國立臺北科技大學
National Taipei University of Technology

資訊安全碩士學位學程

碩士學位論文

Master of Science in Information Security

Master Thesis

將 FIDO2、零信任和多因素身份驗證應用於 B2C 電子商務：綜合研究

Integrating FIDO2, Zero Trust, and Multi-Factor Authentication into B2C E-commerce: A Comprehensive Study

研究生：吳建璋

指導教授：陳香君 博士

中華民國一百一十三年十二月

國立臺北科技大學
研究所碩士學位論文口試委員會審定書

本校 資訊安全學位學程 研究所 吳建璋 君

所提論文，經本委員會審定通過，合於碩士資格，特此證明。

學位考試委員會

委　　員：馬奕薇

吳和庭

陳香君

指導教授：陳香君

所　　長：陳昌珩

中 華 民 國　一百一十三　年　十二　月　四　日

ABSTRACT

Title: Integrating FIDO2, Zero Trust, and Multi-Factor Authentication into B2C E-commerce: A Comprehensive Study

Pages: 64

School: National Taipei University of Technology

Department: Master of Science in Information Security

Time: December, 2024

Degree: Master

Researcher: Chien-Chang Wu

Advisor: Shiang-Jiun Chen, Ph.D.

Keywords: FIDO2, Zero Trust, Multi-factor Authentication, E-commerce, B2B, B2C, Phishing, Resilience, Cybersecurity

E-commerce has rapidly evolved with technological advancements, creating numerous business opportunities. However, this growth is accompanied by evolving cybersecurity challenges, making protecting user information and identities increasingly critical. Traditional security methods are becoming inadequate against modern complex threats, such as the sharp rise in phishing attacks, the growth in Bring Your Own Device (BYOD) usage, and various sophisticated cyberattacks. Against this backdrop, there have been numerous applications of Zero Trust in enterprises, particularly in Business-to-Business (B2B) contexts for remote work during the pandemic, which has addressed many Virtual Private Network (VPN) related issues. Unlike B2B, in Business-to-Consumer (B2C) scenarios, users prioritize convenience while being concerned about security. Zero Trust is expected to become the foundational framework for future security measures. Therefore, leveraging Fast IDentity Online 2 (FIDO2) to reduce complexity and enhance security aligns with this trajectory. Despite the

widespread discussion and application of zero trust in enterprise environments, e-commerce research is relatively lacking. Therefore, this paper aims to investigate and validate the combined application of zero trust, FIDO2, and multi-factor authentication (MFA) in a B2C environment. This approach seeks to fill existing research gaps and provide higher levels of authentication and security while addressing the inconvenience that often accompanies enhanced security measures. Additionally, by integrating various MFA methods, this approach aims to increase system resilience and offer diverse options. This combined method is designed to enhance the overall security of e-commerce platforms while providing a more convenient user experience. As the risks continue to increase, users' concerns about the security of their personal information are also growing. The synergistic application of zero trust, FIDO2 technology, and MFA will offer a more secure and convenient solution, further promoting the development of e-commerce.

Acknowledgements

完成這篇論文的旅程充滿挑戰與成長，我在這段過程中不僅收穫了知識，更得到了來自各方的支持與陪伴，這些經驗與鼓勵讓我在追求學術目標的道路上得以堅持不懈。在此，我謹向所有曾幫助過我的人表達最誠摯的感謝。

首先，我衷心感謝我的指導教授陳香君教授。您的悉心指導與不懈鼓勵，使我能夠穩步完成這項研究。您不僅在學術上提供了專業的指導與寶貴的建議，更在生活中分享了許多寶貴的經驗，並給予我持續的關心與支持。這些經驗與智慧不僅幫助我克服研究上的困難，也讓我在面對生活挑戰時更有自信與坦然。

我要特別感謝我的家人，他們在我求學期間無條件地支持與鼓勵。無論是在我面對困難時的安慰，還是在日常生活中的陪伴，始終是我最堅實的後盾。你們的信任與包容讓我能全心投入學術研究，並在面對挑戰時充滿信心與力量。

此外，我也要感謝研究室的夥伴們與好友，因為有你們的陪伴，為原本枯燥的研究生活注入了豐富的色彩與溫暖，讓這段求學旅程更加充實且富有意義。在研究過程中，無數次的合作、討論與相互支持，不僅開闊了我的思維視野，也讓我深刻體會到團隊合作的力量與重要性。無論是在學術上的相互指導，還是在生活中的互相關懷，你們的鼓勵與幽默為我帶來無窮的動力，成為我生命中珍貴的回憶。

最後，我要感謝自己，在這段旅途中，我見證了自己的成長與突破，深刻體會到堅持與努力的價值。未來，我將帶著這段寶貴的經驗與教訓，勇敢迎接更多挑戰，追求更高的目標。

衷心感謝所有在這段旅程中給予我支持與幫助的人，正是因為有你們，這段時光才得以充滿溫暖與美好的回憶。

吳建璋 謹誌於

臺北科技大學資訊安全碩士學位學程

中華民國 113 年 12 月

Table of Contents

List of Tables

List of Figures

Chapter 1 Introduction

Due to the swift growth of e-commerce, we are facing new information security challenges [1-4]. Most customers opt for internet-based banking, shopping, sales, and procurement. While e-commerce systems offer numerous advantages and benefits, they also present challenges, one of the most significant being security. Current information security frameworks and protective software are increasingly inadequate in fully safeguarding our data and assets as attackers employ increasingly sophisticated methods. This makes us more vulnerable in this digital age [5]. The rising adoption of Bring Your Own Device (BYOD), phishing attacks, inherent password vulnerabilities, and social engineering attacks exacerbate the threat landscape.

In today's digitized work environment, BYOD strategies have significantly increased, becoming a standard practice for many enterprises. Research shows that more than 50% of organizations and more than 70% of employees rely on personal devices for work-related tasks, with these numbers growing quickly [6]. The COVID-19 pandemic has further accelerated this trend, with a 58% increase in BYOD usage during the pandemic [7]. The widespread adoption of BYOD is primarily due to its flexibility and productivity. However, this also leads to a sharp rise in security incidents associated with BYOD. Employees using personal devices to access company data expose corporate networks to various risks, including data breaches, malware, and cyberattacks [8]. Data breaches are considered the greatest security risk associated with BYOD, with 63% of respondents identifying it as a primary concern [7]. Research indicates that the financial losses enterprises suffer due to BYOD-related security incidents are increasing annually, highlighting the urgent need to strengthen security measures and strategies. For instance, Microsoft reported a more than 200% increase in human-operated ransomware attacks since September 2022 [9]. These studies and reports suggest that as BYOD becomes more prevalent, enterprises must implement stricter security policies and technologies to counter potential security risks and attacks effectively.

In recent years, phishing attacks have grown substantially in severity, becoming a significant cybersecurity threat for businesses and individuals. A Zscaler report revealed that phishing attacks rose by 47.2% in 2022 compared to the previous year, as cybercriminals employed more advanced methods to execute large-scale attacks [10]. Additionally, Kaspersky's data indicates a 40% growth in phishing attacks in 2023 [11]. Phishing websites impersonate legitimate sites or trusted institutions to trick users into providing personal information or sensitive data to obtain information or money illegally. The design of phishing websites is often highly sophisticated, closely resembling legitimate websites in appearance and functionality, making it difficult to distinguish them at first glance. These phishing sites commonly mimic banks, email service providers, social media platforms, and other well-known websites, leading users to believe they are real and subsequently enter their account

credentials. Once users input their personal information on phishing websites, scammers can easily access these sensitive details, leading to identity theft, financial fraud, and other criminal activities. Some phishing websites even use social engineering techniques, sending deceptive emails or messages to lure users into clicking on links to fraudulent sites. Phishing attacks constitute more than 80% of all reported security incidents [12]. These trends indicate that with the increase in remote work and digital communication, the phishing threat is intensifying, necessitating stronger cybersecurity infrastructures and proactive measures to mitigate this growing threat.

For decades, we have sought more secure alternatives to replace text-based passwords as the optimal solution for end-user authentication in online environments. Despite numerous attempts, a truly compelling alternative has yet to be found that matches passwords' deployability and usability [13]. Text-based password authentication, introduced in the 1960s to control access to mainframes, was initially considered an effective solution [14]. However, over time, passwords have become vulnerable to various security threats and attacks [15], driving the continuous pursuit of more advanced and secure authentication mechanisms.

A. Disadvantages of Passwords

1. Weak Passwords

Using weak, straightforward passwords can lead to data breaches, account takeovers, and other cyberattacks. To secure accounts, users should follow best practices for password security. Passwords must be strong, incorporating a mix of uppercase and lowercase characters, numbers, and special symbols, and they should be of adequate length. Users must refrain from using easily guessable information like birthdays, names, or addresses as their passwords. Additionally, using different passwords for each website or application is crucial to ensure that others remain secure even if one account is compromised. Besides using complex passwords, users should also change their passwords regularly to reduce the risk of attacks.

2. Guessing Passwords

Password guessing has always been a significant issue in cybersecurity. Attackers can employ various methods to guess users' passwords, including brute force and dictionary attacks. When users' passwords are overly simple or highly predictable, their accounts become susceptible to breaches. In recent years, with the advancement of artificial intelligence (AI) technology, password-guessing attacks have become more intelligent and effective. AI can analyze users' behavior patterns and preferences to generate more likely passwords, increasing the probability of successful breaches. Additionally, AI can continuously learn and optimize algorithms to enhance cracking speed and efficiency. For instance, PassGAN, developed by B. Hitaj et al. [16], utilizes generative adversarial networks (GAN) to mimic human password creation. This deep learning approach has achieved significant success in effectively generating and cracking passwords.

3.Social Engineering Techniques

Social engineering is a dangerous and covert attack method where attackers deceive or manipulate users into divulging their passwords. This attack exploits users' trust or entices them to perform actions that lead to the disclosure of account information. Social engineering attacks include impersonating trusted individuals or institutions, sending phishing emails or messages, and masquerading as legitimate entities to commit fraud. Attackers often exploit users' trust in specific institutions or individuals to deceive them into voluntarily providing their account information. This traps users and causes significant losses for individuals and enterprises.

4. Managing Password Overload

In today's digital world, individuals must keep track of multiple passwords and accounts for various online activities, including e-commerce, social networking, and online banking. Recent studies indicate that the average person manages a rapidly growing number of passwords, with personal users averaging 168 passwords and workplace users averaging 87. Considering the total number of passwords for individuals and enterprises, this figure may reach 255 [17]. Moreover, users spend approximately 10.9 hours annually on password entry and resets, leading to an average yearly productivity loss and labor cost of $5.2 million for businesses [18]. However, due to the diversity and complexity of passwords, many people may encounter issues with forgetting passwords. This phenomenon can be attributed to too many different passwords, making them difficult to remember. Moreover, to enhance security, people often need to change passwords regularly, increasing the risk of forgetting them. Therefore, to address password management challenges, there is a continuous need to find more secure and convenient authentication methods.

However, enhancing our security measures often leads to inconvenience and additional costs. Furthermore, different security methods might introduce new vulnerabilities, making systems susceptible to novel attacks and threats. This situation highlights the significant challenge of relying on a single authentication method. As a result, a more comprehensive, robust, and resilient security framework is urgently required to confront the constantly changing threat landscape. This new security mechanism should balance security and convenience and provide effective protective measures to combat various threats in the modern cyber environment.

In this context, we aim to find a method that offers user convenience and security. This is where the advantages of Fast IDentity Online 2 (FIDO2) technology and the Zero Trust concept come into play. FIDO2 allows users to log in more conveniently and securely, while the Zero Trust model provides stricter access control and continuous verification to ensure the security of personal data. Incorporating various multi-factor authentication (MFA) methods can further enhance security and flexibility. This integration offers a resilient and secure framework.

Despite the widespread discussion and application of zero trust in enterprise environments, research focusing on e-commerce is relatively lacking. With the rapid growth

of e-commerce, future attacks are expected to become more frequent. The primary distinction between Business-to-Consumer (B2C) and Business-to-Business (B2B) e-commerce lies in the importance of convenience. Therefore, this paper aims to explore and validate the integrated application of zero trust, FIDO2, and MFA in a B2C environment, addressing existing research gaps. Such research not only aims to enhance the security of e-commerce but also to provide a better user experience.

Therefore, this paper will explore how to leverage FIDO2 technology and apply the Zero Trust concept in e-commerce to achieve higher security and user convenience. We will examine the working principles of FIDO2 technology, discuss key concepts and best practices of Zero Trust, and introduce various MFA methods to ensure data and transaction security. This will help us better address current information security challenges without sacrificing user experience and convenience.

The remainder of this paper is structured as follows. Chapter 2 introduces the evolution of FIDO technology, covering the UAF, U2F, and FIDO2 protocols and their associated components, such as CTAP and WebAuthn. It also comprehensively examines the theoretical basis and practical uses of Multi-Factor Authentication (MFA) and the Zero Trust architecture, further discussing the implementation challenges of Identity and Access Management (IAM) systems and account recovery mechanisms. Chapter 3 analyzes the key characteristics and security challenges of B2C e-commerce platforms, introducing the QuickSecure Access (QSA) system architecture and its operational processes, emphasizing balancing security, convenience, and usability. Chapter 4 presents examples and applications from various domains, comparing the implementation of FIDO, Zero Trust, and MFA across different scenarios. Finally, Chapter 5 concludes the findings of this research, and Chapter 6 explores future research directions.

Chapter 2 Background

2.1 Fast IDentity Online (FIDO)

Fast IDentity Online (FIDO) is an emerging authentication technology aimed at enhancing the security and convenience of online authentication. Founded in July 2012, the FIDO Alliance [19] comprises major global technology companies such as Google, Microsoft, and PayPal. The alliance aims to establish a unified authentication standard that allows users to verify their identities using multiple authentication methods, thereby reducing the risks of password leaks and identity theft. Its specific objective is to develop robust authentication standards to lessen reliance on passwords. This framework has been widely adopted in recent years, enabling users to authenticate themselves to remote online services and websites using locally trusted authentication methods (e.g., fingerprints or facial recognition on smartphones).

The core concept of FIDO technology involves using public/private key pairs for authentication instead of traditional passwords. When a user registers, the system generates a pair of public/private keys, with the private key stored on the user's device and the public key stored on FIDO-authenticated servers. During authentication, the system uses the public key encryption method to verify the user's identity, completing the authentication if the private key matches successfully. FIDO technology offers several advantages. Firstly, it enhances authentication security since the user's private key never leaves their device. Secondly, it improves user experience by eliminating the need to remember complex passwords, relying instead on their devices for authentication. Additionally, many websites and service providers have begun supporting FIDO standards, allowing users to authenticate using biometrics (such as fingerprints or facial recognition) or hardware security keys (like USB security keys). There are now over 600 certified FIDO products on the market [20]. As a result, users are relieved

from the need to remember complicated passwords or be concerned about them being stolen or compromised.

FIDO technology represents a revolutionary authentication method that enhances online authentication's security and convenience. As more companies and organizations adopt this technology, and more services support FIDO (e.g., Amazon, Google, Discord [21]), its widespread adoption and application are further encouraged. Over 350 companies have already become members of the FIDO Alliance [22]. It is believed that FIDO technology will soon become the mainstream method for online authentication, offering users a more secure and convenient online experience. The initial FIDO protocol suite comprised two specifications: Universal Authentication Framework (UAF) and Universal Second Factor (U2F), which will be discussed separately below.

2.1.1 Universal Authentication Framework (UAF)

The Universal Authentication Framework (UAF) [23-25] is an open standard for web authentication. It aims to provide a secure and convenient method for users to authenticate themselves across different websites and applications. UAF allows users to register accounts with relying parties using trusted authenticators, replacing traditional password-based login schemes. UAF integrates biometric authentication to offer users a seamless, password-free login experience. By installing FIDO UAF on their devices, users can opt to authenticate online using biometric identifiers such as fingerprint recognition, voice recognition, or a personal identification number (PIN), thus bypassing the traditional method of entering lengthy passwords. This enhanced authentication method strengthens security and user experience by enabling seamless access through biometric data. Security analyses of the UAF protocol have identified several vulnerabilities. H. Feng et al. [24] provide specific recommendations to address these issues, ensuring a more robust and secure implementation.

2.1.2 Universal Second Factor (U2F)

Universal Second Factor (U2F) [26] is an authentication technology designed to enhance network security by providing a simple yet powerful method to ensure that only authorized users can access their accounts. U2F enables two-factor authentication (2FA), requiring users to supply a second authentication factor in addition to their username and password to verify their identity. The robust second factor enables services to simplify passwords, such as using a 4-digit PIN, without sacrificing security. Additionally, these additional factors include devices connected via Universal Serial Bus (USB), Near Field Communication (NFC) for close-range wireless communication, and Bluetooth Low Energy (BLE) for mobile devices [27], thereby enhancing the security of the login process. Such security measures protect users' personal data from unauthorized access and hacker attacks, enhancing network security, preventing phishing attacks, and safeguarding user privacy. Therefore, using two-factor authentication is a highly effective method to ensure the security of online accounts, enabling users to use web services confidently.

2.2 Fast IDentity Online 2 (FIDO2)

Fast IDentity Online 2（FIDO2）, jointly developed by the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C), is an open identity authentication standard aimed at replacing password-based authentication systems. Building upon FIDO Alliance's previous work on the Universal 2nd Factor (U2F) standard, FIDO2 was officially introduced in 2018, incorporating the Web Authentication (WebAuthn) specification and the Client to Authenticator Protocol (CTAP) [28].

FIDO2 consists of two sub-protocols: W3C Web Authentication (WebAuthn) allows websites and applications to authenticate users using robust public key cryptography, while CTAP ensures secure communication between devices and browsers. This combination

enhances security and improves user experience by eliminating reliance on vulnerable passwords. The FIDO Alliance now manages communication between clients and authenticators, delegating the responsibility for server-client communication to the W3C. This strategic adjustment enhances the scalability of FIDO-based authentication. Currently, FIDO2 authentication is compatible with major operating systems, such as Windows, Linux, macOS, Android, iOS, and ChromeOS [29] and all major web browsers , including Google Chrome, Apple Safari, Microsoft Edge, Mozilla Firefox, and Opera) [30]. By 2023, the adoption of FIDO authentication will significantly increase, enabling more than 7 billion online accounts to support passwordless logins, highlighting a trend towards more secure and user-friendly authentication methods [31].

Due to its security benefits, passwordless authentication is widely adopted in sensitive areas such as banking applications. Many banking apps have phased out passwords and instead utilize biometric technology or passwordless authentication [32]. Visa has introduced payment passkeys, allowing customers to authorize payments online by scanning biometrics on smartphones or computers [33]. Here are some applications of FIDO2.

Sugimoto and Ogino [34] discuss the benefits of implementing FIDO2 in educational institutions to address increasing phishing attacks in campus environments.

M. Kepkowski et al. [35] explores the challenges and opportunities of FIDO2 in enterprise settings. While FIDO2 excels in preventing phishing, issues like integrity in production environments and account recovery still need to be addressed.

2.2.1 Client-to-Authenticator Protocols 1 (CTAP1)

The FIDO Alliance retained the U2F standard within FIDO2. It renamed Client to Authenticator Protocol 1 (CTAP1) to enable cross-platform two-factor and multi-factor authentication, enhancing network security and user convenience.

2.2.2 Client-to-Authenticator Protocols 2 (CTAP2)

Client-to-Authenticator Protocol 2 (CTAP2) forms an integral part of the FIDO2 standard, expanding upon the capabilities of CTAP1 with enhanced support for authentication device types and security features. It enables a broader range of devices, such as mobile devices and embedded fingerprint scanners, to function as authenticators. Unlike CTAP1, CTAP2 supports single-factor, second-factor, and multi-factor authentication methods. Additionally, CTAP2 introduces two crucial security features: User Presence, which verifies the user's physical presence, and User Verification, which ensures the user's identity can be confirmed. These features are crucial for preserving the security integrity of the authentication process. CTAP2 ensures interoperability among authenticators produced by different manufacturers, allowing seamless integration of various devices and technologies under the FIDO2 standard. Furthermore, it establishes a robust foundation for future expansions in authentication technologies.

2.2.3 Web Authentication (WebAuthn)

Web Authentication (WebAuthn) [36] is a JavaScript API that enables developers to implement robust authentication mechanisms on FIDO-supported browsers or cloud platforms. With WebAuthn, users can log into various application services using methods such as biometrics and app-based authentication. Currently, mainstream browsers like Google Chrome、Apple Safari、Microsoft Edge、Mozilla Firefox, and Opera all support WebAuthn [30]. As more websites adopt WebAuthn, services such as Dropbox, Microsoft accounts, Google accounts, Twitter, and others [37] provide powerful second-factor authentication based on FIDO2. These advancements demonstrate WebAuthn's potential to enhance security and user experience, laying the foundation for future authentication technology developments. The introduction of this API allows web services to more effectively mitigate password leaks

and other security threats, while providing users with a simpler and more secure login experience.

2.2.4 FIDO2 Registration and Login

FIDO2 provides a secure and convenient identity authentication solution through public key encryption technology. As illustrated in Figure 2.1, users start a registration request during the registration process. The client then requests a registration challenge from the server. The server generates the challenge and returns it to the client, along with the configuration information of the user's device. Subsequently, the client sends the challenge to the FIDO authenticator. The user undergoes identity verification through the authenticator and generates a pair of public keys (PK) and private keys (SK). The user's SK is securely stored on the device, whereas the PK is transmitted to the server. The server verifies the validity of the PK, associates it with the user's account, and stores the PK for future authentication purposes.

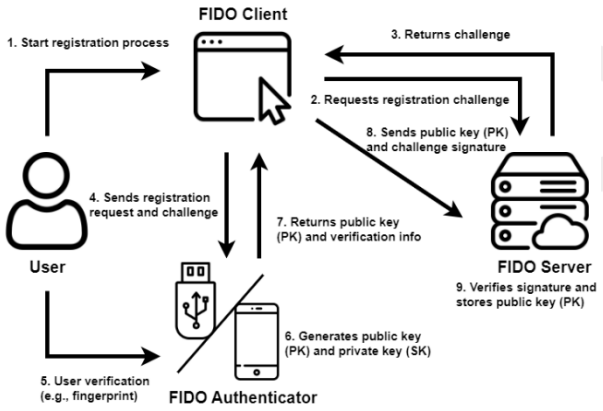

Figure 2.1 FIDO2 Registration

During the login process, as illustrated in Figure 2.2, the user starts a login request, and the client requests an authentication challenge from the server. The server generates the challenge and returns it to the client. The client then sends the challenge to the FIDO authenticator. The user undergoes identity verification through the authenticator, which utilizes the SK to sign the challenge and returns the signature to the client. The client sends

the signature and the user's PK to the server. The server verifies the validity of the signature using the PK. If the verification is successful, the server grants the user access permissions, completing the login process.

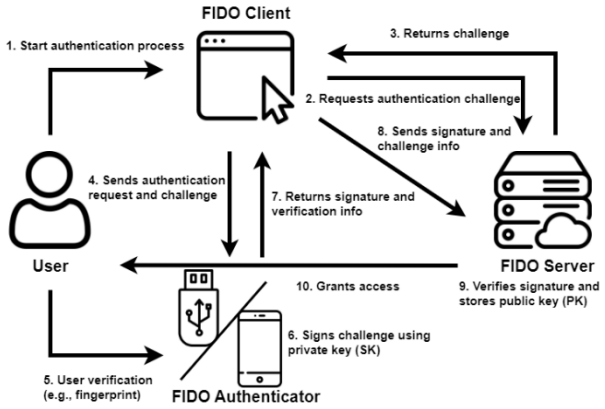

Figure 2.2 FIDO2 Login

This process is designed to offer the highest level of security while maintaining user experience convenience, making FIDO2 one of the most forward-thinking identity authentication standards today.

2.3 Multi-factor authentication (MFA)

Multi-factor Authentication (MFA) is a security technology designed to ensure user identity security by combining multiple authentication factors. Traditional single-factor authentication relies on only one factor the user provides, such as a password or PIN, making systems more vulnerable to breaches and unauthorized access. MFA enhances security by incorporating multiple factors, making it more difficult for attackers to gain access through password guessing or phishing attacks. MFA is widely applied across various domains, including online banking [38], email, social media, and enterprise applications. Many large organizations and institutions have adopted MFA to protect their data and systems from unauthorized access. Numerous government and financial institutions also mandate MFA for users to strengthen identity verification security. Despite its ability to enhance security, MFA

can also introduce some inconvenience for users. For instance, users may need to enter a password and a one-time code each time they log in, which can increase the time and effort required. Therefore, designing an MFA system requires balancing security and user-friendliness to ensure that users can easily and conveniently use the system while maintaining high security levels. The following outlines four authentication methods: Something You Know, Something You Have, Something You Are, and Somewhere You Are.

2.3.1 Something You Know - Knowledge Factor

The "Something You Know" authentication factor emphasizes the use of information known to the user to verify their identity effectively. This factor relies primarily on the user's memory and includes various authentication methods such as passwords, PINs, security questions, and image recognition.

A. Passwords

Among knowledge-based factors, passwords are the most widely used method. However, the security issues associated with passwords have long been a primary challenge for account security. Since the rise of personal computers and the internet, the limitations of password-based authentication have become evident. Numerous studies have pointed out the weaknesses associated with password-based security measures. Passwords are prone to phishing attacks and need to be securely stored by the authentication service, which adds an extra layer of security challenges [39].

B. Personal Identification Numbers (PINs)

Another password-related knowledge factor is the Personal Identification Number (PIN), which can be numeric or alphanumeric. PINs are often used with smart cards or local devices and are typically shorter than passwords. Unlike passwords, PINs are never transmitted to remote systems and serve solely as a local authentication factor, often paired with secure devices like smart cards. When you enter a PIN on a local device, the system converts it into

a specific form and compares it to the same form stored on the device. If they match, the system grants access. This method ensures that even if someone intercepts your PIN, they cannot use it without duplicating the special form. For example, when a user enters a PIN at an ATM, the system converts it into an encrypted form and compares it with the form stored on the smart card. Despite the possibility of attacks focusing on the smart card or secure device, the physical component limits the number of authentication attempts, making PINs relatively reliable, especially when used with smart cards or secure devices.

M Zhou et al. proposed a novel PIN authentication technology called PressPIN [40], which enhances PIN authentication on mobile devices through structure-borne sounds generated by the pressure of the user's finger. Since most mobile phones lack pressure-sensitive touch screens, they utilized structure-borne sounds to estimate pressure on the screen. This method increases the complexity and security of PINs, making them harder to guess through observation or video recording, thereby improving security. Experiments showed that PressPIN has a high accuracy rate in verifying legitimate users (up to 96.7% within two attempts) and strong resistance to various attacks (attack success rate only 2.5%). PressPIN does not require additional hardware and can be easily integrated into existing mobile authentication systems.

T Van Nguyen, N Sae-Bae, and N Memon. introduced Draw-A-PIN [41], a system that authenticates users on touch devices by drawing a PIN with their finger. This method leverages drawing characteristics or behavioral biometrics as additional verification factors, enhancing the security of PINs. Experiments indicated that Draw-A-PIN could achieve an equal error rate of 4.84% even when the attacker knows the PIN. User studies based on the System Usability Scale questionnaire confirmed the high usability of this system.

C. Security Questions

Besides passwords and PINs, other knowledge factors include security questions [42]. These pre-set questions and answers known only to the user serve as an additional layer of

authentication when setting up an account. The security of this method relies not only on the user choosing strong questions and answers but also on providing a fallback option for when the primary authentication method (e.g., password) is forgotten, ensuring that the account can still be correctly authorized.

2.3.2 Something You Have - Possession Factor

The "Something You Have" authentication factor emphasizes the use of physical devices or tokens possessed by the user to effectively verify their identity. This factor relies on the actual ownership of physical items, such as mobile devices, security tokens, smart cards, or other unique hardware devices, which are used as the basis for authentication. These items are typically combined with other authentication factors, such as passwords or biometrics, to enhance security. As a result, "Something You Have" not only provides an additional layer of security but also offers more reliable protection for access to resources or sensitive information.

A. Smart Cards and Fingerprint Authentication

Smart cards are a common example of the "Something You Have" factor. TC Clancy, N Kiyavash, and DJ Lin. [43]proposed a secure authentication system based on fingerprints and smart cards. This system utilizes Juels and Sudan's fuzzy vault scheme to construct a fingerprint vault, enhancing the security of fingerprint data used as a key. When a fingerprint matches, it achieves zero unlock complexity for legitimate users while increasing the unlock complexity for attackers by 269 times. This combination of smart cards and biometrics exemplifies the robust security offered by MFA.

The application scope of "Something You Have" is broad, spanning from personal computers to enterprise-level systems, to protect access to sensitive information. This authentication method is particularly indispensable in industries with high security requirements, such as finance, healthcare, and government. In these sectors, physical or virtual

tokens, such as one-time passwords (OTP) or time-based one-time passwords (TOTP), are widely used.

B. One-Time Password (OTP) and Time-Based OTP (TOTP)

OTP and TOTP are popular implementations of the "Something You Have" factor. In their study, CY Huang, SP Ma, and KT Chen. [44]proposed a method to reduce the incidence of phishing attacks by using OTP for user authentication instead of relying on fixed user-set passwords. These OTP are delivered through real-time messaging services or other widely available communication infrastructures, minimizing deployment costs and enhancing the solution's practicality.

Similarly, R Danthy, KP Pai, and V Rao. [45]proposed an innovative method for securing online banking authentication using TOTP. This method encrypts user credentials with time-based OTP, bolstering the security of online banking systems against common attacks such as replay attacks, brute force attacks, rainbow tables, packet sniffing, and random guessing.

In summary, the "Something You Have" factor significantly enhances authentication security by leveraging physical devices or tokens that are difficult for attackers to replicate or steal. When combined with other authentication factors, it provides a comprehensive and robust approach to safeguarding sensitive information and resources across various sectors.

2.3.3 Something You Are - Biometric Factor

The "Something You Are" authentication factor emphasizes the unique characteristics of the user themselves, making it another crucial authentication method. This method relies on the user's biometric or physical characteristics, including fingerprint scanning, facial recognition, iris scanning, voice identification, and vein pattern analysis. These biometrics are unique and constant for each individual, making them effective in distinguishing between different users. Biometric authentication technologies identify and verify users' identities by scanning, matching, and analyzing their unique biological traits. Compared to traditional

password authentication, biometric technologies are more convenient and secure because they do not require users to remember complex passwords or change them frequently. Moreover, biometric features are difficult to mimic or forge. Systems can more reliably verify users ' identities through the "Something You Are" authentication method, enhancing security. This method is commonly used in high-security applications such as financial institutions, government agencies, and healthcare facilities.

The "Something You Are" authentication method is continuously evolving and improving. With technological advancements, biometric systems have become more precise and reliable, and their applications have expanded. For example, facial recognition technology has significantly progressed in recent years, becoming a common authentication method in many smartphones and computer systems. Despite its many advantages, the "Something You Are" authentication method also faces challenges and limitations. The reliability and accuracy of biometric technologies can be affected by external factors such as lighting, angles, or noise. Additionally, users' biological traits may change over time due to injuries or aging, affecting authentication accuracy.

D Bhattacharyya et al. [46]provided an overview of biometric authentication technologies' current state and applications. The article notes that while biometrics offer high security and convenience, they also face challenges such as privacy protection and error rates in identification.

S Hemalatha. [47]systematically reviewed fingerprint-based biometric authentication systems, highlighting that while fingerprint templates are highly reliable for identity verification, probabilistic features in the matching process can lead to false rejection rates (FRR) and false acceptance rates (FAR). Improvements in image enhancement and recognition algorithms are needed to reduce these error rates.

M Bicego et al. [48]explored using Scale-Invariant Feature Transform (SIFT) features for face authentication, proposing three different matching techniques. The results showed

that the regular grid-based matching method outperformed the other two. Although it did not achieve the performance of the best face classifiers, it demonstrated the potential application of SIFT features in this context.

H Li et al. [49]proposed VocalPrint, a system utilizing millimeter-wave biometric detection for voice authentication. By capturing and analyzing vocal cord vibrations near the user's throat, VocalPrint achieved over 96% accuracy in authentication and demonstrated robustness against complex noise interference and spoofing attacks.

SW Shah et al. [50]introduced the Vein-ID (VID) system, which uses the vein patterns on the back of the hand for human identification. They captured depth information and infrared images using commodity depth cameras and designed two deep learning models for accurate identification and intruder detection. Their tests showed that VID achieved an average accuracy of over 99% in groups of up to 35 people and was able to detect intruders with about 96% accuracy.

As part of MFA, the "Something You Are" method provides a reliable mechanism for identity verification, effectively preventing unauthorized access and identity forgery. Through continuous innovation and improvement, this authentication approach will remain crucial across various sectors, providing higher levels of security for users and systems.

2.3.4 Somewhere You Are – Location Factor

The "Somewhere You Are" authentication factor emphasizes the user's current location as a basis for verifying their identity. This location-based authentication method typically uses technologies such as GPS, IP addresses, and Wi-Fi positioning. When a user attempts to log in or perform a sensitive operation, the system may request authorization to access their current location information to confirm whether the user is within an expected geographic range.

L Fridman et al. [51]explored active authentication on mobile devices using a multi-

modal approach that includes GPS location, stylometry, application usage, and web browsing behavior. Their research found that although the GPS modality had the lowest trigger rate, it significantly enhanced the overall performance of the fusion system, improving the accuracy of unauthorized user detection.

DH Choi, H Kim, and K Jung. [52]proposed a mobile IP authentication method based on a simple identification scheme using one-way functions. This approach effectively prevents replay and man-in-the-middle attacks without requiring mobile nodes to perform public-key cryptographic operations, thus enhancing implementation efficiency.

MN Aman, MH Basheer, and B Sikdar. [53]introduced a location-based two-factor authentication protocol designed for IoT devices, addressing the security needs of these resource-constrained environments. The protocol employs Physically Unclonable Functions (PUFs) to establish a root of trust and uses the IoT node's current geographic location as a second factor for authentication. Their study demonstrated that this location-based protocol can efficiently and accurately verify IoT device locations within a small area and effectively prevent impersonation and other attacks with low computational overhead and energy consumption.

The primary advantage of location-based authentication is its ability to provide enhanced security and improved user experience. By confirming the user's location, systems can prevent account hijacking or identity forgery. Additionally, this method allows users to complete the authentication process quickly and conveniently without remembering complex passwords or carrying additional hardware devices. Location-based authentication is crucial for ensuring security in zero-trust environments. Access permissions consider the user's physical location, requiring users to be in specific locations to access certain applications and services. By integrating location-based authentication within a multi-factor framework, systems can achieve a balanced approach that enhances security while ensuring user accessibility and ease of use. As part of a holistic security strategy, location-based authentication adds an essential

layer that can adapt to the evolving landscape of digital threats.

MFA offers a robust security mechanism by combining multiple authentication factors, including the Knowledge Factor (something you know), Possession Factor (something you have), Biometric Factor (something you are), and Location Factor (somewhere you are). Each method has its strengths and weaknesses, but they provide a higher level of security while maintaining user convenience and a positive user experience. As technology advances and innovates, MFA will play a critical role in protecting sensitive information and system security, becoming an essential tool to combat increasingly sophisticated security threats.

SW Shah and SS Kanhere. [54]discussed recent trends in user authentication, particularly for personal devices, online services, and smart environments. They highlighted the vulnerabilities of traditional authentication mechanisms and proposed various new methods. Their survey provides a comprehensive overview of the literature and guides future research directions.

2.4 Zero Trust

As commercial internet, cloud computing, mobile communications, the Internet of Things (IoT), and remote work policies have expanded, businesses are encountering growing data security challenges. In such an environment, traditional defensive security measures are no longer adequate to address the ever-growing and evolving threats. Consequently, many enterprises are adopting a new security model—Zero Trust. Adopting Zero Trust greatly reduces the risks associated with unauthorized access, internal threats, and malicious attacks.

Zero Trust (ZT) is a revolutionary network security architecture and objective. Its core philosophy is that all transactions, entities, and identities are considered untrustworthy until verified, aiming to minimize potential security risks. This network paradigm fundamentally differs from traditional security notions, which presume the network to be secure until a breach is detected. In contrast, the Zero Trust strategy posits "never trust, always verify" [55][56].

This security model asserts that organizations should not automatically trust anything inside or outside their networks. Every connection, user, or asset is treated as a potential threat and is rigorously verified and authorized, ensuring absolute security through complete distrust.

The traditional security model is often likened to a medieval castle, fortified with thick walls, moats, and a single guarded entrance and exit. In this model, everything outside the walls is deemed potentially dangerous, whereas everything inside is considered trustworthy. Once past the gate, anyone could freely access the castle's resources. John Kindervag, an analyst at Forrester Research, introduced the Zero Trust concept in 2009, asserting that "trust is a vulnerability," which, like all vulnerabilities, should be eliminated [57][58]. Over the years, as businesses across various industries transitioned to more stable foundations, Zero Trust gained increasing support. Zero Trust evolved from a security enhancement discussion into a widely adopted approach to bolster organizational security globally in just a decade. According to a 2021 report by Microsoft, 76% of organizations had started implementing Zero Trust strategies, with 35% reporting full implementation [59]. Okta's 2022 Zero Trust status report also found that 97% of companies either had a Zero Trust plan or planned to implement one within the next 18 months [60]. According to an Environmental, Social, and Governance (ESG) research report, 43% of North American organizations saw improved Security Operations Center (SOC) efficiency after implementing Zero Trust plans [61].

Zero Trust is not a single product but an information security strategy based on distrusting all users and entities until verified. The Zero Trust model ensures stringent access control at all organizational levels, including networks, applications, and data access points. Everyone must undergo rigorous scrutiny, with no exceptions, ensuring every access grant is meticulously verified.

Traditional security methods often focus on protecting the "attack surface," but this approach has proven impractical due to modern attack surfaces' dynamic, complex, and unpredictable nature. Conversely, Zero Trust aims to secure the "protect surface," which

consists of the specific combination of an organization's data, assets, applications, and services (DAAS) [62]. The protected surface is significantly smaller and entirely knowable than the attack surface, making it easier for organizations to defend against various attacks and effectively reduce risks.

Another critical advantage of Zero Trust is its ability to help organizations better understand their protected surface. By comprehensively understanding the protection surface, organizations can better assess their security risks and take appropriate measures to enhance their defenses. Moreover, Zero Trust aids in better prevention and response to security threats. Since the protected surface is entirely knowable, organizations can more easily detect and monitor potential attack behaviors and promptly take responsive actions, minimizing losses and risks.

Implementing Zero Trust requires substantial organizational resources and effort, including technical, human, and financial support. Furthermore, organizations must collaborate with vendors, partners, and third-party entities to establish a comprehensive security ecosystem to address continuously evolving security challenges. While Zero Trust can significantly enhance security, it also presents challenges and limitations. Firstly, it necessitates thorough data classification and risk assessment, impacting business processes and organizational structures. Secondly, maintaining and upgrading security technologies and tools will increase organizational costs and risks.

2.4.1 Core Principles of Zero Trust

A. Always Verification

Every access request, whether internal or external, must undergo continuous verification. This involves authenticating and authorizing users and devices before granting access to ensure each visit is verified.

B. Least Privilege Access

Access privileges are minimized to the least necessary for users to perform their tasks, thereby decreasing the potential impact of account compromises. This strategy ensures that the resulting damage remains confined to a limited extent in the event of a breach.

C. Microsegmentation

Networks are divided into small segments, each with strict access controls, limiting attackers' lateral movement within the network. This way, even if one area is compromised, it is difficult for attackers to expand their influence.

D. Assume Breach

Organizations operate under the assumption that breaches either have occurred or are imminent, prompting proactive defensive measures and rapid incident response. This breach assumption emphasizes the importance of continuous monitoring and swift reaction.

In conclusion, the Zero Trust model offers a modern security framework that addresses current and future network security challenges through continuous verification, least privilege access, microsegmentation, and assume breach. As technology advances and security threats evolve, Zero Trust practices and research will continue to develop, providing organizations with more robust defense mechanisms.

2.4.2 Implementing Zero Trust: Key Technical Components

A. Identity Authentication

Employing strong mechanisms like multi-factor authentication (MFA) to confirm the identity of users and devices guarantees that each access request originates from a verified source. Identity authentication is fundamental to the Zero Trust architecture, guaranteeing that only authorized users and devices are permitted access to resources.

B. Access Control

Access control policies must be dynamic, enforcing rules dictating who can access resources under what conditions. These policies are dynamically adjusted based on user roles,

task requirements, and the current security posture, ensuring resource management.

C. Trust Evaluation

Continuously assessing the trustworthiness of entities based on various factors, including behavioral patterns, device security status, and operating environment. Trust evaluation systems consider both static identity information and dynamic contextual information, providing a comprehensive risk assessment.

Together, these components form the foundation of a robust Zero Trust architecture, enhancing organizational security by ensuring that every access request is rigorously verified and authorized.

The application scenarios for Zero Trust are extensive. Table 2.1 highlights how Zero Trust architecture is implemented in various fields, such as critical cloud computing, the Internet of Things (IoT), and Medical sectors. Analyzing these domains aims to highlight the unique challenges and solutions associated with zero-trust architecture in each field. This comparison helps better understand how different technologies and methods can be employed to adapt Zero Trust principles to meet specific security needs. The table includes the authors, year, title, and description, showcasing how each study utilizes Zero Trust architecture to address specific security issues in these domains.

Table 2.1 Comparative Analysis of Zero Trust Implementations in Cloud Computing, Internet of Things, and Medical

Author(s)	Year	Title	Description
Cloud Computing			
S Mehraj and MT Banday. [63]	2020	Establishing a zero-trust strategy in the cloud computing environment	The proposed strategy seeks to enhance the efficiency of trust establishment and management between cloud service providers (CSPs) and customers in cloud computing. This addresses the dynamic nature of trust in cloud

			services, contrasting with traditional static trust mechanisms that tackle security and privacy challenges.
S Ahmadi [64]	2024	Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities	The paper emphasizes the role of Zero-Trust Architecture (ZTA) in reducing horizontal movement, minimizing insider threats, improving identity and access management, and enhancing micro-segmentation. It outlines recommended practices for adopting ZTA, explores future advancements, and illustrates ZTA's efficacy in bolstering cloud network security. This research offers valuable perspectives for both researchers and practitioners in the domain.
Internet of Things (IoT)			
S Dhar and I Bose [65]	2021	Securing IoT Devices Using Zero Trust and Blockchain	This paper suggests employing risk-based segmentation to improve uniformity within IoT networks and integrates blockchain for enhanced device identification and access control frameworks. It combines Zero Trust principles with blockchain technology to tackle security challenges in IoT. A case study showcases how this approach effectively delivers a robust security solution for varied and geographically dispersed IoT networks.
Y Yang et al [66]	2024	An Anonymous and Supervisory Cross-Chain Privacy Protection Protocol for Zero-Trust IoT	The study proposes a privacy protection protocol for cross-chain transactions in a zero-trust IoT environment. It utilizes the Groth16 zero-knowledge proof algorithm and coin-mixing technology. The research demonstrates that this method effectively secures cross-chain

		Application	transactions while preserving privacy. It addresses the complexity and compatibility challenges associated with blockchain interoperability.
Medical			
B Chen et al [67]	2020	A security awareness and protection system for 5G smart healthcare based on zero-trust architecture	This paper presents a security system for 5G smart healthcare, using Zero Trust Architecture (ZTA) for dynamic access control, real-time security awareness, and continuous identity authentication. It addresses critical security needs in 5G networks, protecting data, users, and services across cloud-edge-terminal setups. Despite implementation challenges, the framework shows promising results in enhancing active defense and overall security in smart healthcare.
Z Wang et al [68]	2023	Research on medical security systems based on Zero Trust	This research introduces a Zero Trust medical security system with dynamic access control (ABEAC) to protect medical systems from data leaks and remote attacks. It enhances security for medical equipment and data, validated through simulations showing its effectiveness over traditional models. Future improvements aim to stabilize the model and simplify authentication processes.

2.5 NIST.SP.800-207

In 2018, the National Institute of Standards and Technology (NIST) released the SP 800-207 "Zero Trust Architecture." This document was updated in 2020 [69]. NIST SP 800-207 does not prescribe a single "correct method" for implementing Zero Trust. Instead, it explores

various possibilities, including underlying architectures, deployment strategies, trust algorithms, and use case variations. NIST describes Zero Trust as a security approach rather than a set of strict policies or technologies, ensuring the report's long-term applicability.

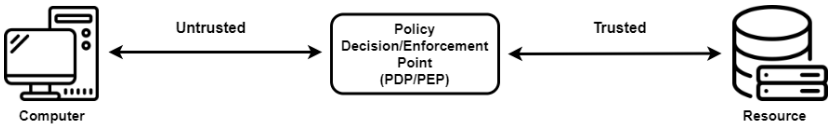

Figure 2.3 Zero Trust Access

Source: NIST.SP.800-207 [70]

Figure 2.3 illustrates the core access control process in the Zero Trust Architecture. It emphasizes the interaction among computers, Policy Decision/Enforcement Points (PDP/PEP), and resources. In this setup, PDP/PEP acts as crucial overseers, dynamically evaluating each access request and enforcing rigorous security measures in real time to prevent potential threats from compromising organizational resources.

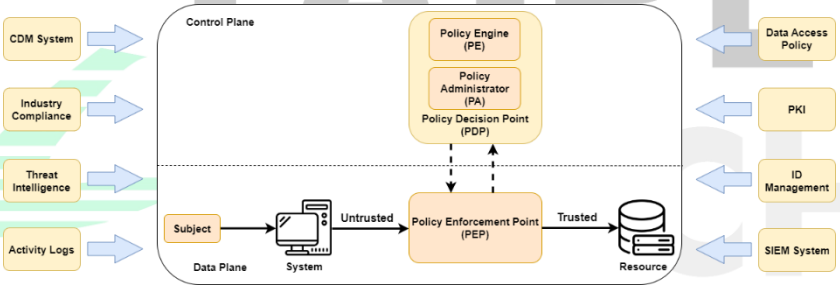

Figure 2.4 Core Zero Trust Logical Components

Source: NIST.SP.800-207 [70]

To further elucidate the structure and functionality of ZTA, Figure 2.4 illustrates multiple key components and interactions within the Zero Trust Architecture (ZTA). It is divided into two primary planes: the control and data planes. ZTA logic components communicate through a separate control plane, while application data is transmitted through the data plane [58][70][71].

A. Control Plane

The control plane comprises various policy and decision components responsible for

formulating and managing policies to control resource access.

Key components include:

1) Policy Engine (PE): The core component responsible for making access decisions based on predefined policies. It evaluates requests and determines whether access should be granted.
2) Policy Administrator (PA): Manages and executes policies formulated by the policy engine. It communicates with the Policy Enforcement Point (PEP) to ensure consistent policy application.
3) Policy Decision Point (PDP): Combining the roles of the PE and PA, it serves as the central authority for decision-making and managing policies. It establishes, oversees, and ultimately disconnects interactions between users and enterprise resources.

B. Data Plane

The data plane processes the actual data flow and access control between subjects (users or devices) and resources (data or services):

1) Subject: Entity requesting access to resources.
2) System: Environment where the subject resides.
3) Policy Enforcement Point (PEP): Responsible for managing the connection between the subject (e.g., user) and the resource, including initiating, monitoring, and terminating the connection. The PEP communicates with the PA to receive requests and policy updates.
4) Resource: Asset the subject is attempting to access.

C. Support Components

Several data sources provide necessary input data and policy specifications to the policy engine for making access decisions, including:

- CDM System (Continuous Diagnostics and Mitigation): Provides real-time security posture and vulnerability information to assist in formulating and adjusting security

policies.

- Industry Compliance: Ensures adherence to industry standards and regulations, which often impact policy development.
- Threat Intelligence: Offers insights into current and emerging threats to aid in predicting and mitigating potential attacks.
- Activity Logs: Offers insights into historical access patterns and behaviors to help detect anomalous activities and improve policies.
- Data Access Policies: Define which roles can access what data under what circumstances.
- PKI (Public Key Infrastructure): Tasked with creating and managing encryption keys and certificates required for secure communication.
- ID Management: Established, stored, and managed user identities and authentication credentials.
- SIEM System (Security Information and Event Management): Gathers security-focused information for the future analysis of security data to enable proactive threat detection.

NIST SP 800-207 is crucial for understanding and implementing Zero Trust Architecture. By adhering to the principles and guidelines outlined in this document, organizations can more effectively safeguard their resources and data, defend against internal and external threats, and enhance their overall cybersecurity posture.

2.6 Identity and Access Management (IAM)

Identity and Access Management (IAM) is one of the key technologies modern enterprises use to ensure system and data security. IAM technologies cover various domains, including single sign-on, MFA, and role-based access control. With the development of artificial intelligence, blockchain technologies, and cloud computing, IAM systems

continually evolve to meet the growing security demands and challenges. The functionalities of IAM vary depending on the size and needs of the enterprise; IAM in large enterprises varies from that in small organizations due to factors like technology, scale, use cases, complexity] employed, and regulatory or legal obligations [35]. Through the use of strong IAM controls, organizations can guarantee that access to their systems and data is limited to authorized users, devices, and applications, thus boosting security and compliance.

Research by SO Olabanji et al. [72]emphasizes the growing role of intelligent authentication in IAM, especially in cloud environments. This paper discusses how AI technologies can enhance user authentication and access control, offering various methods to improve system security and efficiency.

As technology advances and security needs increase, IAM has become increasingly important in modern enterprises. These technologies effectively improve system security and management efficiency. Enterprises of different sizes face unique challenges and requirements when implementing IAM, but by integrating intelligent and unified IAM solutions, they can significantly simplify identity management processes, enhance overall security, and meet compliance requirements. In the future, with ongoing advancements in AI and other cutting-edge technologies, IAM systems will continue to evolve, further enhancing enterprise security and operational efficiency.

2.7 Account recovery

Account recovery is the process by which users regain access to their accounts when they forget or lose their authentication information. This process is crucial for maintaining user experience and security, especially as digital identities become increasingly important. Currently, primary account recovery methods include answering security questions, email verification, and SMS verification. However, these methods come with several security risks and user experience challenges. For instance, security questions can be guessed or obtained

through social engineering, and email and SMS verifications are vulnerable to man-in-the-middle attacks or SIM card hijacking.

The study by A Büttner and N Gruschka. [73] reveals the practical application and challenges of current MFA and account recovery methods. Through the analysis of Google and Apple user accounts, the study provides valuable insights into MFA configurations and account recovery options, emphasizing the necessity of improving these methods to enhance security and user experience. The significance of this study lies in its demonstration of the shortcomings of existing methods and its provision of reference points for future improvements.

The application of FIDO2 in account recovery still faces several challenges, such as the recovery process when a device is lost or when users switch devices, which can lead to inconvenience and security vulnerabilities [35]. For example, when users lose the device registered with the FIDO2 credential, they must rely on backup keys or other alternative recovery options, which can be cumbersome and introduce additional security risks. Furthermore, if users frequently change devices, they must reconfigure FIDO2 authentication each time, increasing complexity and the potential for errors. These challenges require further technical improvements and user education to ensure the effectiveness and convenience of FIDO2 in account recovery.

The study by J. Kunke et al. [74] evaluates 12 account recovery mechanisms in the context of FIDO2 passwordless authentication. Despite the security benefits of FIDO2 passwordless authentication, its account recovery mechanisms present challenges. The study highlights that current recovery methods have flaws, with some still relying on traditional password methods. However, the research suggests several promising solutions, particularly the FIDO2 backup token mechanism. Therefore, to promote the widespread adoption of FIDO2 passwordless authentication, it is necessary to improve its account recovery mechanisms.

Chapter 3 Processes and Architecture

3.1 Key Features of B2C E-Commerce Platforms

Compared to B2B, B2C e-commerce requires a higher level of resilience to address rapidly changing market demands and technological advancements. In B2B environments, transactions typically occur between two businesses in a more controlled setting. In contrast, the B2C environment is entirely different, catering to a large number of individual consumers with frequent transactions. Since B2C platforms directly face end consumers, they need to be more agile in responding to changing user demands. The primary challenge in B2C lies in enhancing security without compromising user experience.

B2C platforms must continually adjust their security strategies to improve security while maintaining a seamless user experience. Consumers in the B2C environment demand convenience, and their needs and behaviors are highly variable. Therefore, security technologies in B2C must offer robust protection while integrating with fast and convenient user experiences. For example, FIDO2's passwordless login and biometric technologies allow users to experience quicker, simpler login processes while maintaining high security. Additionally, MFA can dynamically adjust the strength of authentication based on user behavior and risk, minimizing interference with routine operations. Zero Trust dynamically modifies security policies according to user behavior and environmental factors, enabling platforms to swiftly counter new threats.

3.2 Challenges in B2C E-Commerce Security

In B2C e-commerce, security, convenience, and usability are the three core issues. As more consumers shop online and attack methods evolve, they face increasing security threats, creating numerous challenges that need to be addressed. For instance, too many password and

weak passwords are common problems. Consumers often need to remember multiple account passwords [17], leading to inconvenience, a tendency to forget, and the use of weak passwords, which increases the risk of attacks.

Another major concern is the rapid rise in phishing attacks, which has garnered unprecedented attention [12]. Phishing can lead to severe consequences, as consumers often find it difficult to distinguish between legitimate and fake websites. This can result in financial losses and subsequent disputes, as well as the theft of personal information, leading to identity theft or other forms of fraud. For e-commerce businesses, when consumers' personal information is exposed in phishing attacks or financial losses are reported, the brand's reputation suffers, and consumer trust in the e-commerce platform's security diminishes, leading to a decline in customer confidence.

One challenge that FIDO2 faces in B2C e-commerce is account recovery [35]. Unlike the B2B market, which typically involves long-term cooperation between enterprises and a stable user base with relatively low account recovery needs, the B2C market is vastly different. In a B2C environment, thousands of consumers create and use online accounts daily, with diverse security needs and usage habits. Because consumers may lose devices, forget passwords, or lose security keys, account recovery becomes a crucial issue in ensuring a positive user experience and maintaining customer loyalty. If users cannot quickly and easily recover their accounts, it may lead to customer attrition. This need for flexibility in responding to user demand is especially important in environments where users may be unfamiliar with recovery processes or the operation of FIDO2, or where they may use the same account on multiple devices such as phones, tablets, and computers, increasing the complexity of management and recovery. Therefore, account recovery processes must ensure security without being overly complicated, to avoid negatively impacting user experience. Additionally, offering multiple recovery options ensures that the overall architecture is resilient enough to improve the success rate of recovery while adequately protecting user

privacy by avoiding the over-collection or misuse of personal information.

When considering the application of security measures in B2C e-commerce, the importance of resilience becomes even more critical. With the rise of phishing attacks and other cyber threats, businesses must ensure that their systems can remain stable and operational during attacks or other unforeseen events. Resilience not only involves the ability to quickly resume operations but also includes the capability to prevent, detect, and respond to threats. By having highly resilient systems and architectures, e-commerce platforms can better protect consumer data and financial security, helping businesses maintain their competitive edge and market position in the face of future uncertainties while providing users with a safer and more convenient experience.

3.3 Balancing Security, Convenience, and Usability in Modern E-Commerce

With the advancement of technology, the rise of IoT, cloud services, and remote work has not only enhanced our quality of life but also introduced significant challenges, particularly in information security. Traditional security architectures, such as firewalls, are increasingly inadequate in dealing with the dynamic nature of modern cyber threats. As a result, many companies have either adopted or are shifting toward a zero-trust architecture. As we have discussed, the Zero Trust model, with its principle of "never trust, always verify," addresses the shortcomings of traditional perimeter-based security by offering enhanced protection.

However, despite its many benefits, Zero Trust also introduces new challenges. These include increased architectural complexity, a shift in mindset, and most notably, issues related to convenience and usability. While the multi-layered security of Zero Trust enhances protection, the constant need for verification at every step can reduce user efficiency. For

instance, the requirement for continuous authentication may decrease user satisfaction, and scenarios such as forgetting passwords or not having access to verification tools like USB keys can impair usability. According to the comparative study conducted by Lyastani et al. [37], it was found that although FIDO2 has gained widespread user acceptance, concerns regarding its usability still persist.

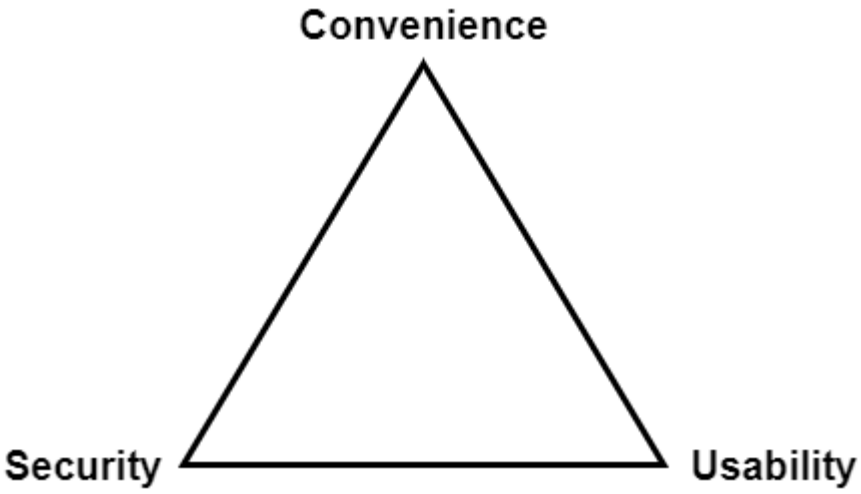

Figure 3.1 The Interplay of Security, Usability, and Convenience

As shown in Figure 3.1, there is often a trade-off between security, convenience, and usability—enhancing security can negatively impact convenience and usability, and vice versa. In e-commerce, it is crucial to provide users with a secure yet convenient experience without compromising on any of these factors. To address the challenges posed by Zero Trust, integrating FIDO2 can effectively increase convenience while simultaneously enhancing security. Additionally, implementing MFA improves usability and overall system resilience.

Therefore, this thesis introduces the QuickSecure Access (QSA) architecture, which balances security, convenience, and usability and enhances overall resilience. QuickSecure Access (QSA) is designed to offer strong security while providing more flexible options to reinforce usability and maintain a seamless user experience.

3.4 QuickSecure Access (QSA) Process

In this section, we first introduce the complete process of the QuickSecure Access (QSA) system and further elaborate on its structure and operational logic. Following this, we will explain the parts that users will interact with, emphasizing that despite the complexity of the overall process, which involves multiple steps, users can still complete registration, login, and resource access through simple and fast actions in practice.

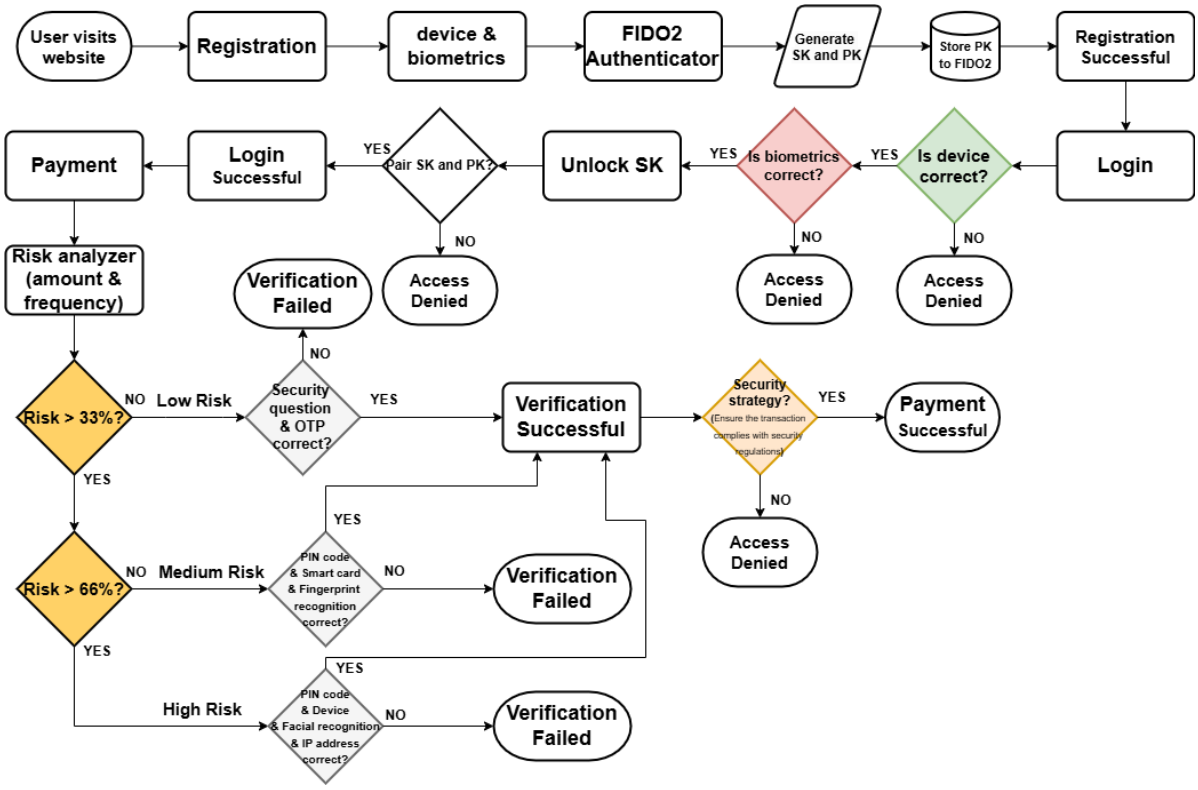

Figure 3.2 QuickSecure Access (QSA) Process Flow Diagram

Figure 3.2 illustrates the complete flowchart of the QuickSecure Access (QSA) system. This flowchart details how FIDO2, Zero Trust, and MFA technologies are integrated and leveraged to protect access to critical resources, forming a comprehensive authentication and authorization process.

The process begins with user registration, where FIDO2 is utilized. Users authenticate themselves using devices such as a USB security key or smartphone, combined with biometric

verification (e.g., fingerprint or facial recognition). The system then generates an asymmetric key pair, with the public key (PK) securely stored on the FIDO server, while the private key (SK) is kept on the user's device, completing the registration process. This process leverages asymmetric encryption to ensure that the SK is never exposed to the network, significantly reducing the risk of phishing attacks. Since the SK remains securely stored on the device and authentication can only occur on legitimate websites, the security is greatly enhanced.

Once registration is complete, users can log in securely using the previously configured device and authentication method. Upon successfully verifying the device and biometric data, the system unlocks and pairs the SK with the FIDO server's PK for encryption. A successful pairing grants the user access to the system. FIDO2 eliminates traditional passwords, which cannot cope with modern cyber threats, while combining physical devices with biometric verification greatly enhances the security and convenience of the login process.

After successfully logging in, when a user attempts to access purchase or perform certain actions, the system conducts a risk analysis based on the transaction amount and frequency to assess the severity of payment risk, thereby triggering the Multi-Factor Authentication (MFA) process. The system provides four authentication factors: Something You Know, Something You Have, Something You Are, and Somewhere You Are. Depending on the requested resource's sensitivity and security requirements, the MFA system may require the user to provide one or more authentication factors at different verification levels. For example, low-risk verification might only require Something You Know (security question), and Something You Have (OTP), mid-risk verification could require Something You Know (PIN code), Something You Have (smart card), and Something You Are (Fingerprint recognition), while access to high-risk resources would necessitate a combination of Something You Know (PIN code), Something You Have (device), Something You Are (facial recognition), and Somewhere You Are (IP address). Additionally, MFA offers a variety of account recovery methods, enhancing the system's flexibility and resilience.

After successful MFA verification, the request moves into the core of the Zero Trust architecture. The Policy Enforcement Point (PEP) collects and analyzes the user's request information and forwards it to the Policy Decision Point (PDP). The PDP conducts a comprehensive assessment based on predefined security policies and dynamic contextual information (e.g., user identity, geographical location, access time, and resource sensitivity) and makes an authorization decision. Based on the PDP's decision, the PEP enforces the corresponding actions, either granting or denying the request, ensuring that only requests that meet all security policies are granted access to sensitive resources. The process ensures that transactions comply with security regulations, safeguarding the integrity and confidentiality of the transaction while adhering to relevant standards and regulations.

This complete process, through multi-layered authentication and real-time authorization mechanisms, achieves high security, flexibility, and convenience in the system, effectively addressing the common security challenges in B2C e-commerce.

3.4.1 Convenient and Secure Resource Access for Users

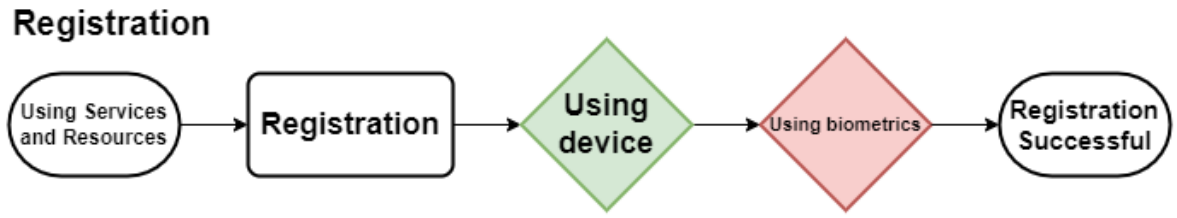

Figure 3.3 User Sign-Up Process Diagram

A registration process is required when a user attempts to access resources for the first time, as shown in Figure 3.3. During the registration process, the user only needs to authenticate themselves using their device through biometric identification (e.g., fingerprint or facial recognition) or a hardware security key (e.g., a USB security key or mobile device). Once the registration process is completed, the user will be granted the corresponding access rights to the resources.

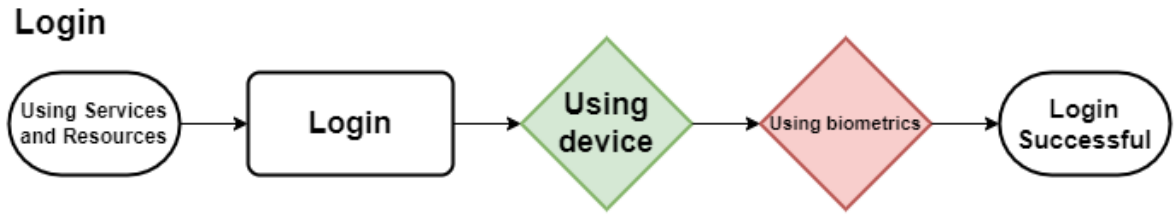

Figure 3.4 User Sign-In Process Diagram

Once the user has completed the registration process, they can log in to verify their identity and gain access rights, as shown in Figure 3.4. During the login process, the user simply uses the device and authentication method configured during registration (e.g., biometrics or a security key). Once the system confirms the user's identity, access to the appropriate resources will be granted. This login method requires only the device and authentication, improving security while simplifying the user experience by eliminating the reliance on traditional passwords.

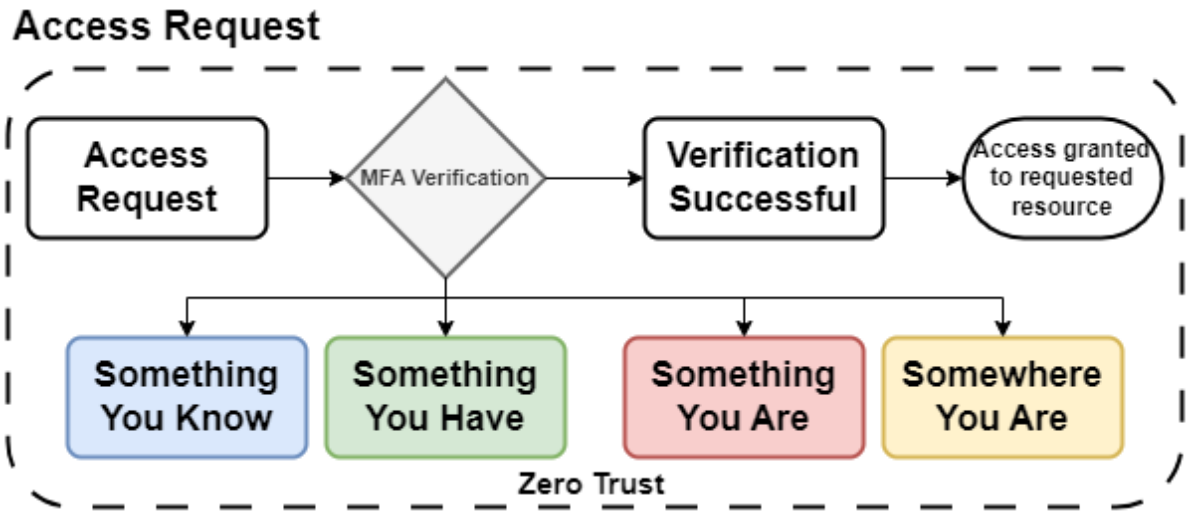

Figure 3.5 User Access Request Process Diagram

After logging in, if a user wants to request access to resources, they must be verified to successfully obtain permissions and access the resources, as shown in Figure 3.5. Under the Zero Trust framework, when users request resource access, they must go through a Multi-

Factor Authentication (MFA) process. There are four authentication factors to choose from: "Something You Know" (e.g., password or PIN), "Something You Have" (e.g., smart card or security key), "Something You Are" (e.g., fingerprint or facial recognition), and "Somewhere You Are" (e.g., Wi-Fi or IP location). Once the user's identity is verified through MFA, the system grants access to the requested resources. This method ensures that every access request undergoes strict multi-factor verification, significantly reducing potential security risks and enhancing the system's resilience, enabling it to effectively defend against various threats.

3.5 QuickSecure Access (QSA) Architecture

The architecture of QuickSecure Access (QSA) is illustrated in Figures 3.6 and 3.7. These diagrams highlight how each component interacts and collaborates to enable secure access and efficient performance within the QSA system. Below, we will provide a detailed explanation of the function, role, and importance of each component in the system as depicted in the architecture diagrams.

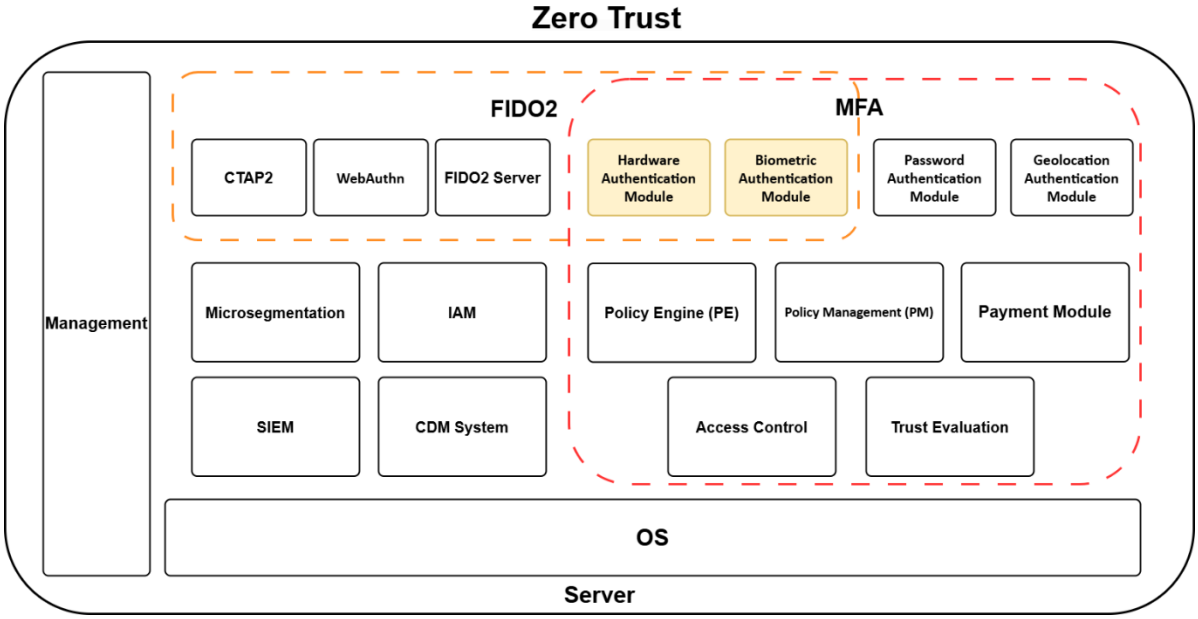

Figure 3.6 QuickSecure Access (QSA) System Framework Architecture Diagram

In the context of rapid digital transformation and the growing complexity of cyber

threats, striking a balance between security, convenience, and usability has become increasingly critical. To address these challenges, the QuickSecure Access (QSA) architecture was developed to create a system that enhances user experience through greater convenience and security by integrating three major security strategies: Zero Trust, FIDO2, and MFA.

The architecture comprises five main components: Zero Trust, FIDO2, MFA, Management, and Operating System (OS). The Zero Trust component includes the Policy Engine (PE) and Policy Management (PM), along with other critical elements such as Microsegmentation, IAM [35][72], SIEM [70], Access Control, Trust Evaluation, and the CDM System [70]. The Policy Management (PM) module is responsible for managing and enforcing policies defined by the Policy Engine. Microsegmentation divides the network into multiple smaller segments, each with its dedicated security controls and policies. Even if an attacker compromises a specific network area, they cannot easily move laterally to other areas. The role of microsegmentation is to limit the spread of threats, strengthen network isolation, and enhance the overall network's security posture and fine-grained security management. Access control is a core mechanism of the Zero Trust architecture, managing who can access which resources under specific conditions. This can be dynamically determined using Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or contextual factors (e.g., time and location). The key role of access control is to ensure that resources are only accessible to authorized users, preventing unauthorized access and thereby protecting sensitive data and system security. Trust Evaluation is a dynamic process that continuously assesses the risk level of users, devices, and requests and adjusts access permissions based on the current context and security status. It considers various factors, such as device health, behavior patterns, and geographic location, to ensure that each access request is verified, preventing improper access, and ensuring a secure and adaptive network environment. The Payment Module is the core component for processing payment transactions, responsible for receiving payment information from the client. It validates the authenticity of the payment

data, processes the transaction outcomes, and returns the results to the client. This ensures that the transactions adhere to security and compliance requirements, safeguarding both the payment process and financial assets.

The FIDO2 component consists of three key elements: CTAP2, WebAuthn [30][36][37], and the FIDO2 Server. The FIDO2 Server is responsible for handling security operations during user registration and login processes. It generates authentication challenges, verifies user signatures, and manages and stores public keys. The FIDO2 Server also interacts with the application server to ensure the security and compatibility of user authentication.

The MFA integrates multiple factors to enhance security and resilience. Something You Know [40-42] is handled by the Password Authentication Module, which processes the user's input and compares it with the server data to verify identity. Something You Have [43-45] is managed by the Hardware Authentication Module, which handles the physical security device and uses encryption keys for authentication. Something You Are [46-50] is processed by the Biometric Authentication Module, which employs biometric technologies to authenticate the user, ensuring their biometric features match the registered data. Somewhere You Are [51-53] is handled by the Geolocation Authentication Module, which collects and processes the user's location data and compares it with the server policies to verify location. By combining these factors, MFA significantly strengthens the system's security and resilience. Even if an attacker gains access to one factor, they still face challenges with the others. Through secure and diversified authentication methods, MFA strengthens both security and convenience while greatly enhancing the overall resilience of the system.

The architecture introduces a significant innovation by integrating Zero trust, FIDO2 and MFA functionalities into a unified framework. Rather than treating them as separate modules, their overlapping components—such as hardware and biometric authentication—are consolidated into a single workflow. This eliminates redundancy, simplifies implementation, and enhances overall efficiency. Moreover, the architecture goes beyond merely placing Zero

Trust, FIDO2, and MFA side by side, it strategically combines their workflows into a cohesive process, allowing developers to avoid duplicative development efforts and streamline security operations. By transforming multiple independent workflows into a singular, efficient process, the architecture optimally addresses key challenges in security and usability. This innovative design not only reduces development complexity but also improves scalability, making it a comprehensive and practical solution for modern e-commerce security needs. For example, we have consolidated the previously dispersed processes a, b, c, and d from Module A and Module B into a unified Module C, enabling each process to independently handle its respective tasks while sharing common module resources. Although the processes perform distinct functions, the unified module architecture simplifies design, development, and operational costs. For instance, processes a and c no longer need to be redundantly implemented in both Module A and Module B but are instead utilized as shared resources within Module C. Furthermore, the unified Module C facilitates the seamless addition of new processes (e.g., processes e or f).

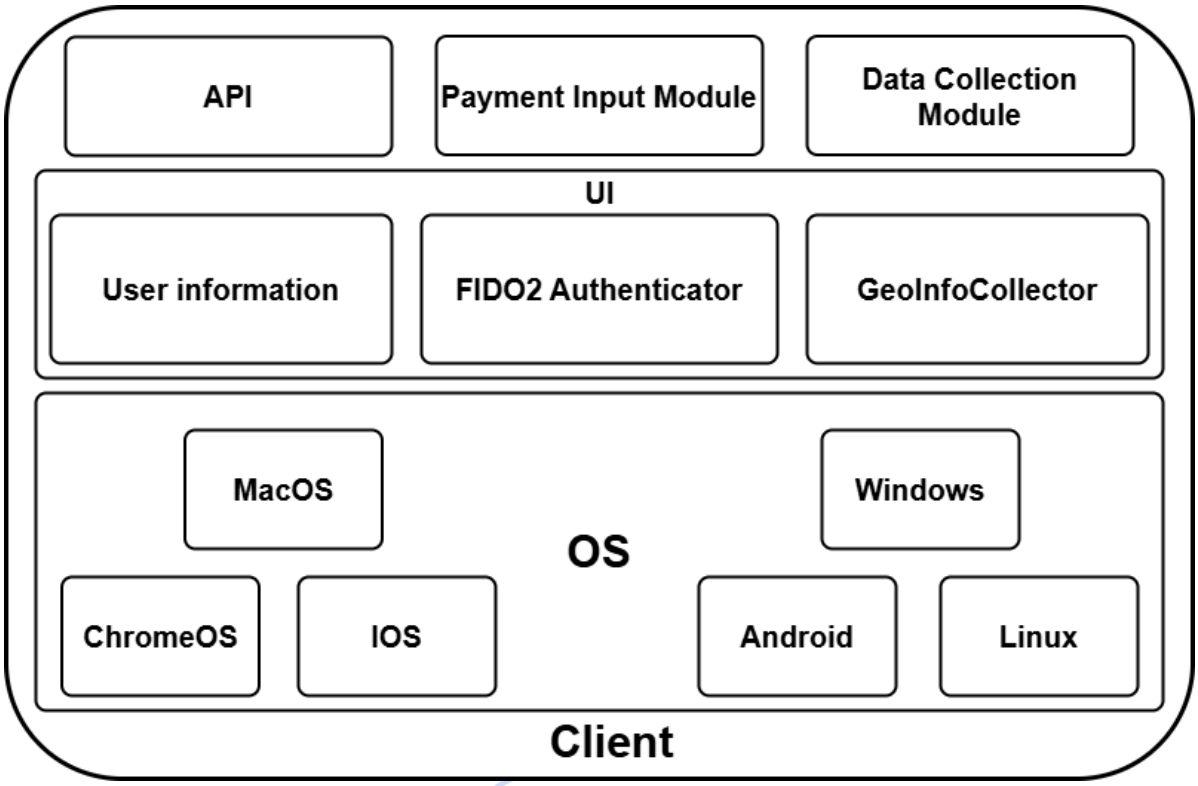

Figure 3.7 QuickSecure Access (QSA) Client Architecture Diagram

The API serves as the core module for data exchange between the client and server, responsible for the unified management of all request transmissions. Acting as a bridge for the entire architecture, it facilitates efficient collaboration among various functional modules and the server. The Payment Input Module collects and encrypts users' payment information, such as credit card numbers, bank account details, or third-party payment credentials, securely transmitting this data to the server-side Payment Module for processing. The Data Collection Module gathers dynamic data related to user devices and behavior, forwarding this information to the server-side Trust Evaluation and Access Control modules for real-time trust scoring and authorization decisions. This process provides critical security insights, enabling the server to conduct more granular and dynamic security assessments. The User Information Module collects and processes users' password inputs, transmitting them to the server for authentication. Additionally, the GeoInfoCollector gathers and provides users' geographic location data to support location-based security control policies, enhancing the authenticity of

user identity and devices. This mechanism effectively mitigates security risks associated with location-based threats.

FIDO2 Authenticator is the core component for enabling passwordless authentication by using cryptographic keys to verify user identity. It can be a hardware device (such as a USB security key) or a software solution (such as security modules built into mobile devices or operating systems). Its primary function is to generate a unique public/private key pair. The private key is securely stored on the user's device, whereas the public key is kept on the server to authenticate the user during access requests. FIDO2 Authenticator plays a crucial role in providing secure and convenient user authentication. In the QuickSecure Access (QSA) framework, FIDO2 Authenticator strengthens the authentication process by ensuring dynamic and trusted user verification for each resource access request. This method significantly reduces the risks associated with password use and effectively mitigates common threats such as phishing attacks and credential breaches.

QuickSecure Access (QSA) is broadly supported across multiple platforms, seamlessly integrating into various operating systems, including macOS, iOS, ChromeOS, Windows, Android, and Linux. This cross-platform compatibility ensures that FIDO2 authentication can be utilized on a wide range of devices, from desktops and laptops to smartphones and tablets, offering a consistent and secure user authentication experience. This multi-platform support not only enhances user convenience but also provides greater flexibility for businesses and developers when deploying security solutions, minimizing compatibility issues across different operating systems.

Chapter 4 Case Study

4.1 BeyondCorp

As companies increasingly adopt mobile and cloud technologies, traditional security models have shown significant problems in this rapidly evolving era. With boundaries becoming more blurred, the implementation and protection of perimeters have become increasingly difficult. Once attackers breach these perimeters, they can relatively easily access a company's internal network. Recognizing the changing enterprise environment and the rising security threats, Google saw an urgent need for a more flexible and secure architecture to protect its resources and users. Consequently, Google turned to the BeyondCorp security model, driven by motivations such as the increasing trend of cloud adoption and mobile work, the rise in security threats, and the need to improve user experience and efficiency.

Google's BeyondCorp initiative began as an internal project in 2009, following a highly sophisticated APT cyber attack known as "Operation Aurora" [75]. In 2021, Google launched the BeyondCorp Enterprise security model, a culmination of over a decade of restructuring its internal security architecture into a zero-trust framework, which it had used internally for many years. BeyondCorp enables Google employees to work securely from anywhere, enhancing productivity while improving security. Initially used only within Google, the rise in demand for zero trust has led Google to offer BeyondCorp as a service to the global market. In BeyondCorp, the identity and security status of users and devices are key factors. By directly connecting applications and resources to the internet, rather than through traditional virtual private networks (VPNs), BeyondCorp eliminates many security vulnerabilities while offering a better user experience and easier management.

Implementing BeyondCorp requires transitioning all company components to the BeyondCorp architecture. However, moving every network user and application to the

BeyondCorp environment in one go can pose significant risks to business continuity. To minimize risks, a phased migration is recommended, which allows for effective change and challenge management, ensuring smooth business operations. Google invested heavily in a phased migration, successfully moving many network users to the BeyondCorp environment with zero impact on productivity [76]. BeyondCorp enables Google employees to work securely from anywhere, with the goal of allowing employees to work remotely without needing a VPN, thus enhancing both security and productivity.

4.2 Cloudflare

Cloudflare [77], founded in 2010, is a global leader in network performance and security platforms. The company offers a range of services designed to improve website performance, availability, and security while reducing the risk of attacks. Cloudflare's network security architecture originally featured a firewall paired with a VPN setup. Employees accessed internal applications and servers through a VPN and, for certain applications, required two-factor authentication (2FA) using authentication apps like Authy or Google Authenticator to generate TOTP [78]. While this architecture appeared robust, its network security model was weak.

Recognizing the limitations of VPNs, Cloudflare sought a more secure and scalable solution, leading to the adoption of a zero-trust architecture and the launch of Cloudflare Access. Cloudflare aimed to migrate to phishing-resistant MFA. With the rise of tools like evilginx2 [79] and the increasing sophistication of phishing attacks targeting mobile authenticators and TOTP, Cloudflare urgently needed a secure solution that could withstand social engineering and credential theft attacks.

In 2018, Cloudflare began adopting FIDO-based security keys to transition from OTP to phishing-resistant FIDO authentication. By leveraging FIDO2, Cloudflare strengthened its authentication process to support its zero-trust model. Currently, all Cloudflare employees use

FIDO2 for secure multi-factor login, alongside Cloudflare's own Zero Trust products for system authentication. This new architecture not only prevents phishing attacks but also simplifies the implementation of least privilege access control [80].

4.3 National Government

As more private enterprises adopt zero-trust strategies, this approach is also taking root in the private sector. The U.S. federal government has taken significant steps to actively promote zero-trust security measures within its agencies. Over the past few years, the U.S. has issued several directives aimed at gradually developing and effectively protecting sensitive data and government information systems. In May 2021, the Biden administration released an executive order requiring federal agencies to comply with NIST 800-207 as an essential measure for implementing zero trust architecture., with the initial migration target set for 2024. This directive also called for advancing zero trust architecture and outlined specific steps to achieve this goal [81]. In October 2022, the Department of Defense released a zero-trust strategy to realize the dozens of capabilities needed for what it calls "targeted zero trust" [82].

Beyond the U.S., other governments are also actively pursuing zero-trust strategies and planning their deployment. For example, the European Union established the EU Cybersecurity Strategy in 2020, and China has formed the "Zero Trust Alliance" as part of its strategic transformation. Taiwan, in alignment with its Sixth National Information and Communication Security Development Program (2021-2024), is promoting the adoption of zero trust networks within government agencies to enhance network and information security infrastructure and services [83].

4.4 Cloud Computing

Amazon Web Services (AWS) [84] was established in 2006 and offers a broad range of

cloud computing products and solutions. AWS's traditional architecture primarily relies on Virtual Private Clouds (VPCs), Identity and Access Management (IAM), and multilayered security measures such as firewalls and encryption technologies. However, as threats become more diverse and complex, the security model of perimeter protection is no longer sufficient to secure distributed and dynamic cloud environments. Zero Trust can more effectively address internal threats and protect access for remote workers [85].

AWS implements Zero Trust through various services and tools, including access control via AWS Identity and Access Management (IAM), centralized single sign-on (SSO) services provided by AWS IAM Identity Center, continuous threat monitoring and detection with Amazon GuardDuty, and centralized security management and monitoring through AWS Security Hub [86]. By leveraging these tools, AWS ensures the security of cloud environments, adhering to the Zero Trust principle of "never trust, always verify".

4.5 Internet of Things (IoT)

Palo Alto Networks [87], founded in 2005, is renowned for its innovative network security products and solutions, dedicated to helping enterprises protect their networks and data from cyber-attacks. As an early proponent and market leader in enterprise firewalls, Palo Alto Networks initially relied on perimeter firewalls and centralized control to secure internal networks. However, with the increasingly complex threat landscape, modern cyber-attacks have become more sophisticated and diverse, making traditional perimeter security models less effective. Furthermore, with the rise of internal threats, relying solely on external defenses is no longer sufficient, necessitating greater focus on the security risks within internal networks.

As technology continues to evolve, traditional defenses are inadequate against various security challenges. The growing number of employees working remotely, using cloud services and mobile devices, has rendered traditional centralized security controls ineffective.

Additionally, the rapid growth of IoT devices has increased potential entry points for network attacks. These devices often lack sufficient security measures, making them potential targets for cyber threats. In response, Palo Alto Networks introduced IoT Security [88][89], a security solution specifically designed for IoT devices. This solution employs Zero Trust principles, machine learning, and behavioral analytics to monitor and protect these devices. For example, it utilizes App-ID technology and machine learning to precisely identify and categorize all OT devices and IoT, and it detects abnormal behavior by identifying the normal behavior patterns of these devices through machine learning and behavioral analysis. Palo Alto Networks has evolved its security strategy to address modern cyber threats effectively. By integrating advanced technologies such as machine learning, behavioral analytics, and Zero Trust principles, the company provides comprehensive solutions that secure networks in an increasingly complex and interconnected digital landscape.

4.6 Medical

Illumio [90] is a cybersecurity company founded in 2013, specializing in micro-segmentation and visualization. Its main product, the Adaptive Security Platform (ASP), uses micro-segmentation to restrict the horizontal movement of threats., thereby protecting workloads in data centers and cloud environments. Before adopting the Zero Trust architecture, Illumio primarily relied on traditional perimeter security models, which are based on the notion of trusting the internal network and protecting it from external threats. The original architecture typically included firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs). However, with the increase in network threats and internal threats, this architecture gradually revealed its limitations.

The proliferation of cloud computing and mobile work, along with more advanced attacker techniques and growing internal threats, has necessitated a shift to the Zero Trust architecture. Zero Trust, based on the principle of "never trust, always verify," requires

authentication and authorization for every access request, no longer assuming the internal network is secure. This approach more effectively protects enterprises from both internal and external threats. Illumio's micro-segmentation technology is a crucial component of the Zero Trust architecture [91], ensuring only authorized communications are allowed by restricting lateral movement between workloads, thereby providing finer-grained security protection.

In the healthcare sector, Illumio applies its Zero Trust Segmentation technology to protect electronic health records (EHR) systems, medical devices, and sensitive data [92]. By implementing micro-segmentation, Illumio helps healthcare organizations secure their critical assets and data against evolving threats, ensuring compliance with stringent regulatory requirements and enhancing overall cybersecurity posture.

4.7 Banking

Bank of America [93], one of the largest financial institutions globally, was established in 1784. Like most banks, Bank of America primarily relied on traditional password authentication systems and one-time passwords (OTPs) sent via SMS or email as additional security measures. While these methods are common, they carry certain security risks, such as password theft or phishing attacks.

Traditional password authentication methods are susceptible to various attacks. FIDO2 significantly enhances security through biometrics and hardware security keys while meeting user demands for passwordless login. This approach offers a more convenient authentication experience and reduces the hassle of remembering passwords. Bank of America supports the use of FIDO2 security keys, such as YubiKey [94][95]. These keys require users to insert the device and authenticate using a fingerprint during login. This method not only provides a more convenient authentication process but also enhances security protection.

Based on the summarized case studies above, Table 4.1 illustrates the use of FIDO2, Zero Trust, and MFA technologies by various companies across different domains. This table

includes examples of each company's products in B2B, national government, cloud computing, IoT, medical, and banking sectors. For instance, Cloudflare Access has extensively integrated FIDO2, Zero Trust, and MFA technologies into its internal operations, enhancing the security and efficiency of its internal systems. AWS has implemented Zero Trust to protect its distributed and dynamic cloud environment, making it more effective at addressing internal threats and securing access for remote workers.

The information presented in this table not only showcases how different companies implement these technologies across various fields but also provides valuable references. Therefore, this paper proposes QuickSecure Access (QSA) for e-commerce applications to effectively apply these technologies within the B2C sector. Given the unique high traffic and variable user behavior patterns in e-commerce, security and user experience become critical issues. By integrating FIDO2, Zero Trust, and MFA technologies to address these challenges, we can significantly improve the overall security and user satisfaction of e-commerce platforms, offering a more secure, convenient, and accessible comprehensive e-commerce solution.

For instance, Cloudflare employs physical security keys in its FIDO2 implementation, while Bank of America utilizes biometric authentication for online verification. In contrast, the QSA architecture combines mobile devices with biometrics to tackle these security challenges more effectively. Mobile devices, which are ubiquitous and carried by users daily, eliminate the inconvenience of carrying additional physical keys. Meanwhile, the use of biometrics enables more precise identity verification. Compared to the solutions offered by Cloudflare and Bank of America, the QSA architecture demonstrates superior performance in both security and convenience.

Table 4.1 FIDO2, Zero Trust, and MFA Technology Applications Across Different Domains

Product	Domain	FIDO2	Zero Trust	MFA
BeyondCorp Enterprise	Web Service		✓	✓
Cloudflare Access	Web Service	✓	✓	✓
National Government	Government		✓	
Amazon Web Services	Cloud Computing		✓	✓
IoT Security	IoT		✓	
Adaptive Security Platform	Medical		✓	
Bank of America	Banking	✓		✓
QuickSecure Access (QSA)	E-commerce	✓	✓	✓

Chapter 5 Conclusion

In this paper, we explored the integration of Zero Trust, FIDO2, and MFA in B2C e-commerce environments to address the evolving challenges of cybersecurity. Traditional security measures have become inadequate in combating increasingly sophisticated threats, particularly in the B2C domain where balancing security, convenience, and usability is paramount. B2C platforms require robust security frameworks that do not compromise the seamless user experience.

Through the introduction of the QuickSecure Access (QSA) architecture, this research provides a comprehensive solution, leveraging Zero Trust's continuous verification, FIDO2's passwordless authentication, and MFA's dynamic adaptability. The QSA architecture not only enhances security but also ensures resilience, convenience, and usability, making it a suitable model for consumer-centric environments.

This study fills a critical gap in current literature by addressing the integration of these technologies within the context of B2C e-commerce. In the future, as technology continues to evolve, the QSA architecture has the potential to set new standards for e-commerce security, providing users with a safer, more convenient, and trustworthy network environment.

Chapter 6 Future work

To continuously enhance security and user experience in B2C environments, future research should focus on improving account recovery mechanisms, enhancing user experience, AI automation, and quantum cryptography. First, improving account recovery mechanisms is crucial for increasing user trust, requiring a balance between security and convenience. Additionally, enhancing user experience by reducing cumbersome processes can better meet the demand for convenience. AI automation can be applied to real-time risk assessment, automatic adjustment of security policies, and access control, allowing for more flexible responses to changing threat environments and significantly enhancing the system's dynamic defense capabilities. Finally, the integration of quantum cryptography can effectively counter future threats posed by quantum computing to existing encryption technologies, ensuring long-term security. These research directions will provide B2C e-commerce platforms with more comprehensive and advanced security protection.

References

[1] S. Badotra, A. Sundas, et al., “A systematic review on security of e-commerce systems,” International Journal of Applied Science and Engineering, vol. 18, no. 2, pp. 1–19, 2021.

[2] D. S. W. Khan, “Cyber security issues and challenges in e-commerce,” in Proceedings of 10th international conference on digital strategies for organizational success, 2019.

[3] Chien Chang Wu and Shiang Jiun Chen, “Enhancing VPN Security through TrustFlex: Integrating Random Port Allocation and Zero Trust Architecture”, TSCE 20th, 2024.

[4] Chien Chang Wu and Shiang Jiun Chen, “The Convergence of FIDO2 and Zero Trust: A Comprehensive Approach to Enterprise Security”, CISC 34th, 2024.

[5] X. Liu, S. F. Ahmad, M. K. Anser, J. Ke, M. Irshad, J. Ul-Haq, and S. Abbas, “Cyber security threats: A never-ending challenge for e-commerce,” Frontiers in psychology, vol. 13, p. 927398, 2022.

[6] PERCEPTION POINT, "BYOD Security: Threats, Security Measures and Best Practices", online available: https://perception-point.io/byod-security-threats-security-measures-and-best-practices/.

[7] Craig McCart, "15 shocking BYOD statistics from 2018 – 2024", online available: https://www.comparitech.com/blog/information-security/byod-statistics/, 2022.

[8] Holger Schulze, "BYOD SECURITY REPORT" online available: https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q2BYOD2021.pdf, 2021.

[9] Connor Jones, "BYOD should stand for bring your own disaster, according to Microsoft ransomware data" online available: https://www.theregister.com/AMP/2023/10/05/microsoft_byod_ransomware/, 2023.

[10] Zscaler Blog, "2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year" online available: https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year, 2023.

[11] Kaspersky, "Kaspersky reports phishing attacks grew by 40 percent in 2023" online available: https://usa.kaspersky.com/about/press-releases/2024_kaspersky-reports-phishing-attacks-grew-by-40-percent-in-2023, 2024.

[12] Rob Sobers, "Cybersecurity Statistics and Trends" online available: https://www.varonis.com/blog/cybersecurity-statistics, 2024.

[13] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in 2012 IEEE symposium on security and privacy, pp. 553 567, IEEE, 2012.

[14] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication,” Communications of the ACM, vol. 58, no. 7, pp. 78–87, 2015.

[15] F. Alqubaisi, A. S. Wazan, L. Ahmad, and D. W. Chadwick, “Should we rush to implement password-less single factor fido2 based authentication?,” in 12th annual undergraduate research conference on applied computing (URC), pp. 1–6, IEEE, 2020.

[16] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, “Passgan: A deep learning approach for password guessing,” in Applied Cryptography and Network Security: 17th International Conference, ACNS 14th, Bogota, Colombia, Proceedings 17, pp. 217 – 237, Springer, 2019.

[17] Kamile Viezelyte, "Juggling security: How many passwords does the average person have in 2024?" online available: https://nordpass.com/blog/how-many-passwords-does-average-person-have/, 2024.

[18] Mark Visser, "Yubico’s 2019 State of Password and Authentication Security Behaviors Report" online available: https://www.yubico.com/press-releases/yubicos-2019-state-of-password-and-authentication-security-behaviors-report/, 2019.

[19] Fido Alliance, online available: https://fidoalliance.org/.

[20] Fido Alliance, online available: https://fidoalliance.org/certification/.

[21] Fido Alliance, online available: https://fidoalliance.org/passkeys-directory/.

[22] Fido Alliance, online available: https://fidoalliance.org/members/.

[23] S. Srinivas, J. Kemp, and F. Alliance, “Fido uaf architectural overview,” FIDO Alliance Proposed Standard, 2013.

[24] H. Feng, H. Li, X. Pan, Z. Zhao, and T. Cactilab, “A formal analysis of the fido uaf protocol.,” in NDSS, 2021.

[25] K. Hu and Z. Zhang, “Security analysis of an attractive online authentication standard: Fido uaf protocol,” China Communications, vol. 13, no. 12, pp. 189–198, 2016.

[26] S. Srinivas, D. Balfanz, E. Tiffany, A. Czeskis, and F. Alliance, “Universal 2nd factor (u2f) overview,” FIDO Alliance Proposed Standard, vol. 15, pp. 1 5, 2015.

[27] Fido Alliance, online available: https://fidoalliance.org/specifications/.

[28] FIDO News Center, "FIDO Alliance and W3C Achieve Major Standards Milestone in Global Effort Towards Simpler, Stronger Authentication on the Web" online available: https://fidoalliance.org/fido-alliance-and-w3c-achieve-major-standards-milestone-in-global-effort-towards-simpler-stronger-authentication-on-the-web/, 2018.

[29] FIDO News Center, "FIDO2 Enhancements for Enterprise & Complex Security Applications" online available: https://fidoalliance.org/fido2-enhancements/, 2021.

[30] FIDO News Center, "FIDO Alliance 2019 Progress Report: FIDO Authentication for Simpler, Stronger Web Logins Now Ready for Rollout on Billions of Consumer Devices" online available: https://fidoalliance.org/fido-alliance-2019-progress-report/, 2019.

[31] FIDO News Center, "FIDO Authentication Adoption Soars as Passwordless Sign-ins with Passkeys Become Available on More than 7 Billion Online Accounts in 2023" online available: https://fidoalliance.org/fido-authentication-adoption-soars-as-passwordless-sign-ins-with-passkeys-become-available-on-more-than-7-billion-online-accounts-in-2023/, 2023.

[32] Stephen Pritchard, "#Infosec2024: CISOs Need to Move Beyond Passwords to Keep Up

With Security Threats" online available: https://www.infosecurity-magazine.com/news/infosec2024-passwordless-future/, 2024.

[33] Mobile ID World, "Passkeys Come to Payments via New Visa Service" online available: https://mobileidworld.com/passkeys-come-to-payments-via-new-visa-service/, 2024.

[34] Sugimoto, Osamu, and Hiroshi Ogino. "Building a Passwordless Campus Network with FIDO2 Server and Identity Security Keys" [FIDO2 サーバーと身分証型セキュリティーキーによるパスワードレス・キャンパスネットワークの構築]. Proceedings of the 84th National Convention, Originally published in Japanese, 2022.

[35] M. Kepkowski, M. Machulak, I. Wood, and D. Kaafar, “Challenges with passwordless fido2 in an enterprise setting: A usability study,” in IEEE Secure Development Conference (SecDev), pp. 37–48, IEEE, 2023.

[36] W3C Recommendation, "Web Authentication: An API for accessing Public Key Credentials Level 1" online available: https://www.w3.org/TR/webauthn-1/, 2019.

[37] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, “Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication,” in IEEE Symposium on Security and Privacy (SP), pp. 268–285, IEEE, 2020.

[38] N. A. Karim, O. A. Khashan, H. Kanaker, W. K. Abdulraheem, M. Alshinwan, and A. Albanna, “Online banking user authentication methods: A systematic literature review,” IEEE Access, 2023.

[39] P. Peng, C. Xu, L. Quinn, H. Hu, B. Viswanath, and G. Wang, “What happens after you leak your password: Understanding credential sharing on phishing sites,” in Proceedings of the ACM Asia conference on computer and communications security, pp. 181–192, 2019.

[40] M. Zhou, Q. Wang, X. Lin, Y. Zhao, P. Jiang, Q. Li, C. Shen, and C. Wang, “Presspin: Enabling secure pin authentication on mobile devices via structure-borne sounds,” IEEE

Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1228–1242, 2022.

[41] T. Van Nguyen, N. Sae-Bae, and N. Memon, “Draw-a-pin: Authentication using finger-drawn pin on touch devices,” computers & security, vol. 66, pp. 115–128, 2017.

[42] A. Rabkin, “Personal knowledge questions for fallback authentication: Security questions in the era of facebook,” in Proceedings of the 4th Symposium on Usable Privacy and Security, pp. 13–23, 2008.

[43] T. C. Clancy, N. Kiyavash, and D. J. Lin, “Secure smartcardbased fingerprint authentication,” in Proceedings of the ACM SIGMM workshop on Biometrics methods and applications, pp. 45–52, 2003.

[44] C.-Y. Huang, S.-P. Ma, and K.-T. Chen, “Using one-time passwords to prevent password phishing attacks,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1292–1301, 2011.

[45] R. Danthy, K. P. Pai, and V. Rao, “Secure online banking authentication system using time bound password,” in IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), vol. 5, pp. 130–135, IEEE, 2024.

[46] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi, et al., “Biometric authentication: A review,” International Journal of u-and e-Service, Science and Technology, vol. 2, no. 3, pp. 13–28, 2009.

[47] S. Hemalatha, “A systematic review on fingerprint based biometric authentication system,” in International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), pp. 1–4, IEEE, 2020.

[48] M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli, “On the use of sift features for face authentication,” in Conference on Computer Vision and Pattern Recognition Workshop (CVPRW’06), pp. 35–35, IEEE, 2006.

[49] H. Li, C. Xu, A. S. Rathore, Z. Li, H. Zhang, C. Song, K. Wang, L. Su, F. Lin, K. Ren, et al., “Vocalprint: exploring a resilient and secure voice authentication via mmwave

biometric interrogation," in Proceedings of the 18th Conference on Embedded Networked Sensor Systems, pp. 312–325, 2020.

[50] S. W. Shah, S. S. Kanhere, J. Zhang, and L. Yao, "Vid: Human identification through vein patterns captured from commodity depth cameras," IET Biometrics, vol. 10, no. 2, pp. 142–162, 2021.

[51] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location," IEEE Systems Journal, vol. 11, no. 2, pp. 513–521, 2016.

[52] D. H. Choi, H. Kim, and K. Jung, "A secure mobile ip authentication based on identification protocol," in Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS., pp. 709–712, IEEE, 2004.

[53] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for iot with location information," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3335–3351, 2018.

[54] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication–a survey," IEEE access, vol. 7, pp. 112505–112519, 2019.

[55] M. Shore, S. Zeadally, and A. Keshariya, "Zero trust: the what, how, why, and when," Computer, vol. 54, no. 11, pp. 26–35, 2021.

[56] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," Computers & Security, vol. 110, p. 102436, 2021.

[57] M. Campbell, "Beyond zero trust: Trust is a vulnerability," Computer, vol. 53, no. 10, pp. 110–113, 2020.

[58] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," IEEE access, vol. 10, pp. 57143–57179, 2022.

[59] Microsoft Security, "Zero Trust Adoption Report" online available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha, 2021.

[60] Okta, "The State of Zero Trust Security 2022" online available: https://www.okta.com/sites/default/files/2022-09/OKta_WhitePaper_ZeroTrust_H2_Campaign_.pdf, 2022.

[61] Connor Craven, "What Are Zero-Trust Benefits and Challenges?" online available: https://www.sdxcentral.com/security/zero-trust/definitions/what-are-zero-trust-benefits-and-challenges/, 2021.

[62] M. Campbell, “Beyond zero trust: Trust is a vulnerability,” Computer, vol. 53, no. 10, pp. 110–113, 2020.

[63] S. Mehraj and M. T. Banday, “Establishing a zero trust strategy in cloud computing environment,” in International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6, IEEE, 2020.

[64] S. Ahmadi, “Zero trust architecture in cloud networks: application, challenges and future opportunities,” Ahmadi, S. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, vol. 26, no. 2, pp. 215–228, 2024.

[65] S. Dhar and I. Bose, “Securing iot devices using zero trust and blockchain,” Journal of Organizational Computing and Electronic Commerce, vol. 31, no. 1, pp. 18–34, 2021.

[66] Y Y. Yang, F. Bai, Z. Yu, T. Shen, Y. Liu, and B. Gong, “An anonymous and supervisory cross-chain privacy protection protocol for zero-trust iot application,” ACM Transactions on Sensor Networks, vol. 20, no. 2, pp. 1–20, 2024.

[67] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, “A security awareness and protection system for 5g smart healthcare based on zero-trust architecture,” IEEE internet of things journal, vol. 8, no. 13, pp. 10248–10263, 2020.

[68] Z. Wang, X. Yu, P. Xue, Y. Qu, and L. Ju, “Research on medical security system based

on zero trust," Sensors, vol. 23, no. 7, p. 3774, 2023.

[69] National Institute of Standards and Technology, "NIST SP 800-207 Zero Trust Architecture" online available: https://csrc.nist.gov/pubs/sp/800/207/final, Aug. 2020.

[70] V. Stafford, "Zero trust architecture," NIST special publication, vol. 800, p. 207, 2020.

[71] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, vol., no. 1, p. 6476274, 2022.

[72] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, "Ai for identity and access management (iam) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems," Authorization, and Access Control within Cloud-Based Systems, 2024.

[73] A. Büttner and N. Gruschka, "Evaluating the influence of multi-factor authentication and recovery settings on the security and accessibility of user accounts," arXiv preprint arXiv:2403.15080, 2024.

[74] J. Kunke, S. Wiefling, M. Ullmann, and L. L. Iacono, "Evaluation of account recovery strategies with fido2-based passwordless authentication," arXiv preprint arXiv:2105.12477, 2021.

[75] BeyondCorp, online available: https://www.beyondcorp.com/.

[76] R. Ward and B. Beyer, "Beyondcorp: A new approach to enterprise security," ; login:: the magazine of USENIX & SAGE, vol. 39, no. 6, pp. 6–11, 2014.

[77] Cloudflare, online available: https://www.cloudflare.com/.

[78] FIDO Case Studies, "Cloudflare embraces FIDO to help its own security" online available: https://fidoalliance.org/cloudflare-embraces-fido-to-help-its-own-security/, 2023.

[79] Kuba Gretzky, "evilginx2" online available: https://github.com/kgretzky/evilginx2,

2024.

[80] Evan Johnson and Derek Pitts, "How Cloudflare implemented hardware keys with FIDO2 and Zero Trust to prevent phishing" online available: https://blog.cloudflare.com/how-cloudflare-implemented-fido2-and-zero-trust, 2022.

[81] The White House, "Executive Order on Improving the Nation's Cybersecurity" online available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, 2021.

[82] SandboxAQ, "Bridging Post-Quantum Cryptography and Zero Trust Architecture" online available: https://www.sandboxaq.com/post/bridging-post-quantum-cryptography-and-zero-trust-architecture, 2023.

[83] National Institute of Cyber Security, "Government Zero Trust Network Instructions" online available: https://download.nics.nat.gov.tw/UploadFile/zerotrustnetworks/%E6%94%BF%E5%BA%9C%E9%9B%B6%E4%BF%A1%E4%BB%BB%E7%B6%B2%E8%B7%AF%E8%AA%AA%E6%98%8E_V1.9_1110712.pdf, 2022.

[84] Amazon Web Services, online available: https://aws.amazon.com/.

[85] Amazon Web Services, online available: https://aws.amazon.com/tw/security/zero-trust/.

[86] Amazon Web Services, online available: https://aws.amazon.com/tw/products/security/.

[87] Paloalto Networks, online available: https://www.paloaltonetworks.com/.

[88] Paloalto Networks, online available: https://www.paloaltonetworks.tw/network-security/enterprise-iot-security.

[89] Jamison Utter, "The Only Way to Secure the IoT Is Zero Trust" online available: https://www.paloaltonetworks.com/cybersecurity-perspectives/the-only-way-to-secure-iot-is-zero-trust.

[90] illumio, online available: https://www.illumio.com.

[91] Systex, "Illumio Zero Trust Segmentation zero trust micro-segmentation solution" online

available: https://tw.systex.com/illumio-zero-trust-segmentation/.

[92] illumio, online available: https://www.illumio.com/resource-center/securing-healthcare-organizations/.

[93] Bank of America, online available: https://www.bankofamerica.com/.

[94] Bank of America, online available: https://www.bankofamerica.com/security-center/online-mobile-banking-privacy/usb-security-key/.

[95] Multipoint GROUP, "Bank of America allows authentication with FIDO security keys" online available: https://multipoint.eu.com/blog/2021/10/05/bank-of-america-allows-authentication-with-fido-security-keys/, 2021.