The 2024 Change Healthcare Cyberattack and the Imperative of Multi-Factor Authentication

Namrata Vijay Mali

[malinamratavijay@cityuniversity.edu](mailto:malinamratavijay@cityuniversity.edu)

Ayush Kumar Gupta

[guptaayushkumar@cityuniversity.edu](mailto:guptaayushkumar@cityuniversity.edu)

Sai Mani Ritish Upadhyayula

[upadhyayulasaimanir@cityuniversity.edu](mailto:upadhyayulasaimanir@cityuniversity.edu)

CS504 Full Software Engineering, MSCS

School of Technology & Computing

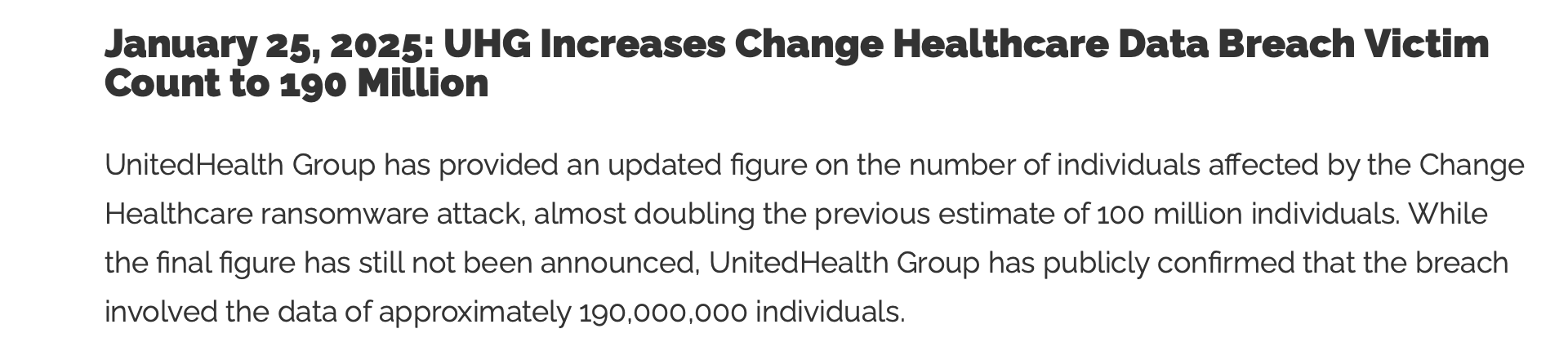
City University of Seattle

Seattle, WA 98121, USA

**Abstract**

In February 2024, a major cyberattack took place targeting Change Healthcare, a subsidiary of UnitedHealth Group, causing considerable disruption to healthcare operations throughout the United States. The breach stemmed from a Citrix remote access portal that did not have Multi-Factor Authentication (MFA), giving threat actors an unimpeded route to install ransomware and steal sensitive patient and organizational information. The repercussions of this attack highlighted the immediate requirement for enhanced cybersecurity measures, especially in the healthcare industry, which manages extensive quantities of sensitive and vital data. This case analysis examines the technical and organizational weaknesses taken advantage of during the attack and highlights the preventive benefits of implementing MFA. It additionally examines four popular MFA solutions—Microsoft Azure Active Directory MFA, Google Authenticator, Duo Security, and Okta MFA—evaluating them on factors like security effectiveness, integration potential, user satisfaction, and cost-effectiveness. Drawing from this analysis, the study suggests Google Authenticator as the best choice due to its robust security framework, user-friendly interface, offline capabilities, and low cost, positioning it as an ideal option for organizations looking to enhance access security without facing significant complexity or expenses.

**Keywords:** Multi-Factor Authentication, Access control, Biometrics, Cybersecurity



1. **INTRODUCTION**

The healthcare industry is progressively depending on digital systems to handle patient information, billing, and other essential functions. This reliance on digital technology makes it a main target for cyberattacks. The 2024 cyberattack on Change Healthcare underscored weaknesses in access control measures, especially the lack of MFA on essential systems [1]. Implementing MFA is a crucial measure for improving cybersecurity since it needs that users supply various forms of verification, which lowers the chances of unauthorized access.

1. **OVERVIEW OF THE CHANGE HEALTHCARE CYBERATTACK**

**2.1** **Summary of the Incident**

On February 21, 2024, Change Healthcare discovered a ransomware assault that penetrated its systems through a Citrix remote access portal without MFA. Cybercriminals used compromised credentials to infiltrate the system, implement ransomware, and extract data from February 17 to February 20, 2024. The violation interrupted payment and claims processing across the country, affecting healthcare providers and patients. UnitedHealth Group later verified that the ransomware collective ALPHV/BlackCat was accountable and paid a ransom of $22 million to alleviate the attack.

**2.2 Evaluation of Impact**

* Operational Disruption: The assault interrupted electronic payments and the processing of medical claims, resulting in major delays in patient care and financial pressure on healthcare providers.
* Data Breach: Personal details of around 100 million people were breached, comprising health insurance IDs, treatment details, and Social Security numbers.
* Financial Implications: The incident led to significant financial losses, including the ransom paid and the expenses related to system recovery and data breach remediation [2].

1. **MULTI-FACTOR AUTHENTICATION (MFA): A CRITICAL SECURITY MEASURE**

MFA improves security by causing that users present two or more verification elements to access a system. These elements usually consist of:

**Something you are aware of:** Password or PIN

**An item in your possession:** Security token or mobile device

**An aspect of your identity:** Biometric authentication like fingerprints or facial recognition.

Using MFA greatly lowers the chances of unauthorized access, even if a single credential is breached.

1. **LITERATURE REVIEW**
   1. **Multi-Factor Authentication (MFA): A Critical Security Measure**

To choose the four MFA systems analyzed in this study, the team utilized these criteria:

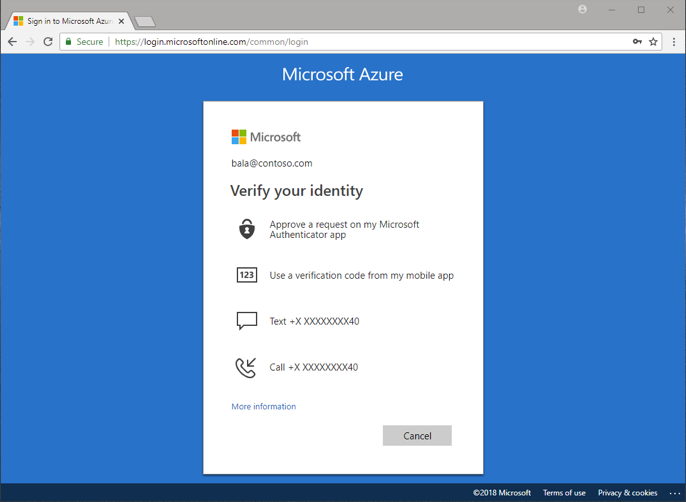
* **Popularity and Usage:** Systems commonly utilized in educational organizations and companies.
* **Variety of Technology:** Platforms providing several authentication options (push notification, biometric, TOTP, SMS).
* **Accessibility:** Systems readily accessible to users without needing specialized equipment.
* **Security Track Record:** Systems that have proven robust security and earned industry credibility.

Following these standards, the team selected Microsoft Azure Active Directory MFA, Google Authenticator, Duo Security, and Okta MFA.

**4.2 MFA SYSTEMS AND THEIR FUNCTIONALITY**

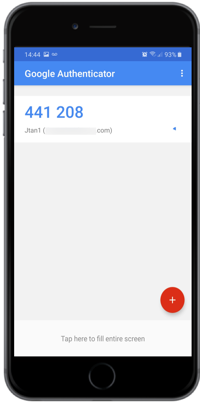
1. **Microsoft Azure Active Directory MFA**

* Used in educational institutions (e.g., CityU login).
* Supports mobile app notifications, phone calls, and SMS.
* Example: On login, a user receives a push notification on Microsoft Authenticator for approval.



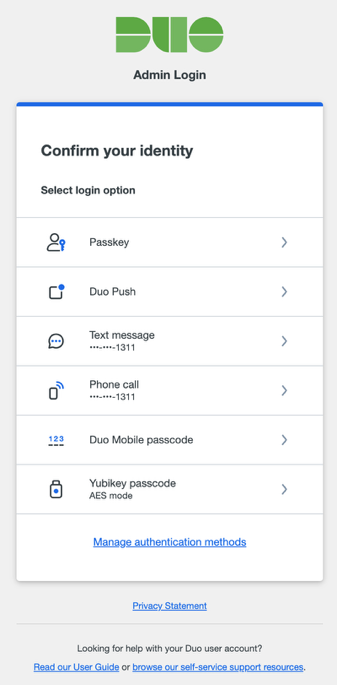
1. **Google Authenticator**

* Time-based One-Time Password (TOTP) system.
* Used by Google accounts, GitHub, and many SaaS apps.
* Example: Scanning a QR code during setup, then entering a 6-digit code during login.



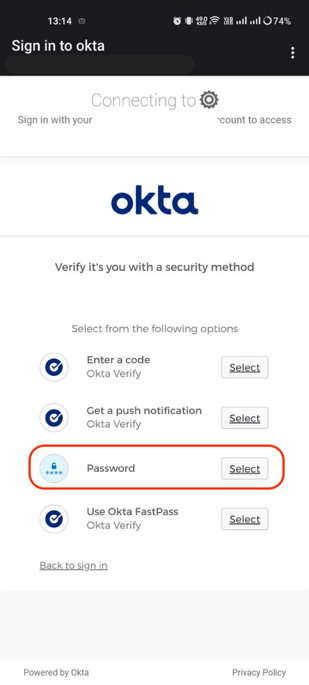
1. **Duo Security (by Cisco)**

* Offers app push, phone call, passcode, and biometric options.
* Used in universities (e.g., UC Berkeley) and enterprises.
* Example: Push notification approval using Duo Mobile app.



1. **Okta MFA**

* Cloud-based identity platform.
* Supports app push, WebAuth, SMS, and email verification.
* Example: After entering credentials, a prompt verifies identity through the Okta Verify app.



* 1. **Project Description**

This project explores the function of MFA in thwarting cyberattacks, concentrating on a case study of the 2024 Change Healthcare event. The group created and established a small-scale MFA system with Google Authenticator to mimic a secure login procedure. The backend, developed using Flask and MongoDB, manages user registration, QR code creation, and OTP verification, while the React front-end interface directs the user through every step: account setup, QR scanning, OTP submission, and confirmation. Further project responsibilities involved implementing CORS for cross-origin requests, creating user-friendly interfaces, managing error scenarios, and confirming accurate OTP time window validation. By means of this thorough construction, the team examined both the technical and user experience elements of MFA implementation.

* 1. **Usefulness**

The practical value of this project goes beyond theoretical concepts, providing real-world perspectives on the design, execution, and operational effects of MFA systems. Through the creation and evaluation of a live MFA prototype, the team gained a hands-on understanding of system security integration, backend-frontend interactions, and user onboarding difficulties. The initiative highlights that MFA can significantly minimize the exposure to credential theft attacks, even with simple setups. Furthermore, the initiative acts as an educational resource, illustrating to stakeholders how straightforward, affordable tools such as Google Authenticator can deliver significant security enhancements and how these applications can be expanded or modified for broader organizational settings.

1. **METHODOLOGY**
   1. **MFA SYSTEMS AND THEIR FUNCTIONALITY**

**Suggestion: Google Authenticator**

Considering the Change Healthcare breach, Google Authenticator appears to be an effective remedy:

**Simplicity**: Simple to implement and utilize, lowering obstacles to acceptance

**Offline Functionality**: Produces codes without needing internet connectivity, improving dependability

**Economical**: No cost involved, allowing accessibility for organizations of different sizes.

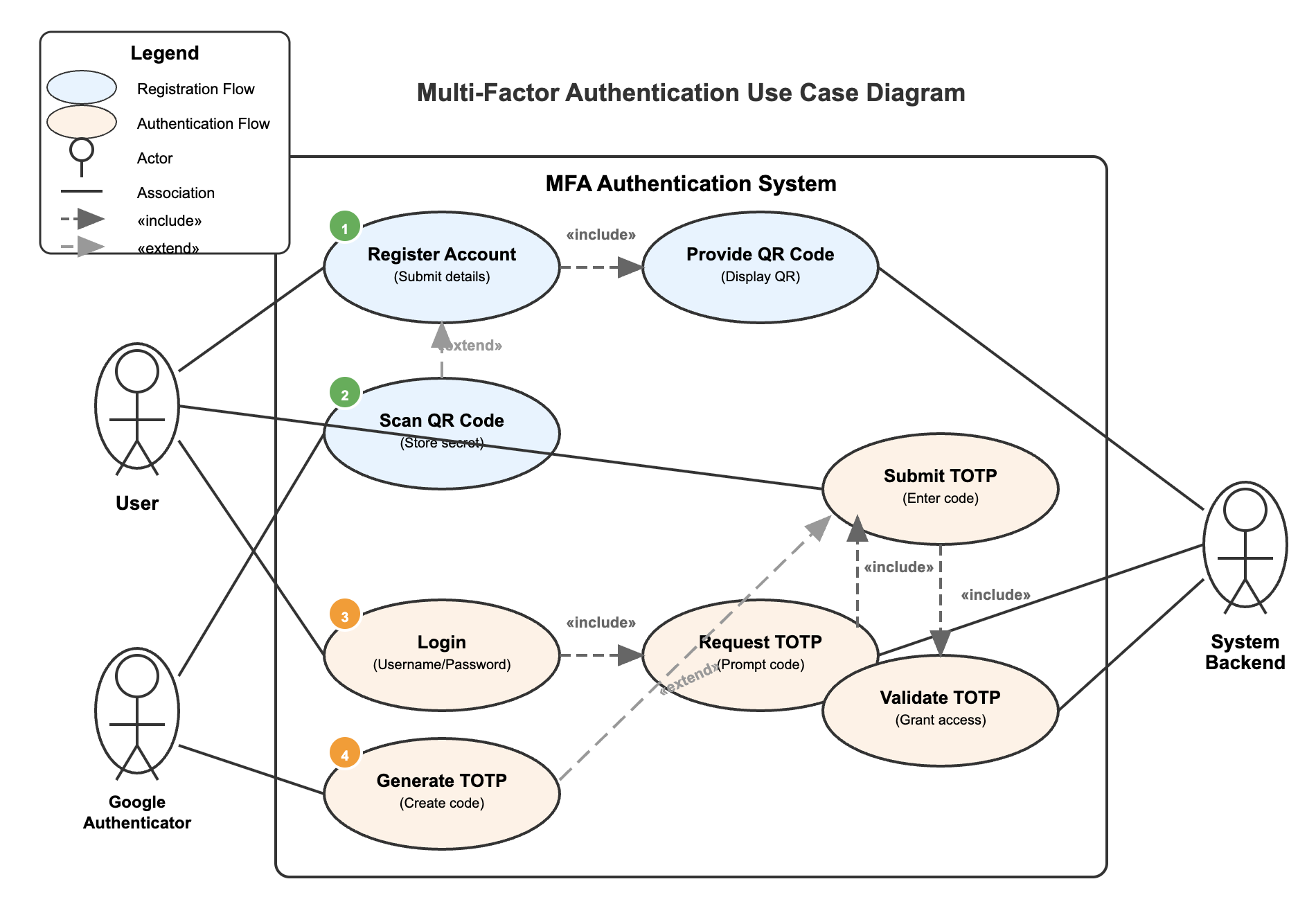
**Security:** Offers a strong level of protection via TOTP, reducing the dangers linked to credential theft.

Although other solutions provide advanced features tailored for large corporations, Google Authenticator offers a harmonious blend of security and ease of use, making it an excellent option for organizations aiming to improve their authentication systems without substantial burden.

* 1. **Use Cases to Be Covered**

**Main Use Cases:**

1. **Register Account**
   * User → System: Submit username + password
   * System → User: Display QR code for MFA setup
   * User → Google Authenticator: Scan QR code and store secret
2. **Login**
   * User → System: Enter username + password
   * System → User: Prompt for 6-digit OTP
   * User → Google Authenticator: Retrieve current OTP
   * User → System: Submit OTP
   * System → System: Verify OTP
   * System → User: Grant or deny access
   1. **Use Case Diagram**

****

* 1. **Class Diagram**

**A screenshot of a computer

AI-generated content may be incorrect.**

* 1. **Interaction/Activity Diagram**

**A diagram of a system

AI-generated content may be incorrect.**

* 1. **Swim lanes**

**A diagram of a computer program

AI-generated content may be incorrect.**

* 1. **Database ER Diagram**

**A screenshot of a computer

AI-generated content may be incorrect.**

* 1. **Link to GitHub**

**https://github.com/namumali/MFA**

* 1. **GUI Images**

1. **New User Registration**

**A screenshot of a login form

AI-generated content may be incorrect.**

1. **User Login + Second Level authentication**

**A screenshot of a login page

AI-generated content may be incorrect.**

1. **Login after registration (within time session without MFA)**

**A screenshot of a login page

AI-generated content may be incorrect.**

1. **2-minute timeout to re-trigger 2nd level authentication (asks MFA)**

**A screenshot of a login form

AI-generated content may be incorrect.**

1. **Successful Login**

**A screen shot of a computer screen

AI-generated content may be incorrect.**

1. **Result**
   1. **COMPARISON & PREFERRED SYSTEM**

|  |  |  |  |
| --- | --- | --- | --- |
| **MFA System** | **Methods Supported** | **Ease of Use** | **Security Level** |
| **Azure AD MFA** | Push, SMS, Call | High | High |
| **Google Authenticator** | TOTP only | Medium | Moderate |
| **Duo Security** | Push, Call, Biometric | High | Very High |
| **Okta MFA** | Push, WebAuthn, Email, SMS | High | Very High |

Duo Security and Okta MFA provide robust protection with sophisticated features like biometric verification and WebAuthn; however, these systems are typically designed for enterprise settings and may require extra setup and licensing fees. Azure AD MFA works smoothly within Microsoft environments but is not as suitable for scenarios outside of Microsoft.

Google Authenticator, while restricted to TOTP, provides a simple and safe option that functions offline, is not reliant on cellular networks or push alerts, and is available at no cost. Its straightforward implementation and minimal entry requirements position it as an excellent choice for organizations looking to enhance their authentication security swiftly and efficiently.

**Suggested MFA Solution: Google Authenticator**

In the scenario of the Change Healthcare breach, where access was jeopardized due to the absence of a secondary authentication factor, even a simple but strong TOTP-based approach such as Google Authenticator could have reduced the risk. Weighing the factors of security, user-friendliness, and implementation expenses, Google Authenticator stands out as the most effective and user-friendly option to avert similar occurrences in healthcare and other critical fields.

1. **Mock Situation: Google Authenticator in the Change Healthcare Cyber Incident**

In the recent Change Healthcare breach, intruders utilized compromised credentials to enter the Citrix remote access portal, which did not have an additional authentication layer. Without Multi-Factor Authentication (MFA), when attackers obtained the username and password, they quickly obtained complete access, which enabled them to deploy ransomware and retrieve sensitive information.

If Google Authenticator had been used, the login process would have been much more secure. Once the intruder entered the pilfered username and password, the system would request a 6-digit Time-Based One-Time Password (TOTP) produced by the Google Authenticator app, which is exclusively connected to the legitimate user's mobile device. Lacking physical access to this device and the secret key associated with it, the attacker cannot generate the necessary code. Consequently, the login attempt would be unsuccessful, effectively halting the attack at the access control level.

**Username and Password Input**: An employee or external vendor tries to access the system by entering their correct username and password.

**Time-Based One-Time Password (TOTP)**: Right after entering login details, the portal requests a 6-digit code produced by Google Authenticator, specifically linked to that user’s mobile device.

**Validation**: The assailant, without access to the registered user's mobile phone and TOTP key, is unable to generate the correct code.

**Access Denied:** The system refuses the login attempt, preventing the unauthorized session.

This straightforward action would have successfully disrupted the attack chain during authentication, neutralizing the threat prior to any harmful actions taking place.

By necessitating a second factor that is generated in real time and kept apart from the main login, Google Authenticator might have been pivotal in blocking unauthorized access—showcasing its usefulness as an economical and effective defense layer in high-risk settings.

1. **CONCLUSION**

The findings of this study clearly show that even a simple application of Multi-Factor Authentication can greatly enhance system protection against cyber threats. The team demonstrated that basic MFA techniques, by constructing and evaluating a prototype with Google Authenticator, can effectively thwart unauthorized access attempts, hindering attackers from victimizing stolen credentials.

Out of the four MFA solutions assessed, Google Authenticator stood out as the most well-rounded option for small to medium-sized businesses, providing strong time-based one-time password (TOTP) security, offline functionality, ease of use, and affordability. Although enterprise-centric options such as Duo Security and Okta MFA provide sophisticated features, the ease of use and low setup demands of Google Authenticator render it an excellent choice for organizations aiming for quick enhancements without significant financial or technical strain.

The Change Healthcare cyberattack highlights that essential security failures can result in devastating effects across the country. Implementing MFA is no longer a luxury or an optional enhancement—it has become a vital protection for any organization managing sensitive or crucial data. Implementing MFA practices allows organizations to greatly minimize their attack surface and strengthen their resilience in a cybersecurity environment that is becoming more hostile.

1. **WORKLOAD ASSIGNMENT**

|  |  |
| --- | --- |
| **TEAM MEMBER** | **CONTRIBUTION** |
| Namrata | Researched Microsoft Azure AD MFA and Okta MFA; drafted Introduction and Abstract; formatted the paper; helped implement the MFA prototype and backend logic. |
| Ayush | Analyzed Duo Security and Google Authenticator; contributed to comparison table; gathered references; implemented front-end integration and QR code generation. |
| Ritish | Compiled findings for the Comparison & Preferred System section; edited and reviewed for consistency and technical accuracy; contributed to backend testing and MFA verification logic. |

**10. REFERENCES**

* Change Healthcare Responding to Cyberattack. HIPAA Journal. Retrieved from: [Link](https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/)
* Kapko, M. (2024, May 6). Change Healthcare cyberattack: 5 technical takeaways from UnitedHealth CEO’s testimony. Healthcare Dive. [Link](https://www.healthcaredive.com/news/unitedhealth-change-attack-tech-takeaways/715274/)
* What is: Multifactor Authentication - Microsoft Support. (n.d.). [[Link]](https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661)
* What is Multi-Factor Authentication (MFA)? | OneLogin. (n.d.). [[OneLogin]](https://www.onelogin.com/learn/what-is-mfa)
* What is MFA? - Multi-Factor Authentication and 2FA Explained - AWS. (n.d.). Amazon Web Services, Inc. [[Link]](https://aws.amazon.com/what-is/mfa/)
* Bigelow, S. J., Yasar, K., & Shacklett, M. E. (2025, February 28). What is multifactor authentication? Search Security. [[Link]](https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA)