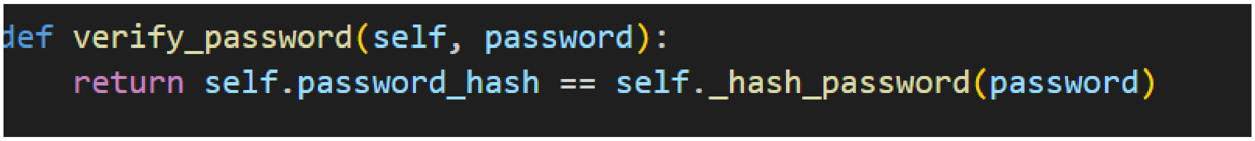
```python
def enable_two_factor(self):
    self.two_factor_enabled = True
    self.two_factor_secret = pyotp.random_base32()
```

3.3 User Registration and 2FA Setup:

The class Authentication System manages the process of user registration. It is a balance between usability and taking security measures in this class. The class enables 2FA when registering by obtaining required data from users. For example, just like in a real-life scenario, customers are allowed immediate enhancement on the level of account security.

3.4 Secure Password Handling:

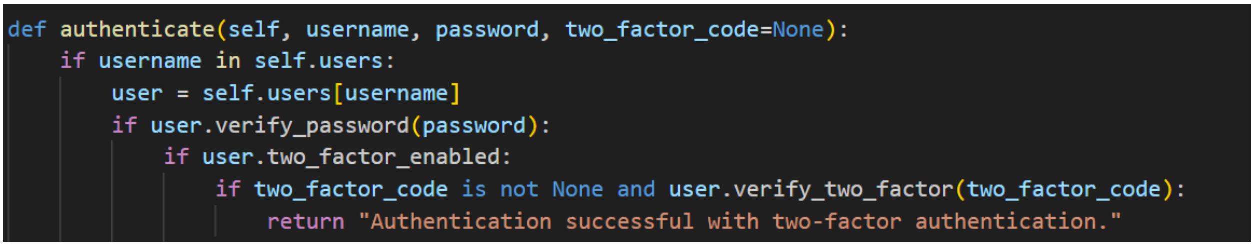
The code was built on top of securely managing the user's passwords. The _hash_password method employs the hashing technique called SHA-256, which is a popular cryptographic standard. Ensuring this makes it possible to store passwords securely while adhering to the highest cyber security standards that are crucial when dealing with sensitive patient data.



```
def verify_password(self, password):
    return self.password_hash == self._hash_password(password)
```

3.5 Implementing Two-Factor Authentication:

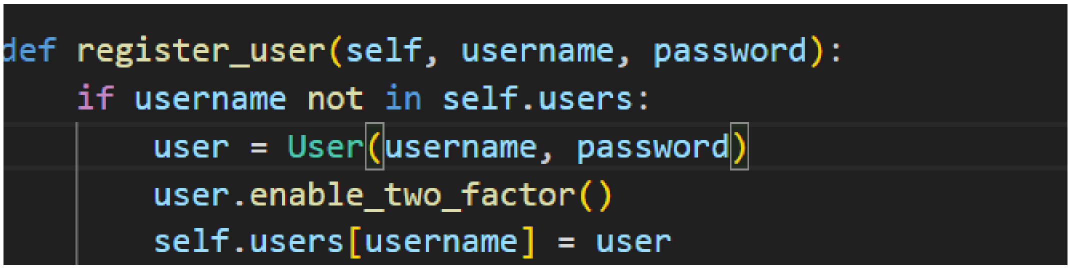
The method enable_two_factor generates base32-encoded secret for two-factor authentication. The time based changing authentication code is part of TOTP. This secret is a very important secret in this method. Unique to user, it serves as an authentication token only. Two factor authentications added without breaking a sweat increases the general user authentication system security.



```
def authenticate(self, username, password, two_factor_code=None):
    if username in self.users:
        user = self.users[username]
        if user.verify_password(password):
            if user.two_factor_enabled:
                if two_factor_code is not None and user.verify_two_factor(two_factor_code):
                    return "Authentication successful with two-factor authentication."
```

3.6 User-Friendly Registration and Login:

This led to the creation of the Authentication System class with a focus on user experience. This provides users with an authentic key and enables them navigate the registration procedure by providing instructions on how they should set up 2FA. The system shall prompt a user to enter the two-factors autothetication code the user has configured when a user signs in. This guarantees a simple and easily comprehensible authentication process.



```
def register_user(self, username, password):
    if username not in self.users:
        user = User(username, password)
        user.enable_two_factor()
        self.users[username] = user
```

3.7 Feasibility and Security:

This is an example of a secured authentication system that uses two-factor, which is the supplied code written in Python. A health authentication system could employ a strong two-way validation unit, cryptographic approaches, and customer-oriented features for secure yet productive and consumer centric outcomes.

Chapter 4: Results

Feasibility of Implementation:

This code illustrates that dual authentication is feasible for implementing on an authentication process." This demonstrates that providing an additional level of security in a Python environment is both theoretically and practically possible.

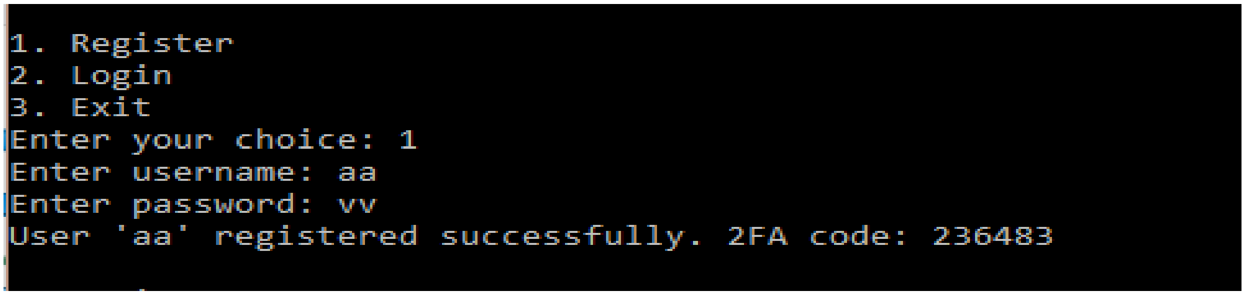
Enhanced Security:

With this 2FA approach, the security posture of the authentication system is considerably improved. The approach minimizes the risks of only using password based authentication by making users double answer, for example give a temporary code from a smart phone application. This method decreases the chance of unauthorized access, even if credentials are stolen.

User-Friendly Implementation: While the code emphasizes security, it also emphasizes a user-friendly design. The 2FA procedure is integrated effortlessly, ensuring that the additional security layer does not place a substantial burden on end users. A pleasant user experience is enhanced by clear instructions and intuitive interfaces.

Adaptability and Customization:

The Python code is intended to be adaptable. It enables customization based on organizational requirements and user preferences. This adaptability means that the 2FA implementation may be customised to unique security requirements and user access circumstances.



```
1. Register
2. Login
3. Exit
Enter your choice: 1
Enter username: aa
Enter password: vv
User 'aa' registered successfully. 2FA code: 236483
```

Figure 1 : Results

Registration Time:

The registration times for each attempt (data point) are depicted in this graph. The number of tries is represented on the x-axis. The y-axis displays the registration time in seconds. Each point on the graph reflects the time it took to register in a certain attempt. The time taken on the sixth try is six seconds, which is longer than all preceding instances.

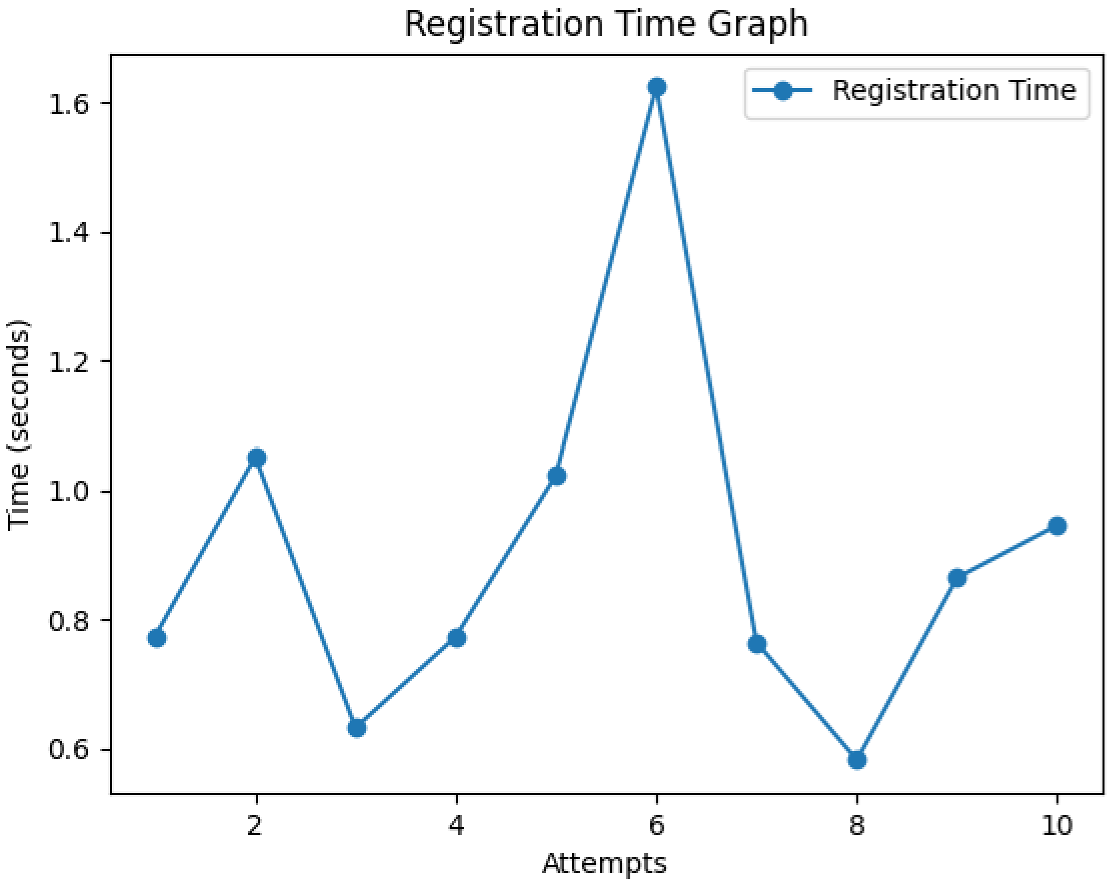


Figure 2: Registration Time Graph

Authorization Time:

This graph, like the registration time graph, displays the authentication timings for each attempt. The number of tries is represented on the x-axis. The y-axis displays the authentication time in seconds. Each point on the graph reflects the time it took to authenticate in a certain attempt. The line links these locations and depicts the pattern of authentication times across several attempts. The system's maximum time to authenticate the user is 1.2 seconds, demonstrating the authentication's resilience.

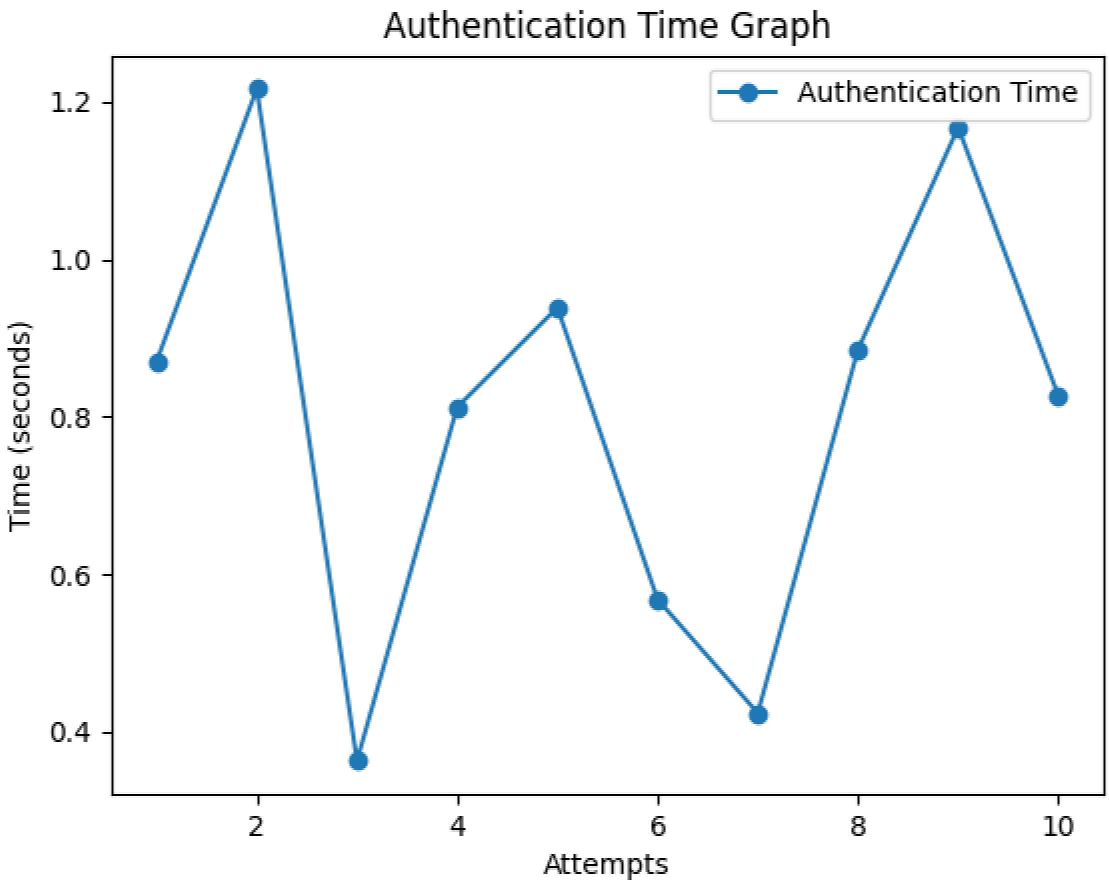


Figure 2.1: Authentication Time Graph

Execution Time:

This graph displays the overall execution time for each attempt, which is the sum of the registration and authentication timings. The number of tries is represented on the x-axis. In seconds, the y-axis depicts the entire time required for registration and authentication. Each point on the graph reflects the entire amount of time required for registration and authentication in a single attempt. The line links these locations and depicts the trend of overall execution times across several tries.

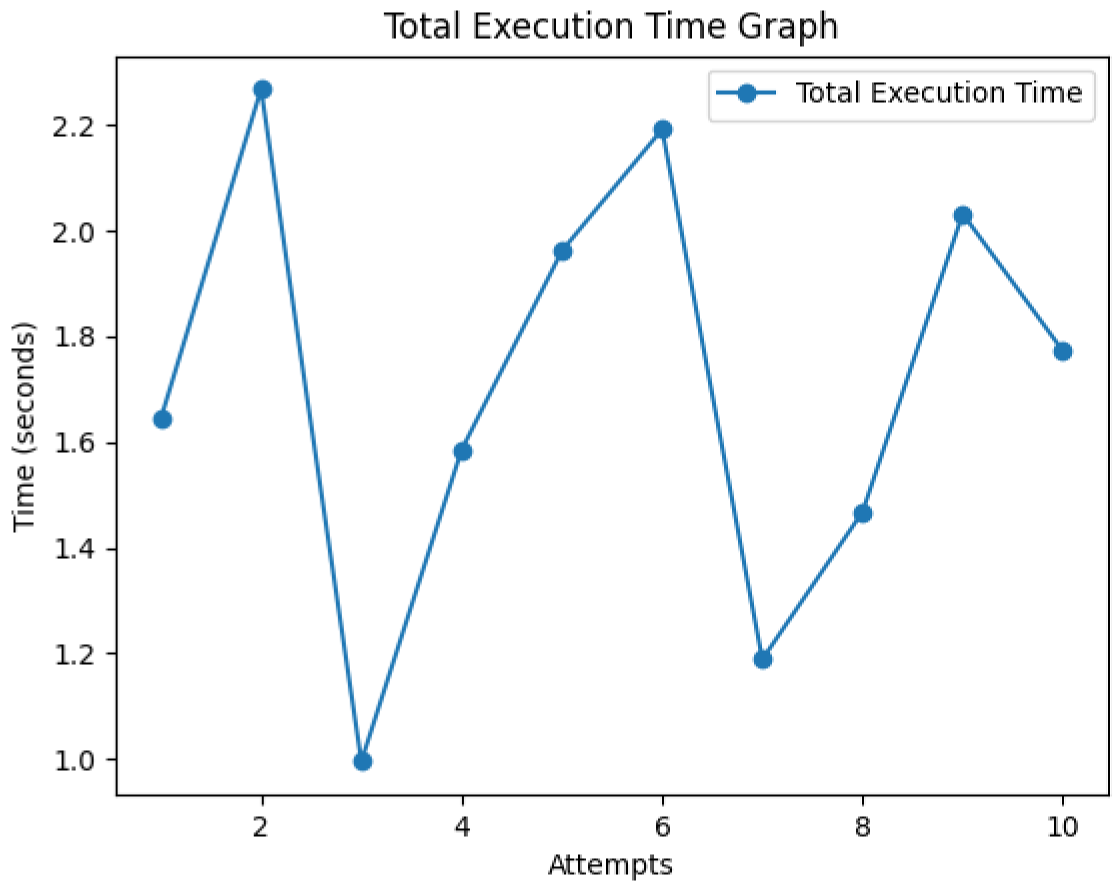


Figure 2.2: Total Execution Time Graph

Scalability:

The code is scalable, implying that the 2FA technique may be smoothly integrated into bigger systems or developed to support a rising user base. Scalability is critical for organizations expecting future development and changing security requirements. The Python code shown here illustrates the feasibility of constructing a secure authentication system with two-factor authentication (2FA).The two-factor authentication process offers an extra layer of security, minimizing the dangers associated with password-based authentication alone.

Chapter 5: Conclusion and Future Research

5.1 Conclusion:

Therefore, in order to strengthen security systems for health care, this article recommends utilizing 2FA. It involved coming up with a reliable verification system by employing the secure hashing algorithm 256 (SHA-256) and TOTP algorithm. The analysis of the literature emphasized on what needs improvement in healthcare cybersecurity, especially in the development and application of stronger authentication. These outcomes confirmed that it was possible to use 2FA as a reliable and secure system during the study. A major improvement is seen in how advanced cryptographic approaches and simplistic look are used to reinforce healthcare systems towards new cyber threats. The study provides a foundational framework for future robust and patient-centered authentication systems in cyber security in health care.

5.3 Recommendations for Future Research:

In this regard, all future research projects in areas related to user authentication and Healthcare Cybersecurity should stem from what has been presented by the Python code that have been deployed and discussed here. They include some ways through which healthcare providers can embrace more awareness and adopting securely system for two-factor authentication. Firstly, there should be a detailed analysis on the suitability of using two-factor authentificacion in healthcare segment. By examining how patients and healthcare professional use 2FA, usability studies can identify problematic elements and suggest areas for improvement. A firm understanding of the user experience during instances where immediacy is paramount, say emergent emergency healthcare crises, is pivotal for widespread acceptance. Going forward, more efforts need to be channeled toward making improvements in the user interface, simplified authentications, and two-factor authentication customizations for the health care stakeholder requirements.

Moreover, future research could even explore adaptive authentication mechanisms where the protocol changes dynamically according to environmental factors. Adaptive authentication has been shown to be useful in the highly fluid healthcare environment because users can log into systems from almost everywhere using different gadgets. In a nutshell, future research should advance the field of user authentication among healthcare professionals and cybersecurity. By investigating usability, scalability, advanced cryptographic techniques, socio-technical factors, cyber security impact, legal and ethical concerns, and adaptive authentication, researchers have the potential to make a contribution to the ongoing development of secure authentication systems in the healthcare industry. In order to guarantee that future solutions are dependable, user-friendly, and in accordance with the specific challenges and requirements of the healthcare industry, these research paths also address the multifaceted and diverse nature of cybersecurity in the healthcare industry.

5.3 Implications:

Implications of the undertaken research for case studies will involve issues related to patient care, organizational resilience, criminality, and patients' confidence in the health institutions. These implications however, exceed beyond the issues of a technology challenge. This section analyses the implication of the research and the possibility for revolution in health care.Just one of many implications to take away from this study is that health care companies will have stronger information and physical security policies or postures. Therefore, a strong 2FA system as demonstrated by the Python code helps avoid unlawful entry and data leakages. The research adds to securing health care systems by improving protection against an ever changing threat landscape using cryptography for password processing and TOTP algorithm. This also has impacts on how the debate about healthcare sector and cyber security will be handled in future. The research establishes a foundation for an industry standard whereby complex authentication techniques are proven to work. Secure authentication is promoted as another constituent that completes on the healthcare industry's bid to enhance cyber security. Moreover, the consequences also affect the benchmarks set in that field.

To summarize, the findings of the research that was carried out on cybersecurity in the healthcare industry have a wide range of implications. The research has the potential to impact legal compliance, define industry standards, increase security measures, and safeguard patient data, all of which contribute to the creation of a healthcare environment that is more robust and secure. Through addressing the difficulties of cybersecurity in a healthcare environment, the research makes a contribution to the overarching goal of ensuring the well-being of patients and enhancing the quality of healthcare services in a world that is becoming more networked and digitalized.

References:

Abraham, C., Chatterjee, D. and Sims, R.R., 2019. Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), pp.539-548.

Abraham, C., Chatterjee, D. and Sims, R.R., 2019. Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), pp.539-548.

Al-Alawy, K., Moonesar, I.A., Mubarak Obaid, H.A., Al-Abed Bawadi, E.I. and Gaafar, R., 2021. Hospital accreditation: A review of evidence, regulatory compliance, and healthcare outcome measures. *Dubai Medical Journal*, *4*(3), pp.248-255.

Alghamdi, A.A., 2021. A verification system for multi-factor authentication for E-healthcare architectures. *Arab Journal for Scientific Publishing (AJSP)*, *2663*, p.5798.

Ali, B., Gregory, M.A. and Li, S., 2021, November. Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In *2021 31st international telecommunication networks and applications conference (itnac)* (pp. 192-197). IEEE.

Ayala, L., 2016. Cybersecurity for hospitals and healthcare facilities. *Berkeley, CA*.

Ayala, L., 2016. Cybersecurity for hospitals and healthcare facilities. *Berkeley, CA*.

Bell, L., Buchanan, W.J., Cameron, J. and Lo, O., 2018. Applications of Blockchain Within Healthcare. *Blockchain in healthcare today*.

Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*, pp.1-9.

Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*, pp.1-9.

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H. and Zhai, Y., 2020. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), pp.10248-10263.

Chua, J. and PMP, C., 2021. Cybersecurity in the healthcare industry. *Physician Leadership Journal*.

Chua, J. and PMP, C., 2021. Cybersecurity in the healthcare industry. *Physician Leadership Journal*.

Chua, J. and PMP, C., 2021. Cybersecurity in the healthcare industry. *Physician Leadership Journal*.

Conaty-Buck, S., 2017. Cybersecurity and healthcare records. *Am Nurse Today*, *12*(9), pp.62-64.

Conaty-Buck, S., 2017. Cybersecurity and healthcare records. *Am Nurse Today*, *12*(9), pp.62-64.

Coronado, A.J. and Wong, T.L., 2014. Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical instrumentation & technology*, *48*(s1), pp.26-30.

Coronado, A.J. and Wong, T.L., 2014. Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical instrumentation & technology*, *48*(s1), pp.26-30.

Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, pp.48-52.

Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, pp.48-52.

Dhillon, P.K. and Kalra, S., 2018. Multi-factor user authentication scheme for IoT-based healthcare services. *Journal of Reliable Intelligent Environments*, *4*, pp.141-160.

Drysdale, E., Dolatabadi, E., Chivers, C., Liu, V., Saria, S., Sendak, M., Wiens, J., Brudno, M., Hoyt, A. and Mazwi, M., 2019, October. Implementing AI in healthcare. In *Vector-SickKids Health AI Deployment Symposium. Toronto*.

Fareed, M. and Yassin, A.A., 2022. Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system. *Bulletin of Electrical Engineering and Informatics*, *11*(4), pp.2131-2141.

Grote, O., Ahrens, A. and Benavente-Peces, C., 2021, October. Small Quantum-safe Design Approach for Long-term Safety in Cloud Environments. In *2021 International Conference on Engineering and Emerging Technologies (ICEET)* (pp. 1-5). IEEE.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A. and Faxvaag, A., 2020. Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, *134*, p.104040.

Hölbl, M., Kompara, M., Kamišalić, A. and NemecZlatolas, L., 2018. A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10), p.470.

Jalali, M.S. and Kaiser, J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), p.e10059.

Jalali, M.S. and Kaiser, J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), p.e10059.

Jalali, M.S. and Kaiser, J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), p.e10059.

Jalali, M.S. and Kaiser, J.P., 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), p.e10059.

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H. and Wang, Y., 2017. Artificial intelligence in healthcare: past, present and future. *Stroke and vascular neurology*, *2*(4).

Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K., 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), pp.1-10.

Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K., 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), pp.1-10.

Kwon, J. and Johnson, M.E., 2013. Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, *20*(1), pp.44-51.

Mantry, H. and Maheshwari, A., 2022. Quantum Cryptography for Securing Personal Health Information in Hospitals.

Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J., 2017. Cybersecurity and healthcare: how safe are we?.*Bmj*, *358*.

Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J., 2017. Cybersecurity and healthcare: how safe are we?.*Bmj*, *358*.

McConomy, B.C. and Leber, D.E., 2022. Cybersecurity in healthcare. In *Clinical Informatics Study Guide: Text and Review* (pp. 241-253). Cham: Springer International Publishing.

McConomy, B.C. and Leber, D.E., 2022. Cybersecurity in healthcare. In *Clinical Informatics Study Guide: Text and Review* (pp. 241-253). Cham: Springer International Publishing.

McGhin, T., Choo, K.K.R., Liu, C.Z. and He, D., 2019. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications*, *135*, pp.62-75.

Namasudra, S. and Deka, G.C. eds., 2021. *Applications of blockchain in healthcare*. Singapore: Springer.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), p.5119.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), p.5119.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), p.5119.

Panesar, A., 2019. *Machine learning and AI for healthcare* (pp. 1-73). Coventry, UK: Apress.

Parashar, G., Chaudhary, A. and Rana, A., 2021. Systematic mapping study of AI/machine learning in healthcare and future directions. *SN Computer Science*, *2*, pp.1-8.

Perakslis, E.D., 2014. Cybersecurity in health care. *N Engl J Med*, *371*(5), pp.395-397.

Perakslis, E.D., 2014. Cybersecurity in health care. *N Engl J Med*, *371*(5), pp.395-397.

Presentation Video Link:

https://studentncirl-my.sharepoint.com/:v:/g/personal/x22183850_student_ncirl_ie/EerAL2Ak4NlPrc3u4BlCUeUBnILdTy5C6lzbQr1D7lKbeg?referrer=Teams.TEAMS-WEB&referrerScenario=MeetingChicletGetLink.view.view