Al-Zaytoonah Journal of Business, Vol. 01 No. 03, November 2025

Mitigating Cyber Risk and Current Trends in Modern Authentication Techniques for Businesses

Khaled Musa[1], Omid Afshinpour[2], Christian Avila[3], Sarah Jimenez[4]
[1]California State University, Sacramento, k.musa@csus.edu
[2]omidafshinpour@csus.edu
[3]christianavila2@csus.edu
[4]sjimenez10@csus.edu

Abstract
Cyber risk and data breaches for organizations increasingly arise from outdated password practices, influenced by human behavior, mistakes, and the reliance on information that individuals must remember. Cybercriminals and hackers exploit vulnerabilities in password security and the tendency of users to reuse passwords across various platforms, including work and personal websites, as well as for multiple purposes. Leaders in the IT industry and Chief Information Officers have advocated for organizations and users to eliminate traditional password security measures in favor of more robust authentication methods, such as biometric and multifactor approaches. These advanced security techniques offer companies and users enhanced opportunities to safeguard themselves against cyber threats and data breaches. However, user resistance and a lack of familiarity with contemporary authentication methods pose significant challenges to the adoption of passwordless solutions
This paper will examine various aspects of contemporary passwordless authentication techniques. Firstly, it will discuss the recent trends in shifting away from exclusively password-based security systems and analyze what modern authentication solutions offer to both businesses and users, including multifactor authentication (MFA), biometric logins, and hardware security keys. Secondly, it will address the challenges that organizations encounter in the implementation and adoption of these modern methods. Thirdly, it will explore the opportunities for enhancing education and awareness among users regarding the advantages of transitioning from passwords to modern authentication factors, thereby safeguarding themselves against cyber risks. Lastly, this paper will review case studies illustrating how modern authentication methods could have averted substantial financial and health losses for prominent companies.

Keywords—Cyber Risk, Cyber Threat, Biometric, Multifactor Authentication (MFA), Passwords, Data Breach

1 Introduction

Usernames and passwords often serve as the initial access point for individuals logging into systems for both professional and personal use. Whether it is for banking, healthcare, government services, or social media, users are increasingly encouraged to manage a significant portion of their lives online. Traditionally, passwords have been utilized as a means of safeguarding security for both organizations and individuals. Despite receiving guidance to select strong, unique, and complex passwords, individuals frequently opt for passwords that expose themselves and their organizations to considerable cyber threats, thereby heightening the risk of data breaches. Passwords are commonly compromised due to users relying on easily identifiable information (such as their names, birth dates, home addresses, and phone numbers), writing down their passwords, reusing them across various platforms, sharing them within their organizations, or selecting passwords that are simple for cybercriminals to decipher [1]. A study conducted by Verizon Wireless revealed that in 2024 alone, over 2.8 billion passwords were made available for purchase or free distribution in criminal forums [2]. Furthermore, the same Verizon study indicated that research on password datasets demonstrated that only 3% of the total unique passwords fulfill complexity criteria.

Recently, the personal genetics company 23andMe declared bankruptcy in the spring of 2025 due to significant financial difficulties and a series of cyber-attacks. A cybercriminal exploited users' tendency to reuse usernames and passwords to gain unauthorized access to user accounts [3]. As a result, the

cybercriminal disclosed the display name, gender, birth year, and certain information regarding genetic ancestry results for more than four million 23andMe users in 2023. In February 2024, UnitedHealth Group fell victim to hackers who exploited the absence of multifactor authentication (MFA) measures [4]. The repercussions of this attack were anticipated to cost UnitedHealth over $2 billion to rectify.

Regardless of prompts, reminders, and suggestions: “Humans are bad at choosing strong passwords, we frequently reuse them and we are victims of Social Engineering fairly consistently” [2]. Multifactor authentication faces opposition as it is viewed as slow and is not well comprehended [4].

By adopting contemporary authentication techniques that do not depend exclusively on passwords or entirely eliminate their use, organizations and individuals can safeguard their data and personal information, thereby mitigating the risk of cyber-attacks or data breaches within the workplace. Contemporary authentication techniques, including multifactor authentication, biometric logins, and hardware security key protection, offer numerous opportunities to transition from "something the user knows" (i.e., their memorized password) to "something the user has" (i.e., their mobile device for verification or access) or "something the user is" (i.e., their fingerprint or facial recognition), as illustrated in Figure 1 [1]. These latter two categories of information and authentication strategies significantly increase the difficulty for cybercriminals to obtain access [5]

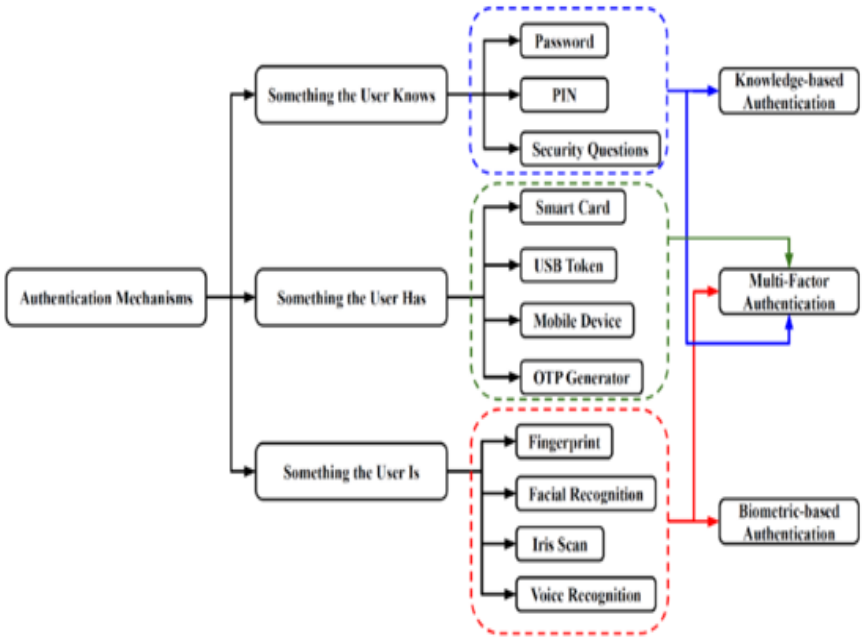

Figure 1: Albesher, A. S., Alkhaldi, A., & Aljughaiman, A. (2024). Toward secure mobile applications through proper authentication mechanisms. *PLoS One, 19*(12)

Despite the challenges associated with transitioning users and organizations to contemporary authentication methods, the escalating threats and attacks related to cyber risks underscore the necessity for more sophisticated solutions. Furthermore, the concept of passwordless authentication is becoming increasingly familiar as public cloud services, mobile providers, and applications, such as those offered by Amazon, Apple, and Google, readily provide these alternatives. This allows the public to authenticate their login and activities using biometric methods like fingerprints or facial recognition [6]. Organizations have the potential to capitalize on the practices that users already engage in across various aspects of their lives. However, the broader adoption and implementation of modern authentication techniques necessitate enhanced education regarding the convenience and security of passwordless options, user-friendly training, and dedicated time to assist users during the initial setup of these advanced methods.

2 Trends And the Shift Toward Stronger Authentication

Numerous companies in the present day are enhancing their cybersecurity measures in response to the increasing frequency of cyberattacks observed over the last decade. Research indicates that enhancing password protection techniques that extend beyond the conventional username and password framework is effective in thwarting unauthorized access. As cyberattacks evolve in sophistication, depending solely on passwords is insufficient to safeguard company data [7]. Although the basic username and password method remain prevalent, many organizations are starting to implement more secure authentication strategies. Password managers represent another tool that provides a level of password protection. Rather than reusing identical passwords or attempting to recall multiple passwords for various logins, a password manager consolidates them all under a single master password. However, this approach has faced criticism, as compromising the master password would also jeopardize all other stored passwords. These trends illustrate the transition towards more robust and convenient methods of data protection. While there are numerous strategies to enhance a company's cybersecurity, three methods have been identified as particularly effective: multifactor authentication, biometric authentication, and hardware security keys.

Multifactor authentication is rapidly becoming one of the most widely adopted security measures across various industries, necessitating that users confirm their identity through two or more steps during the login process. Google first implemented this method in 2011 and has recently made it a requirement for all customers accessing Google Cloud, aiming to safeguard sensitive information [8]. Typically, this procedure entails obtaining a verification code or notification sent to the registered phone number or email for login purposes. The intent of this additional step is to mitigate the risk of unauthorized access, even in cases where the password may have been compromised.

Biometric authentication enables users to access their accounts through distinctive physical characteristics, such as fingerprints or facial features. This technology gained popularity following Apple's launch of the Touch ID feature on iPhones in 2013, which permitted users to log in with their finger rather than relying on traditional passwords or codes. The facial recognition systems employed by numerous companies, including Apple, are engineered to thwart prevalent spoofing methods. These systems can identify three-dimensional faces, reject two-dimensional images, and require that the user's eyes remain open for access [9]. Additionally, fingerprint scanners possess the capability to sense body heat and authentic skin, making it challenging for individuals to gain unauthorized access using replicas.

Hardware security keys are tangible devices utilized for logging in, serving either as a substitute for or an enhancement to the conventional password. These security keys typically take the form of USB devices or Near-Field Communication (NFC) enabled cards, which can be either inserted into or tapped against a device. A prominent example of this effective security approach is the YubiKey, widely adopted by numerous major corporations, including Google. In fact, Google reported in 2017 that after mandating all employees to utilize the security key, there have been no successful phishing attempts on employee accounts [10]. This method adds an additional layer of security, as it necessitates physical possession of the security key for login. Hardware security keys are regarded as one of the most reliable options for sectors that manage sensitive data, such as finance, technology, and human resources [11].

As cyberattacks grow increasingly sophisticated, it is imperative for companies to proactively implement advanced security measures to safeguard against both current and emerging threats. The transition towards more robust authentication methods signifies a wider acknowledgment that digital security has transitioned from being optional to becoming essential for a successful business and fostering customer loyalty. Organizations that allocate resources to these technologies illustrate their dedication to maintaining customer trust by ensuring the protection of their data. Although there are numerous strategies to enhance an organization's cybersecurity, these authentication methods have consistently demonstrated their effectiveness in decreasing the frequency of attacks across various industries, as evidenced in Figure 2 [12].

Department	MFA Adoption (%)	Phishing Incidents Reduced (%)
HR	85%	72%
Finance	92%	78%
IT	95%	85%

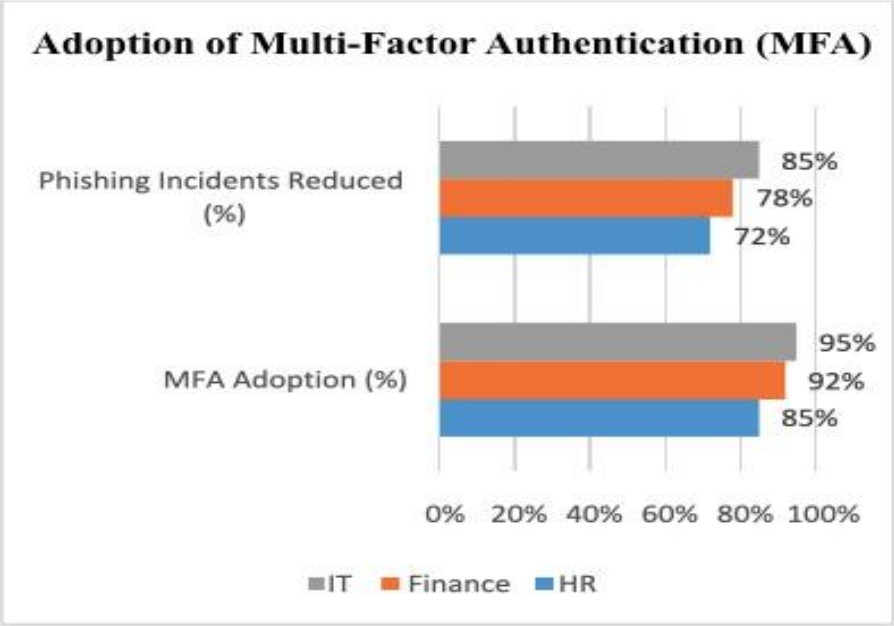

Figure 2: Shaheen et al. (2025). Data privacy in HR: Securing employee information in U.S enterprises using Oracle HCM Cloud. *International Journal of Research Radicals in Multidisciplinary Fields, 3*(2)

3 Challenges And What Is Holding Back Modern Authentication

Despite the increasing recognition of the shortcomings associated with password-based security, the adoption of contemporary authentication techniques, including biometric authentication, multi-factor authentication (MFA), and hardware security keys, presents a significant challenge for organizations regarding risk-based access. These challenges stem not only from user behavior but also from technical constraints, the preparedness of infrastructure, financial considerations, and cultural obstacles.

One of the most urgent challenges is the disparity between awareness and implementation. Organizations may advocate for MFA or passwordless systems; however, the absence of enforcement mechanisms and adequate infrastructure frequently results in these solutions being underutilized. For instance, credential abuse remains one of the primary threat vectors, not solely due to weak passwords, but also because MFA is applied inconsistently across various systems and user groups [2]. This lack of consistency enables attackers to take advantage of systems where protections are either weak or absent.

In addition to enforcement deficiencies, user resistance continues to be a significant obstacle. Although users may recognize that fingerprint scanners or verification codes offer enhanced security, many view these systems as inconvenient or perplexing. Studies indicate that in developing regions, particularly where cybersecurity awareness is limited, such resistance can be even more pronounced [13]. Consequently, this results in low adoption rates, even when systems are designed to support modern authentication methods [5]..

The integration of technology presents a considerable challenge. Numerous legacy systems were not originally designed to accommodate biometric data, adaptive authentication methods (which modify verification criteria based on user behavior or context), or token-based login processes such as hardware

security keys. In cloud-based settings, identity verification must be synchronized across multiple platforms and endpoints, frequently necessitating custom development and collaboration with vendors [15, 14].

The financial implications of upgrading identity frameworks represent another significant hurdle, particularly for small and medium-sized enterprises. Costs encompass software purchases, hardware provisioning, employee training, and compliance management. These expenses can appear daunting, even in light of the long-term security advantages [15; 5].

Additionally, there are pressing issues regarding user privacy and data ethics. Unlike passwords, biometric identifiers cannot be altered once they have been compromised. Users are becoming increasingly apprehensive about how their facial scans, fingerprints, or behavioral data are stored and who has access to this information. In the absence of well-defined policies and secure data management practices, organizations risk undermining user trust [13].

Additionally, some tools marketed as "secure by design," Furthermore, certain tools promoted as "secure by design," like password managers, are frequently misinterpreted. Users might assume that keeping passwords in a single vault suffices, failing to recognize that without Multi-Factor Authentication (MFA), the vault itself turns into a single point of failure [1]. Awareness regarding these tools is scarce, particularly in organizations lacking specialized cybersecurity training.

The implementation of zero trust frameworks introduces both cultural and technical obstacles. These frameworks necessitate ongoing verification and detailed access control, which can hinder productivity if not executed correctly. Numerous companies are ill-equipped for the mindset shift required from implicit trust to continuous verification and neglect to provide the essential operational support [16].

Even well-structured authentication systems can be disregarded if the user experience is inadequate. Multi-layered logins, frequent prompts, or poorly integrated biometric processes can irritate users and compel them to find alternative solutions. In such scenarios, usability itself becomes a security vulnerability [15, 14].

In conclusion, moving towards modern authentication is not simply a technological enhancement; it requires comprehensive changes across the organization in training, infrastructure, and policy. For success, businesses must view the transition as both a cultural and operational transformation, as well as a technical upgrade..

4 People Drive Adoption Of Modern Authentication Methods

There are numerous opportunities for the increased adoption of contemporary authentication security methods, including MFA, biometric authentication, and hardware security keys among both users and organizations. Nevertheless, it is crucial to remember that the adoption and implementation hinge not solely on technology but also on human factors. Individuals are the primary contributors to successful cyberattacks, encompassing both cybercriminals and the millions of users with weak passwords. Furthermore, it is individuals who influence the utilization of security methods and determine which ones prevail in both domestic and professional environments. Enhancing workplace training, broadening educational and awareness initiatives, and lowering barriers to adoption begins with prioritizing people in the practices of implementation and adoption.

Users who adopt advanced security tools such as biometric and multifactor authentication frequently express feelings of trust, usefulness, and ease of use regarding these methods. This indicates that companies should take into account human behavior, attitudes, and emotions when disseminating information about non-password methods, as well as assisting individuals in comprehending the rationale behind more modern authentication techniques. Merely presenting facts and information may not motivate individuals to take action; rather, their emotional responses to a method are significant. Additionally, the simplicity of adoption will enhance how users perceive the integration of new methods. Research indicates that fingerprint, voice, and facial recognition options, which are now widely available on mobile devices and applications, have contributed to improved usability due to the rapid access and significant convenience they offer during login processes.

Raising awareness about contemporary authentication techniques and implementing extensive educational initiatives in workplaces and communities presents a significant opportunity for businesses to assist users in adopting more secure tools. When users possess a deeper understanding of these methods, coupled with a positive training experience, it fosters a more secure cyber environment [17]. Users can feel empowered to identify and effectively respond to cyber threats, as well as adopt superior authentication security practices that do not expose them to vulnerabilities [18]. By dedicating time to enhance digital literacy and educating

users about security methods, the incidence of human error that leads to cyberattacks can be significantly reduced.

Moreover, beyond increased awareness, training, and education, research indicates that users require direction on what they can discard and "unlearn." Users have been conditioned to rely on outdated or ineffective practices, such as passwords, making it challenging to abandon what they learned during their initial technological encounters. By demonstrating, rather than merely informing, users about real-world security breach incidents—particularly in finance or health—they may be more inclined to unlearn and adopt modern authentication techniques [18]. Rather than clinging to obsolete practices out of fear, users may be motivated to take action based on their newfound knowledge.

Finally, there exists a chance to further diminish obstacles to the adoption of contemporary authentication techniques by enhancing biometric and multifactor technologies to thwart bypassing methods [5]. Although numerous platforms and mobile applications incorporate user-friendly facial recognition, for instance, or multifactor authentication within their systems, users still possess various means to circumvent these measures and may choose to bypass them. Ongoing enhancements to intuitive interfaces that cater to diverse levels of digital literacy can significantly contribute to ensuring accessibility and user-friendliness [5]. Certain application developers advocate that multifactor authentication should be mandatory to safeguard both users and organizations [2].

5 The Cost of Weak Authentication

To enhance the understanding of the importance of secure authentication methods, it is beneficial to analyze several recent incidents involving major corporations. These incidents provide crucial insights for businesses regarding the necessity of safeguarding their systems and data.

In 2016, the Hollywood Presbyterian Medical Center in Los Angeles was among the numerous hospitals targeted in a ransomware attack [19]. Cybercriminals successfully installed a virus on the hospital's systems, encrypting their files. To regain access, the hospital was compelled to pay hackers a ransom of $17,000 in Bitcoin. Although it is reported that the breach began when an employee opened a phishing email, the absence of multifactor authentication enabled the hackers to completely compromise the hospital's systems.

In early 2024, cellular service provider AT&T and health insurance provider UnitedHealth Group experienced significant data breaches around the same time, also due to the lack of multifactor authentication. Hackers managed to penetrate one of AT&T's third-party platforms using stolen credentials. To avert the leakage of customer data, they reportedly paid a ransom of $370,000 and incurred a $130 million loss in market value as a result of the incident. Similarly, UnitedHealth's systems were breached through a comparable method, leading to widespread disruption of their healthcare services and jeopardizing the data and lives of many patients. The company disclosed that it paid a ransom of $22 million to prevent any data leaks [4]. Both occurrences underscore the vulnerabilities associated with traditional login methods and illustrate how effective modern secure authentication methods could have been in averting these crises.

One of the notable events that has transpired in recent years is the cyberattack executed by Salt Typhoon, a notorious Chinese hacking group. In late 2024, this group successfully infiltrated the systems of several U.S. cellular service providers, gaining access to sensitive customer data, including phone calls and text messages [20]. The companies affected include prominent names such as AT&T, T-Mobile, Verizon, and Consolidated Communications, all of which have been established in the industry for over two decades. Although they were compromised through advanced attacks, analysts suggest that these incidents might have been averted with the implementation of secure authentication methods.

These real-world instances of major corporations suffering significant losses underscore the necessity for every business to invest in cybersecurity measures to reduce the likelihood of an attack. From employees falling victim to phishing emails and the lack of multifactor authentication to vulnerabilities within infrastructure, each scenario illustrates how a single weak point can result in substantial financial loss, data breaches, or operational disruptions. Companies that do not evolve and embrace modern authentication techniques face risks that extend beyond mere inconvenience; they jeopardize their trust, reputation, and long-term viability. Moving forward, multifactor authentication, biometric authentication, and hardware security keys should be regarded as essential elements of conducting business in the digital era.

6 Conclusion

As cyber threats continue to rise, the dangers associated with outdated password-based authentication methods become increasingly pronounced. This paper has explored the significant transition towards contemporary authentication technologies, such as multifactor authentication, biometric verification, hardware security keys, and various passwordless solutions, which are vital for bolstering cybersecurity.

Current trends indicate that numerous leading organizations are embracing these tools to remain ahead of emerging threats. Nevertheless, the implementation process is fraught with challenges. Technical limitations, integration difficulties with legacy systems, budgetary constraints, user resistance, and privacy issues persist in obstructing widespread adoption. Despite these hurdles, there are considerable opportunities to enhance adoption through user-centered design, focused training, and extensive public education initiatives.

Real-world case studies illustrate both the costs of inaction and the advantages of implementing modern security measures. High-profile breaches reveal how inadequate, or nonexistent authentication protocols can result in substantial financial, operational, and reputational harm. In contrast, when effectively executed, modern authentication can successfully thwart sophisticated attacks and safeguard sensitive systems.

Ultimately, enhancing authentication transcends mere technical upgrades. It represents a strategic necessity. Moving forward, organizations must embrace a layered and user-aware approach to authentication that integrates technology, policy, and education. The journey towards stronger cybersecurity commences with re-evaluating how users access systems and investing in secure, scalable, and resilient authentication practices suitable for the digital era.

7 References

1. Albesher, A. S., Alkhaldi, A., & Aljughaiman, A. (2024). Toward secure mobile applications through proper authentication mechanisms. PLoS One, 19(12)https://doi.org/10.1371/journal.pone.0315201
2. Verizon, “Data Breach Investigations Report” [Online] Available: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf [Accessed 05 03 2015]
3. R. Holthouse, S. Owens, and S. Bhunia, The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies, Dept. of Computer Science and Software Engineering, Miami Univ., Oxford, OH, USA.
4. Rundle, J., & Stupp, C. (2024). Data Breaches Highlight Lack of Basic Cyber Controls; AT&T, UnitedHealth Group join a growing list of companies with hacks traced to the absence of one particular security measure: multifactor authentication. WSJ Pro.Cyber Security
5. Irfan, R., Shah, M., & Sinan, G. M. (2025). Strengthening Cybersecurity Resilience: An Investigation of Customers’ Adoption of Emerging Security Tools in Mobile Banking Apps. Computers, 14(4), 129. https://doi.org/10.3390/computers14040129
6. I. Gordin, A. Graur, S. Vlad, and C. I. Adomniței, Moving forward passwordless authentication: Challenges and implementations for the private cloud, Ștefan cel Mare Univ. Suceava, Romania.
7. Mapgaonkar, D. (2024). Digital authentication: 4 steps to move beyond passwords. WSJ Risk & Compliance Journal, https://deloitte.wsj.com/riskandcompliance/digital-authentication-4-steps-to-move-beyond-passwords-d526e404
8. Upadhyay, M. (2024). Mandatory MFA is coming to Google Cloud: Here’s what you need to know. Google, https://cloud.google.com/blog/products/identity-security/mandatory-mfa-is-coming-to-google-cloud-heres-what-you-need-to-know
9. Apple. (2023). About Touch ID advanced security technology. Apple, https://support.apple.com/en-us/105095
10. Krebs, B. (2018). Google: Security keys neutralized employee phishing. KrebsOnSecurity, https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
11. Lang, J. (2016). Security keys: Practical cryptographic second factors for the modern web. Google, https://www.researchgate.net/publication/306373685_Security_Keys_Practical_Cryptographic_Second_Factors_for_the_Modern_Web

12. Shaheen, N., Jaiswal, S., Chinta, U., Singh, N., Goel, O., & Chhapola, A. (2025). Data privacy in HR: Securing employee information in U.S enterprises using Oracle HCM Cloud. International Journal of Research Radicals in Multidisciplinary Fields, 3(2), https://www.researchgate.net/publication/390040166_Data_Privacy_in_HR_Securing_Employee_Information_in_US_Enterprises_using_Oracle_HCM_Cloud
13. Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A systematic literature review of the types of authentication safety practices among internet users. International Journal of Advanced Computer Science and Applications, 12(7), 500–506. https://www.proquest.com/docview/2655113137
14. Anitha, S., & Jayarekha, P. (2021). MultiStage authentication to enhance security of virtual machines in cloud environment. International Journal of Computer Applications, 174(10), 1–5. https://www.proquest.com/docview/2655113601
15. Mostafa, R., El-Alfy, E., & Alsulaiman, M. (2023). Strengthening cloud security. International Journal of Computer Applications, 176(2), 20–25. https://www.proquest.com/docview/2904646301
16. Kang, E., Mowbray, M., & Watanabe, Y. (2023). Theory and application of zero trust security: A brief survey. International Journal of Computer Applications, 175(3), 10–15. https://www.proquest.com/docview/2876465838
17. Zwilling, M.; Klien, G.; Lesjak, D.;Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. J. Comput. Inf. Syst. 2022, 62, 82–97. [CrossRef]
18. Gundu, T. (2024). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. Academic Conferences International Limited
19. Yadron, D. (2016). Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. The Guardian, https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center
20. Jaikaran, C. (2025). Salt Typhoon hacks of telecommunications companies and federal response implications. Library of Congress. https://www.congress.gov/crs-product/IF12798