SUBJECT CODE: BCN 2053

SUBJECT NAME: OPERATING SYSTEM

SEMESTER: SEM 11 2023/2024

LECTURER NAME: PN. SURAYA BINTI ABU BAKAR

PROJECT OF BCN2053			
GROUP NAME: GROUP 2			
TEAM MEMBERS:			
NO	**MATRIC NUMBER**	**NAME**	**SECTION**
1	**CB22034**	**NUR ALIA NADHIRAH BINTI MUHAMMAD ZAILI**	**01**
2	**CB22040**	**NUR AMIRA SOFEA BINTI OTHMAN**	**01**
3	**CB22062**	**NUR AUNI LIYANA BINTI MOHD KHAIRI**	**01**
4	**CB22090**	**UMAIRAH SHUHADA BINTI AHMAD**	**01**

TABLE OF CONTENT

❖ INTRODUCTION

There is a growing need for a more robust and secure method of asset protection than password-based security solutions can offer due to the recent increase in data breaches and sophisticated hacking attempts targeting sensitive data. More advanced security measures must be implemented since password-cracking techniques are becoming more complicated. Many people are also realizing the benefits and efficiency that biometric authentication provides. Passwords, personal identification numbers (PINs), and security tokens are used by millions of users to access emails, many data apps, and corporation databases that hold private financial and corporate data. Owing to password susceptibility, several hacking approaches exist for obtaining these kinds of credentials, which might result in major data security breaches. Because passwords are easily guessed, stolen, or obtained illegally through covert monitoring, they have become useless. Password theft is a major factor in data breaches. Password compromises constitute a factor in 48% of hacker-related data breaches. The surge in data breaches in recent times has demonstrated the extreme vulnerability of password- or PIN-based authentication techniques, which have not kept up with the ever-evolving sophistication of data breach threats.

In contrast to conventional password-based systems, biometric authentication technology uses an individual's distinctive physical or behavioral traits, such as voice, iris patterns, fingerprints, or facial features, to confirm their identification. It is a more convenient and safe option. When authentication is needed, this technology works by taking biometric data, storing it, and using it to produce a digital template that can be compared to a live sample. Anyone may be quickly identified in a couple of seconds when using biometric identification for individual authentication. With the advancement of technology, businesses can nowadays easily access and exploit this more advanced technology for a variety of uses, including biometric single sign-on (SSO) for enhanced network security. As a safe way to access systems or databases, end users can utilize biometric credentials in place of passwords, tokens, or personal identification numbers (PINs) with the help of a biometric single sign-on (SSO), a biometric identification management system. Password memory is rendered unnecessary by biometrics, which recognizes people based on "who they are."

For example, facial recognition systems record the distances and proportions of facial characteristics, fingerprint scanners examine the distinctive ridges and patterns on a person's fingertip, and iris identification technology recognizes the complex patterns in the colored area of the eye [1]. Because biometric data is intrinsically unique to each individual, these technologies offer major security advantages by minimizing the danger of unauthorized access and making it exceedingly difficult for attackers to copy or steal [3]. Additionally, biometric authentication makes users' lives easier by removing the need to keep track of and manage several complicated passwords. Simply presenting a biometric characteristic, such as a fingerprint or face, to a sensor allows users to swiftly and easily authenticate themselves [1]. This usability is especially helpful in routine situations like using applications, shopping online, or entering restricted areas at work. Furthermore, biometric sensors are becoming more widely available on contemporary gadgets like computers and smartphones, which makes it easier for people to embrace and incorporate this technology into their daily lives [3] [1]. Nevertheless, there are drawbacks to using biometric systems, such as privacy issues and the possibility of data breaches. Because biometric data cannot be changed, unlike passwords, any breach might have long-term effects. For this reason, it's critical to implement strong data protection procedures and adhere to legal frameworks such as the Biometric Information Privacy Act (BIPA) [2]. Furthermore, the precision and dependability of biometric recognition systems [1] can be impacted by variables including aging, trauma, and environmental circumstances.

Despite these obstacles, the usage of biometric authentication is expected to increase due to technological developments and growing awareness of its advantages in improving user experience and security. In the future, biometric authentication will be a crucial component of digital identity verification due to ongoing advancements and the incorporation of multimodal biometric systems, which employ multiple biometric factors for authentication. These developments will further enhance security and convenience [3][1].

- **The relation between the technology with the operating system security**

Because biometric authentication technology offers a more easy and safer way to verify users, it is closely related to operating system security. The basic layer of a computer, the operating system (OS), controls all hardware and software resources, including user authentication and security procedures. By guaranteeing that access to critical information and system operations is limited to verified users only, the OS's integration of biometric authentication improves overall system security. Access control requires a reliable way to confirm user identification, which biometric authentication offers. To stop unwanted users from accessing system resources, the operating system depends on robust authentication procedures. The OS can lower the danger of unauthorized entry and possible breaches by incorporating biometrics to guarantee that only those with confirmed physical attributes, such as fingerprints or facial features, may access the system[3] . Processing and storing biometric data securely is under the control of the OS. This includes the use of encryption and secure storage methods, such as Secure Enclaves or Trusted Platform Modules (TPMs), to prevent unauthorized parties from gaining access to or changing biometric templates. The OS makes sure that biometric data is safe even in the event of a device hack by securely handling this [2]. You may have many alternatives when it comes to using biometric authentication to safeguard your access, depending on your device and operating system. For instance, Windows Hello, a feature that lets you log in to your device, applications, and online services using your face, fingerprint, or PIN, is supported by Windows 10. Touch ID is a technology that works with macOS that lets you use your fingerprint to pay, unlock your Mac, and make transactions. Numerous biometric identification techniques, including fingerprint, face, and iris recognition, are also supported by Android and iOS devices.

Additionally, continuous biometric authentication is a feature that modern operating systems may utilize to keep users secure during a user session. This implies that in order to make sure the authorized user is still present, the OS re-authenticates the user regularly by examining biometric characteristics. By preventing unauthorized access in the case that the device is left unattended, this method adds a security layer [1]. To identify and stop fraudulent activity, the OS uses biometric authentication. For example, critical tasks like financial transactions, changing system settings, or accessing private information may need biometric verification. The OS lessens the

possibility of fraud and illegal changes by making sure that these activities may only be carried out by authorized users.

The operating system's use of biometric authentication greatly enhances system security by offering a dependable, approachable means of identity verification. Biometric technology is essential to strengthening the security framework that the operating system (OS) manages because it enables continuous authentication, improves access control, secures biometric data, integrates with system services, prevents fraud, and promotes compliance. Biometric technology will probably play a bigger part in OS security as it develops and becomes more sophisticated, which will enhance the security of personal data and digital assets.

❖ HISTORICAL MILESTONE

Biometrics technology was already being introduced long before we decided to type our passwords but it is not widely used for security purposes since the development is taking its time to evolve, back then we would use fingerprints and handprints. The earliest fingerprints were recorded in 500 BC during the Babylonian Empire. It is found recorded by clay. [5] Then, in 1800s a biometrics identification system was found first in Paris. Alphonse Bertillon create a system to categorize and compare criminal individual body size. Biometrics authentication keeps evolving to the 1960s where facial recognition was developed. It was also supported by the Federal Bureau of Investigation(FBI) in 1969 thus encouraging biometrics development.[6] Biometrics technology is life-changing for our security. It provides strong security and uses our unique aspects of the body such as fingerprints, handprints, faces to have access to our security. Biometrics technology secures our data more efficiently. Hence, the rapid evolution of biometrics technology keeps expanding from facial recognition to voice recognition in the 1980s to 1990s by the National Institute of Standards and Technology(NIST). [6] Until the present day, we already use biometrics in our daily life, we could say that this technology is widely used especially in our devices , home security and others. To reach this phase biometrics technology also faces its challenges especially in terms of privacy concerns and technology limitations for the developments. However this challenge was successfully overcome by the industry, resulting in artificial intelligence technology. [7] Last but not least, biometric technology has bring our worlds, especially in IT, to more advanced futures. This technology can be found everywhere in our daily lives, even the closest one to us in our mobile devices. Majority of the devices nowadays implement biometrics technology to replace the old ways which is type our passwords. This technology definitely saves our time and we do not have to worry about our data being stolen by another party.

- Infographic of biometrics technology:

This infographic will simplify the journey of biometric authentication.

❖ ADVANTAGES AND DISADVANTAGES

- THREE (3) points of advantages

1) Security, privacy concern and lower risk of identity theft

Biometric authentication significantly bolsters the security of operating systems by utilizing distinct physical or behavioral traits to authenticate identity, offering a superior level of certainty compared to traditional passwords. This approach diminishes the likelihood of unauthorized access, as attributes such as fingerprints, retinas, or facial features are inherently challenging to forge or mimic.[8] Consequently, only approved individuals, like vetted personnel in a high-security government facility with unique iris scans stored in the system, can gain entry, rendering it arduous for imposters to breach security. Furthermore, biometric systems exhibit greater resistance to attacks such as brute force, phishing, and replay assaults, with contemporary systems integrating anti-spoofing mechanisms to identify and thwart the use of prerecorded biometric data. Given that the operating system regulates access to every facet of the system, its security is paramount, and the adoption of biometric authentication presents a robust substitute for passwords and PINs, augmenting overall system fortification and curtailing the risk of identity theft and unauthorized intrusion.

For instance, a financial institution might deploy biometric authentication to safeguard sensitive client information and its internal infrastructure. Employees can access their workstations via fingerprint scanners. Each time an employee endeavors to log in, the system scans and verifies their fingerprints against the stored dataset, which encompasses the unique fingerprint patterns of authorized personnel. This protocol ensures that only approved employees can access the system, markedly complicating unauthorized entry attempts. Such stringent security protocols not only uphold the integrity and confidentiality of client data but also serve to forestall the compromise of sensitive financial information.

2) User convenience (fast and convenient)

Biometric systems simplify the process of logging in, so users don't have to remember complex passwords anymore. Instead, they can easily access their devices by using their unique biometric features like fingerprints or facial scans. This makes logging in faster and reduces mistakes.[8] Plus, biometric authentication makes it harder for someone to fake or steal your identity compared to passwords. By adding biometric authentication to operating systems, it not only makes things easier for users but also makes them more secure.

A good example of this is Apple's Touch ID and Face ID on iOS devices. Instead of having to type in a password every time you want to unlock your phone or make a purchase, you can simply use your fingerprint or look at your phone to unlock it. This removes the hassle of remembering and typing passwords while also making sure that only you can access your device. By using biometric data like fingerprints or facial features, Apple's iOS devices provide a smooth and secure experience for users, showing how biometric authentication can make operating systems more secure and easier to use.

3) Multi-factor authentication

Multi-factor authentication (MFA) significantly strengthens operating system security by incorporating biometric data alongside conventional password-based authentication methods. By substituting typed passwords with biometric identifiers like fingerprints or facial patterns, MFA establishes multiple layers of defense against unauthorized access. Biometric authentication provides an additional level of security by relying on unique physical characteristics that are challenging to replicate or counterfeit, thereby reducing the risk of unauthorized access resulting from stolen or guessed passwords. This fusion of biometrics with traditional authentication mechanisms enhances the resilience of the operating system's defenses, addressing vulnerabilities associated with password-based attacks such as phishing or password theft.

An illustrative example of integrating biometrics into operating system security is the utilization of fingerprint recognition to unlock mobile devices. Modern smartphones equipped with fingerprint scanners enable users to securely access their devices by verifying their distinct fingerprint patterns.[9] This form of biometric authentication supersedes traditional typed passwords, offering a more convenient yet robust method for protecting sensitive information stored within the device. By seamlessly integrating biometric data into the authentication process, users benefit from heightened security without sacrificing usability, showcasing the effectiveness of biometrics in bolstering operating system security

- THREE (3) points of disadvantages

1) Privacy and Ethical Concerns

Significant privacy and ethical issues are raised when biometric data is used in operating system security instead of typed passwords. While biometrics offer convenience and potentially stronger security, the reliance on immutable biometric traits raises serious privacy issues. Unlike passwords, biometric data cannot be changed if compromised, leading to lifelong security vulnerabilities for individuals. Moreover, the collection and storage of sensitive biometric information, such as fingerprints or facial features, create opportunities for unauthorized access and misuse.[8] This raises ethical questions about the responsible use and protection of biometric data, as well as the potential for surveillance or tracking without consent, thus challenging the fundamental principles of privacy and autonomy.

An example illustrating the privacy and ethical concerns of using biometric data instead of passwords in operating system security involves a workplace implementing fingerprint scanning for employee attendance and access control. While the company may aim to increase efficiency and security by using biometrics, employees may feel uneasy about the collection and storage of their sensitive fingerprint data. Concerns arise regarding the potential misuse of this data, such as tracking employees' movements beyond the workplace or even selling the biometric data to third parties without consent. Moreover, if the biometric system experiences a breach, employees face the risk of identity theft and unauthorized access to their personal information.

This scenario underscores the importance of ethical considerations and robust privacy protections when implementing biometric authentication systems in operating system security to ensure the rights and autonomy of individuals are respected.

2) Failure to enroll

Failure to enroll in biometric systems, when used to replace typed passwords for operating system security, occurs when the system is unable to create a valid template for a user's biometric information. This can result from various factors such as low-quality reference data due to poor sensor performance or unfavorable environmental conditions during enrollment, like inadequate lighting.[10] Additionally, physical or medical conditions may prevent some individuals from successfully providing the necessary biometric input. Ensuring high enrollment rates is vital for the effectiveness of biometric authentication systems, as failure to enroll not only excludes individuals but also undermines the system's reliability and inclusivity.

An example of failure to enroll in a biometric system could involve a fingerprint scanner used for operating system login. If the scanner consistently fails to capture a clear fingerprint due to poor sensor quality or a user's faint fingerprints, the system will not be able to create a reliable template. This situation could be exacerbated by environmental factors such as excessive dryness or humidity affecting the fingerprint's clarity.

3) False acceptance and rejection rates

False positives in biometric authentication occur when the system incorrectly matches an individual's biometric data with a stored template, granting access to an unauthorized user.[10] This issue undermines the reliability of using biometrics as a replacement for typed passwords in operating system security. Since biometric systems analyze defining points rather than an extremely detailed record, errors can arise from various factors like the sensor’s cleanliness, lighting conditions, or the physical condition of the biometric trait (e.g., a cut on a finger). These inaccuracies pose significant security risks, as they can allow intruders to gain access to sensitive data and systems, compromising the overall integrity of the security framework.

An example of a false positive in biometric authentication could involve a fingerprint scanner used for logging into a computer system. If the scanner is dirty or the user's finger is smudged, the system might incorrectly identify another user with a similar fingerprint pattern, granting them access. This scenario can lead to unauthorized access where an intruder, perhaps even a colleague, gains entry to the operating system due to the misidentification. The consequences of such errors are particularly severe in high-security environments where sensitive information is stored, highlighting the need for constant vigilance in maintaining and updating biometric systems to minimize such risks.

❖ 4 REAL WORLD EXAMPLE

1. **Apple Face ID and Touch ID (Fingerprint and Facial Recognition)**

   This biometric technology is used on iPhones, where Touch ID is fingerprint recognition while Face ID is facial recognition. Touch ID is only available from iPhone 6 until iPhone 8.This sensor is put on the iPhone's home button. Face ID is able to provide authentication by using TrueDepth camera system and some advanced technologies that allow it to scan accurately the user face.However, this biometric features have same function which are to unlock device or user account, secure purchases with Apple Pay and use system provided APIs for third party app to ask user authenticate their account.By using this features , user do not need to remember their password for third party and make a secure payment.

2. **Nuance Gatekeeper / Nuance Free Speech (Voice Biometric)**

   Nuance Free Speech is a voice biometric authentication technology that is used by Barclays which is a British universal bank. Nuance Free Speech was implemented in Barclays to improve their telephony security service. This technology will authenticate and verify the caller identity and ensure the flow of call is not interrupted. "The biometric verifications will verify the client identity through their voice print , so that the agent does not need to ask for password or question to verify it"[7]. With that, it will save time , increase security in terms of fraud and increase customer satisfaction because they will not be rejected.

3. **Amazon One (Palm Identification)**

   Amazon One is a device that allows customers to enter a building, identify themselves, and pay with their palms in a quick, convenient, and contactless manner. The service is extremely secure, and it employs custom-built algorithms and hardware to generate a person's unique palm signature, simplifying a variety of tasks ranging from payment to access [5]. This technology can be used at Amazon Fresh stores and Whole Foods Market locations, or at third party businesses that have Amazon One for payment and identification.The reasons why they choose palm recognition is to let the user in control

of when and where they can use it, resulting in more secure. Therefore, instead of a key in their password or PIN for credit or debit card , they can only wave their palm to verify their bank account or identity.

4. **HP Ultrasonic Fingerprint Scanner**

The HP fingerprint scanner is implemented in their HP Laptops such as HP ZBook Firefly (16) G10 Mobile Workstation PC and HP Spectre x360 2-in-1 Laptop (14-ef2036TU) . This fingerprint scanner allows the user to unlock their laptop with a single touch without typed the password. This ultrasonic fingerprint scanner has more accuracy and speed to detect the fingerprint. How it works is by capturing an image of the user fingerprint and checking it with a stored fingerprint database [8]. There are three primary categories of scanners which are optical,capacitive and ultrasonic. These scanners play a crucial role in fingerprint reading .

❖ TASK DISTRIBUTION

TASK DISTRIBUTION	PIC
Introduce the technology	NUR AMIRA SOFEA BINTI OTHMAN
Historical Milestones	NUR ALIA NADHIRAH BINTI MOHD ZAILI
Advantages And Disadvantages	UMAIRAH SHUHADA BINTI AHMAD
Real World Examples	NUR AUNI LIYANA BINTI MOHD KHAIRI

REFERENCES

[1] "Use Touch ID on iPhone and iPad – Apple Support (MY)," *Apple Support*, Feb. 14, 2024. https://support.apple.com/en-my/102528

[2] "Uses for face ID and touch ID," *Apple Support*. https://support.apple.com/en-my/guide/security/secc5227ff3c/web

[3] C. McDonald, "Barclays to use voice recognition for phone banking," *ComputerWeekly.com*, Aug. 01, 2016. [Online]. Available: https://www.computerweekly.com/news/450301604/Barclays-to-use-voice-recognition-for-phone-banking

[4] Nuance Communications, "Barclays improves their customer experience.," Nuance Communications, May 2014. [Online]. Available: https://www.nuance.com/content/dam/nuance/en_uk/collateral/enterprise/case-study/cs-barclays-en-uk.pdf

[5] "Palm-based Identity Solution – Amazon One FAQs – Amazon Web Services," *Amazon Web Services, Inc.* https://aws.amazon.com/one/faqs/

[6] "Amazon One," *Amazon One*. https://one.amazon.com/

[7] "Biometric Authentication | Strong Customer Authentication | Nuance," *Nuance Communications*. https://www.nuance.com/omni-channel-customer-engagement/authentication-and-fraud-prevention/biometric-authentication.html

[8] H. O. Store, "How Fingerprint Reading Tech Works in HP Laptops," *HP Tech Takes*, Nov. 08, 2023. https://www.hp.com/in-en/shop/tech-takes/post/fingerprint-reading-tech-works

[9] "HP Spectre 34.3 cm x360 2-in-1 Laptop 14-ef2036TU - Black," *13.5 (7Y6U3PA) - Shop HP.com India*. https://www.hp.com/in-en/shop/laptops-tablets/hp-spectre-x360-2-in-1-laptop-14-ef2036tu-bundle-7y6u3pa.html?facetref=e34d615df8488dbf

[10] "HP ZBook Firefly 16 G10 Mobile WorkStation PC," *40.64 Cm (16) (8L129PA) - Shop HP.com India*. https://www.hp.com/in-en/shop/laptops-tablets/hp-zbook-firefly-16-g10-mobile-workstation-pc-8l129pa.html

[11] L. Hendrickson, "Biometrics in Digital Identity: The Future of Secure Authentication," *Identity*, Oct. 09, 2023.
https://www.identity.com/the-growing-importance-of-biometrics-in-digita (accessed May 28, 2024).

[12] R. de Fremery, "You Are the Password: Understanding Biometric Authentication - The LastPass Blog," *blog.lastpass.com*. https://blog.lastpass.com/posts/2023/05/you-are-the-password-understanding-biometric-authentication (accessed May 28, 2024).

[13] "Biometrics will soon replace passwords once and for all," *www.mastercard.com*. https://www.mastercard.com/news/perspectives/2024/biometrics-will-soon-replace-passwords-once-and-for-all/

[14] J. Trader, "How Effective are Biometrics as an Alternative to Passwords?," *M2SYS Blog On Biometric Technology*, May 18, 2015. https://www.m2sys.com/blog/biometric-technology/how-effective-are-biometrics-as-an-alternative-to-passwords/

[15] BCAdmin, "A Brief History of Biometrics | BioConnect," *BioConnect | Biometric Authentication for Trusted Access*, Dec. 08, 2021. https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/

[16] LoginID, "The History of Biometric Technology [Infographic]," *The Local Brand®*, Dec. 26, 2021. https://thelocalbrand.com/the-history-of-biometric-technology-infographic/

[17] "The Evolution of Biometric Technology: Past, Present, and Future," *www.tbs-biometrics.com*, Jun. 03, 2020. https://www.tbs-biometrics.com/en/blog/evolution_of_biometrics

[18] "8 Different Biometric Authentication Advantages and Disadvantages – Ray's Now." https://www.raysnow.com/8-different-biometric-authentication-advantages-and-disadvantages/

[19]M. AlRousan and B. Intrigila, "Multi-Factor Authentication for e-Government Services using a Smartphone Application and Biometric Identity Verification," *Journal of Computer Science*, vol. 16, no. 2, pp. 217–224, Feb. 2020, doi: https://doi.org/10.3844/jcssp.2020.217.224.

[20] OVIC, "Biometrics and Privacy - Issues and Challenges," *Office of the Victorian Information Commissioner*, Jul. 2019. https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/