PiFortify: A Raspberry Pi-based Encryption Tool with Biometric Authentication

Melisha Kaur A/P Narinder Singh
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
tp057958@mail.apu.edu.my

Julia Juremi
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@staffemail.apu.edu.my

***Abstract*—To preserve the security and integrity of the sensitive data, encryption tools employ a variety of algorithms and approaches to ensure only authorised users are able to receive access. Various technologies can facilitate the identity verification process, including auditory and visual biometric devices such as iris scans, facial recognition, fingerprint scanners or voice recognition, and vascular scanners that use finger vein patterns for authentication. In certain cases, behaviour identifiers like typing recognition are utilized, which analyses an individual's typing pattern to identify them. This paper proposes a system that combines both encryption and biometric technologies to develop an encryption tool that requires biometric authentication via a fingerprint scanner to ensure verification for authorized user access. A Raspberry Pi to power both systems, to effectively implement this project. Additionally, a user-friendly graphical user interface (GUI) will be designed to ensure easy usage for end-users.**

Keywords—ciphers, cryptography, encryption, biometric

I. INTRODUCTION

In this digital era, the ever-increasing need for secure and user-friendly methods of data protection has created an urgent demand for reliable and easy-to-use encryption tools which combine robust security measures. Asian organisations were the most targeted globally in 2021 (Yu, 2022). In Malaysia alone, it was reported between the years 2017 and 2021, an astounding 70% of all business crime cases were categorised under cybercrime, with victims suffering losses that totalled to approximately RM2.23 billion ringgit (Basyir, 2021). The prospect of cyberattacks hangs over the globe menacingly, fuelling worries about risks to national security, economic instability and potential anarchy in our interconnected digital culture.

For many organisations, the implementation of proper security features to protect their digital assets is a necessity, either in compliance to industry standards or in order to ensure the longevity and safety of their organisation. However, this does not necessarily mean that the efforts being taken by these firms to secure their assets are efficient or effective. Many organisations may be utilising outdated security protocols or failing to address new and emerging threats, leaving their assets vulnerable to attackers (Dosal, 2020).

Even in cases where the scenarios mentioned above are not the case, many organisations fail to see the security gaps they have left behind, such as poor access role control, weak passwords, or unsecured networks, leaving an enticing trail for cyber-attackers to follow (Nayyar, 2020). Numerous departments store unique and independent types of sensitive information, each of which is equally critical to safeguard. When one department within an organisation is left vulnerable, it inevitably leads to an impact on the whole organisation. One form of security feature that is often left behind or regarded as of less importance is encryption. Inadequate encryption has been the result of many infamous cyber-attacks, such as the Equifax Data Breach which contained poor encryption of social security numbers of US citizens (Fruhlinger, 2020), Target Data Breach which had improper encryption of its payment systems (Hartzog & Solove, 2022) and Sony Pictures Hack, who failed to encrypt sensitive data, such as employee records, confidential emails and financial information (Young, 2021).

II. DOMAIN RESEARCH

A. Cryptography Encryption

According to Gençoğlu, a key tool for securing computer-mediated information transmission is cryptography. Data is artistically transformed using cryptography into an unintelligible format so that only the intended receiver can comprehend and utilise it. The paper, entitled 'Importance of Cryptography in Information Security' was written by Gençoğlu in 2019, and mainly focuses on exploring the critical role of cryptography in information security. The paper provides an in-depth analysis of the techniques and development of cryptography as well as its application in protecting sensitive information in various scenarios. The author emphasises the vital role encryption plays in cryptography, stating that cryptography is commenced by encryption and decryption keys.

B. Confidentiality in CIA Triad

The CIA triad is a fundamental concept in cybersecurity, consisting of three key principles: confidentiality, integrity, and availability, which form the basis for safeguarding information systems and data. The primary focus of this domain is specifically placed on the confidentiality element of the CIA triad. Samonas and Coss (2014) discuss the concept of confidentiality as a fundamental principle of information security. They trace the origin of the term to its Latin roots, which conveys the idea of trust and reliance. The authors note that confidentiality has its roots in military operations that required top-down control over information access, limited to only those with access due to a need-to-know basis. They emphasize that the protection of data and information must ensure that its use is authorized, confined to only authorized people for authorized purposes.

C. Biometrics

Biometric data is unique to an individual which makes it an optimal solution across a wide range of fields such as military, government, organisations and even commercial application. Various biological traits are typically collected and utilised in identification systems such as fingerprints scanning, facial recognition, voice recognition, iris recognition, retinal scan, hand geometry, signatures, DNA-based recognition or even a hybrid consisting of more than one trait. The implementation of biometric solutions extends to various security domains such as access control, surveillance, mobile device security, disaster management, fraudulent technologies, attendance management, law enforcement and so on.

III. CURRENT AVAILABLE ENCRYPTION SYSTEM

A. Bitlocker

Bitlocker Drive encryption is a Microsoft Windows feature which functions to protect confidentiality of data and is integrated to the operating system itself. It tackles risks related to theft of data or vulnerability of lost, stolen or improperly decommissioned devices. Bitlocker's performance is enhanced and higher security is provided when utilised alongside Trusted Platform module or widely recognised as TPM which is a hardware component installed in most of the modern computers by production team. Although the combination of TPM and Bitlocker provides reinforced security to protect data and eliminate any possibilities that the system has not been tampered with during its offline period, Bitlocker can still be employed for Windows operating system drive with an additional step where the user is required to insert a physical USB startup key in order to access the computer. Other than TPM, there is also a method to lock the normal startup process with Bitlocker and the system can only be accessed with a PIN (Personal Identification Number) or with a startup key appended to a USB which ensures a computer cannot be broken into since multifactor authentication is implemented. Bitlocker helps to prevent unauthorised third party access by heightening systems and files security as well as making it a priority to ensure that the system data cannot be accessed even when the computers are sold, stolen, recycled or decommissioned. Figure 1 below shows the Bitlocker icon available in Microsoft Windows platform.

Figure 1 Bitlocker (Tan, Zhang & Bao, 2020)

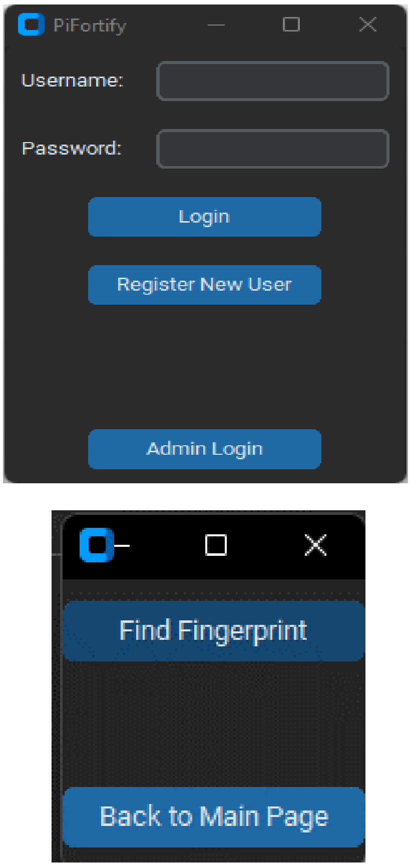
B. AXCrypt

AxCrypt is an encryption software application utilised to encrypt open-source files and folders. This tool uses 256-bit AES for its encryption process without the need of connection to the internet. However, AxCrypt mostly focuses on file encryption and is not capable of full disk encryption. AxCrypt generates an archive which holds the encrypted file and extra metadata and once a file has been encrypted, the initial file will be deleted and removed. This particular software can be implemented and used in various operating systems such as Windows, Mac, Android and iOS. AxCrypt only requires one master password to encrypt and decrypt the files. Moreover, it has various features such as key sharing, password management and password reset. Key sharing allows sharing of the secured and encrypted files with other users whereas password manager provides an encrypted space to save passwords. The cryptography algorithms used are AES-128 and AES-256 for file encryption, PBKDF2 with HMAC-512 for deriving keys, HMAC-512 to check data integrity and finally 4096-bit RSA for the account key. Figure 2 below shows the logo for the AXCrypt tool.

Figure 2 AxCrypt Encryption Tool (axcrypt.net,, 2023)

IV. PROPOSED SYSTEM - PiFortify

Figure 3 below shows the graphical user interface for user login. Once a user has keyed in the correct username and password associated with their account, they will be brought to the second form of user authentication which has been implemented into the system, a fingerprint- based form of biometric authentication.

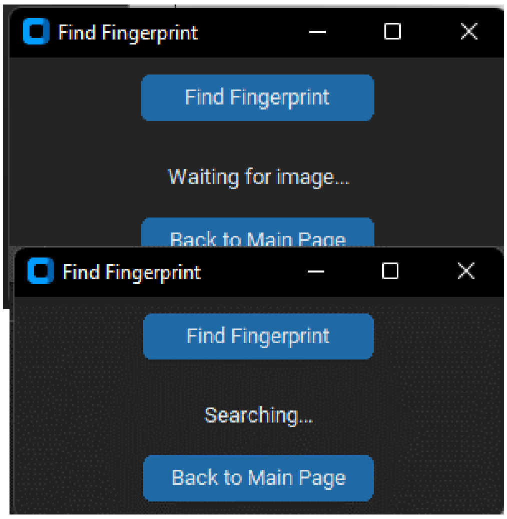


Username:

Password:

Figure 3 PiFortify Login Page

When a user clicks on the 'Find Fingerprint' button, the system will prompt the user to place their fingerprint on the fingerprint scanner, as seen in Figure 4 below.

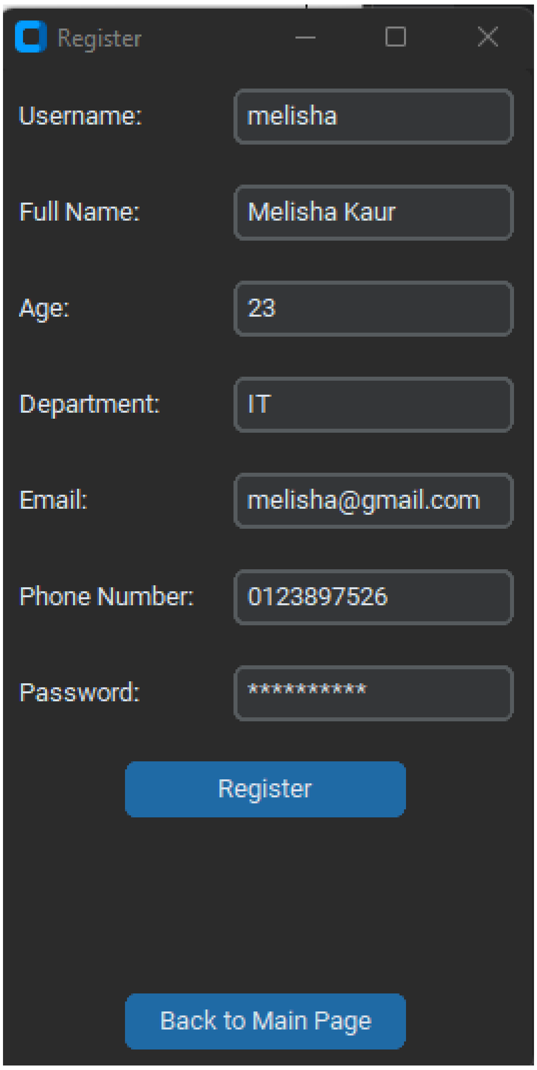


Waiting for image...

Searching...

Figure 4 PiFortify Searching for Fingerprint

Once the fingerprint has been placed by the user, the system will automatically begin templating the fingerprint data and start authenticating the fingerprint image to ensure that the user's fingerprint matches the user's profile. Once the user has successfully authenticated their fingerprint, they can begin using the main application where the encryption and decryption process occurs. To begin using the application, a user must first create a profile before they are able to log in. This is when the user registration process occurs, where users are prompted to fill up their personal details for record keeping, including their username, password, age, full name, department, email, phone number and password. Once a user clicks the Register button, they will be brought to a new window that allows them to enroll their fingerprint, which can be seen in Figure 5 and 6 below.



Username: melisha

Full Name: Melisha Kaur

Age: 23

Department: IT

Email: melisha@gmail.com

Phone Number: 0123897526

Password: **********

Figure 5 PiFortify Registration Page

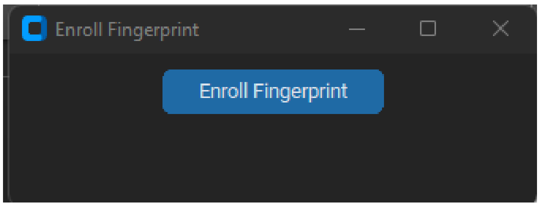
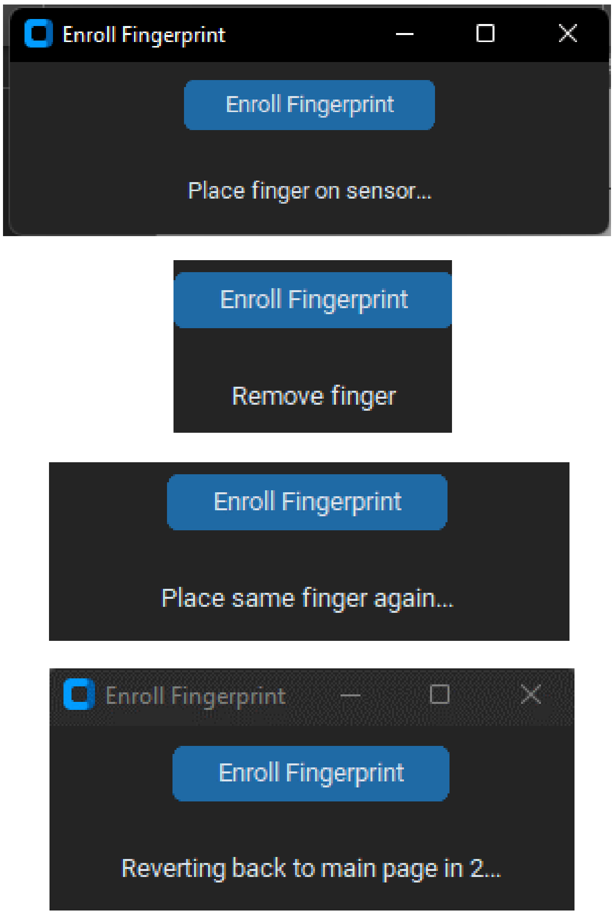


Figure 6 PiFortify Enrolling Fingerprint 1

Clicking the Enroll Fingerprint button will automatically allow the system to begin the template matching algorithm, the process can be seen in Figure 7 below.



Place finger on sensor...

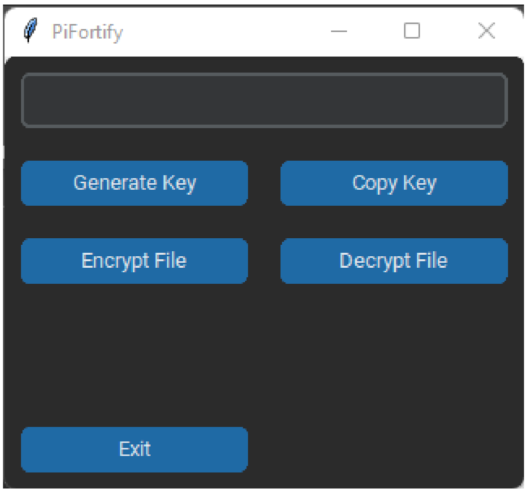
Remove finger

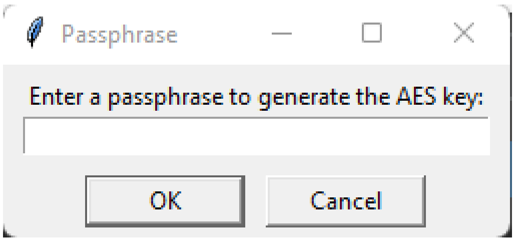
Place same finger again...

Reverting back to main page in 2...

Figure 7 PiFortify Enrolling Fingerprint II

Once the user has completed the fingerprint registration, the system will revert the user back to the main menu. A user can log into their account once an administrator has approved their user registration request. The main application is where the user can perform their encryption and decryption. To begin, a user must first click on the 'Generate Key' button, which will allow the system to bring up a window that asks the user for a passphrase, which can be seen in Figure 8 below.

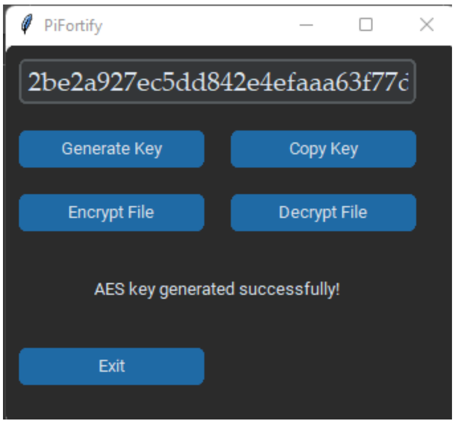




Enter a passphrase to generate the AES key:

Figure 8: PiFortify Encryption Decryption Page

To generate the AES key, a user must provide a passphrase. This passphrase will be converted into an AES key, which will then be used for the encryption and decryption process. Once a passphrase is provided, the AES key is generated, which can be seen in Figure 9 below.

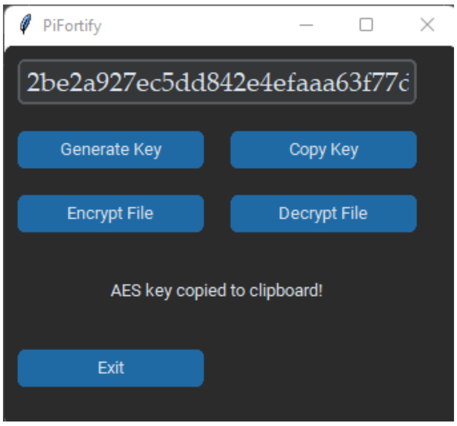


2be2a927ec5dd842e4efaaa63f77c

AES key generated successfully!

Figure 9 PiFortify AES Key Generation

Once the AES key has been generated, a user can then begin encrypting their file. They may do this by first clicking the Encrypt File button which will allow the user to click on a file they would like to encrypt. Once the file is chosen, the system will automatically encrypt the file's contents. To decrypt the file, the user must place the same AES key used to encrypt the file in the provided text field. They must then click the Decrypt button, which will allow them to choose their file. Once a file is chosen and the AES key is provided, the file's contents will be decrypted.



2be2a927ec5dd842e4efaaa63f77c

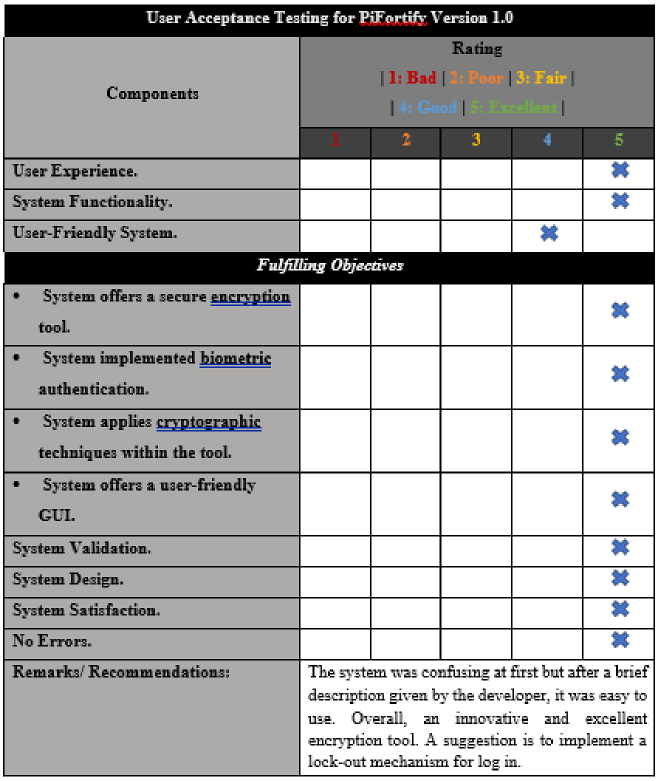
AES key copied to clipboard!

Figure 10 PiFortify AES Key Copy Option

Lastly, for ease of use, a copy key is provided as shown in Figure 10. To copy the AES key onto a user's clipboard, all they must do is click the Copy Key button and the system will automatically copy the key. To log out of the system, the user must click the exit button.

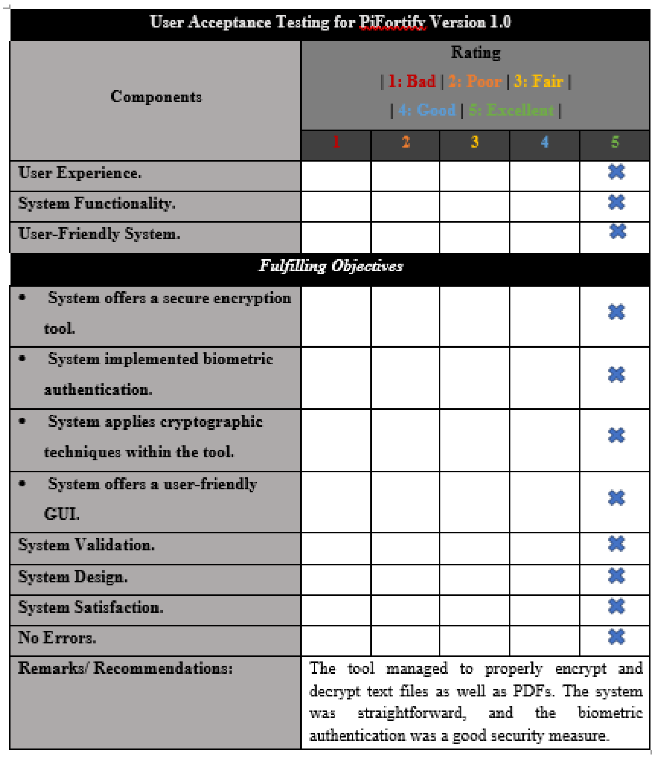
IV. USER ACCEPTANCE TESTING (UAT)

The test was conducted with 5 users, all of whom are currently working in a workspace that handles confidential data, as these are the target users. The test was done in real life as users had to physically use the fingerprint scanner to utilise the application. Users were given a brief description of how to utilise the tool and were then asked to fill the form up based on their respective experiences. Figure 11 – Figure 15 below shows the UAT results coming from all 5 users.



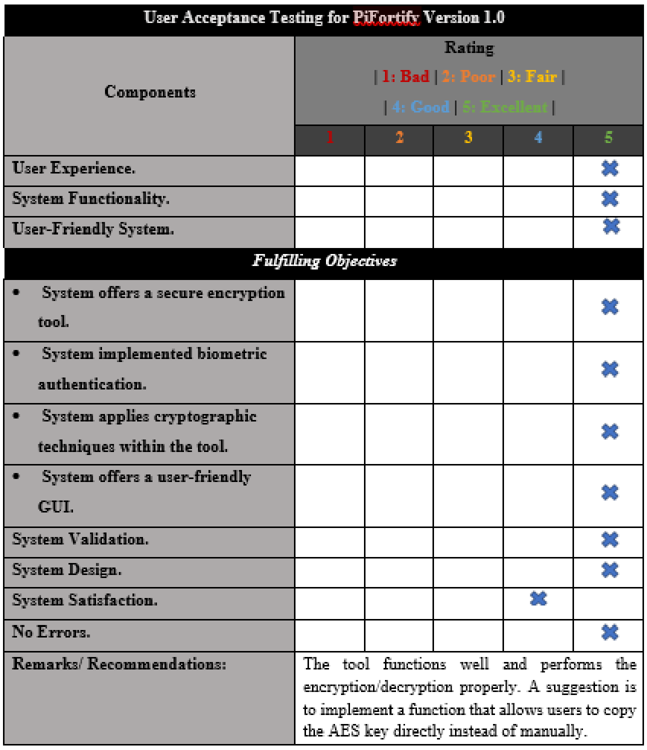
User Acceptance Testing for PiFortify Version 1.0					
Components	Rating | 1: Bad | 2: Poor | 3: Fair | | 4: Good | 5: Excellent |				
	1	2	3	4	5
User Experience.					✖
System Functionality.					✖
User-Friendly System.				✖	
Fulfilling Objectives					
• System offers a secure encryption tool.					✖
• System implemented biometric authentication.					✖
• System applies cryptographic techniques within the tool.					✖
• System offers a user-friendly GUI.					✖
System Validation.					✖
System Design.					✖
System Satisfaction.					✖
No Errors.					✖
Remarks/ Recommendations:	The system was confusing at first but after a brief description given by the developer, it was easy to use. Overall, an innovative and excellent encryption tool. A suggestion is to implement a lock-out mechanism for log in.				

Figure 11 PiFortify UAT Result 1



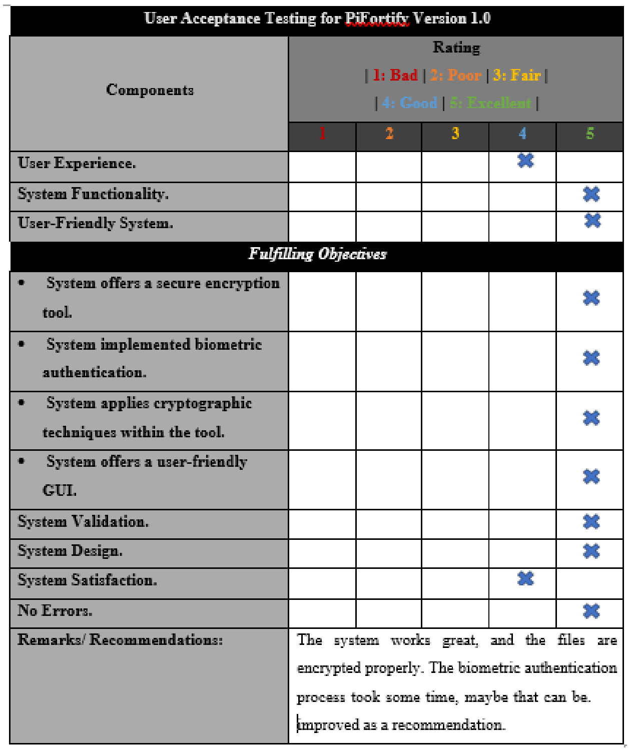
User Acceptance Testing for PiFortify Version 1.0					
Components	Rating | 1: Bad | 2: Poor | 3: Fair | | 4: Good | 5: Excellent |				
	1	2	3	4	5
User Experience.					✖
System Functionality.					✖
User-Friendly System.					✖
Fulfilling Objectives					
• System offers a secure encryption tool.					✖
• System implemented biometric authentication.					✖
• System applies cryptographic techniques within the tool.					✖
• System offers a user-friendly GUI.					✖
System Validation.					✖
System Design.					✖
System Satisfaction.					✖
No Errors.					✖
Remarks/ Recommendations:	The tool managed to properly encrypt and decrypt text files as well as PDFs. The system was straightforward, and the biometric authentication was a good security measure.				

Figure 12 PiFortify UAT Result 2



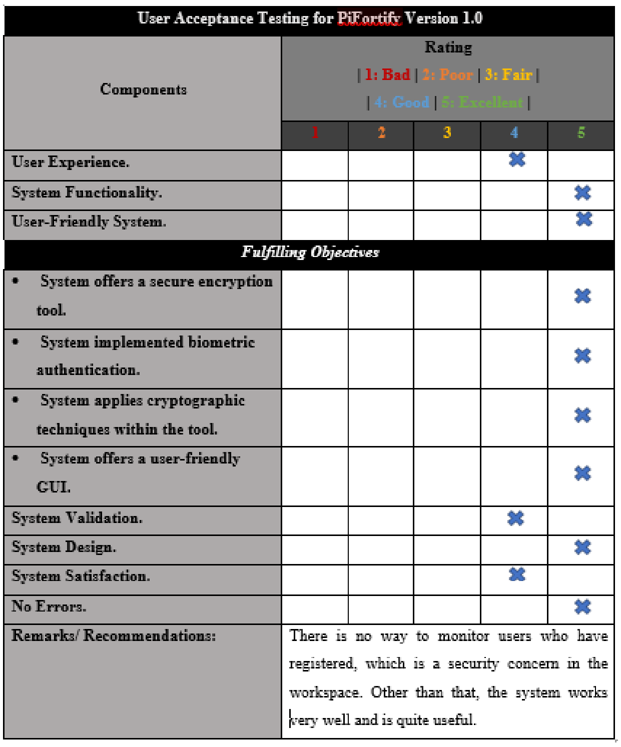
User Acceptance Testing for PiFortify Version 1.0					
Components	Rating | 1: Bad | 2: Poor | 3: Fair | | 4: Good | 5: Excellent |				
	1	2	3	4	5
User Experience.					✖
System Functionality.					✖
User-Friendly System.					✖
Fulfilling Objectives					
• System offers a secure encryption tool.					✖
• System implemented biometric authentication.					✖
• System applies cryptographic techniques within the tool.					✖
• System offers a user-friendly GUI.					✖
System Validation.					✖
System Design.					✖
System Satisfaction.				✖	
No Errors.					✖
Remarks/ Recommendations:	The tool functions well and performs the encryption/decryption properly. A suggestion is to implement a function that allows users to copy the AES key directly instead of manually.				

Figure 13 PiFortify UAT Result 3



User Acceptance Testing for PiFortify Version 1.0					
Components	Rating | 1: Bad | 2: Poor | 3: Fair | | 4: Good | 5: Excellent |				
	1	2	3	4	5
User Experience.				✖	
System Functionality.					✖
User-Friendly System.					✖
Fulfilling Objectives					
• System offers a secure encryption tool.					✖
• System implemented biometric authentication.					✖
• System applies cryptographic techniques within the tool.					✖
• System offers a user-friendly GUI.					✖
System Validation.					✖
System Design.					✖
System Satisfaction.				✖	
No Errors.					✖
Remarks/ Recommendations:	The system works great, and the files are encrypted properly. The biometric authentication process took some time, maybe that can be improved as a recommendation.				

Figure 14 PiFortify UAT Result 4



User Acceptance Testing for PiFortify Version 1.0					
Components	Rating | 1: Bad | 2: Poor | 3: Fair | | 4: Good | 5: Excellent |				
	1	2	3	4	5
User Experience.				✖	
System Functionality.					✖
User-Friendly System.					✖
Fulfilling Objectives					
• System offers a secure encryption tool.					✖
• System implemented biometric authentication.					✖
• System applies cryptographic techniques within the tool.					✖
• System offers a user-friendly GUI.					✖
System Validation.				✖	
System Design.					✖
System Satisfaction.				✖	
No Errors.					✖
Remarks/ Recommendations:	There is no way to monitor users who have registered, which is a security concern in the workspace. Other than that, the system works very well and is quite useful.				

Figure 15 PiFortify UAT Result 5

During this test version, 5 testers were given the freedom to utilise the application in any way they deem necessary, including access to admin roles as well to allow them to see the tool in its entirety. The consensus from these tests concluded that the system ran well and up to expectations, but there were certain improvements that could be made to the system to enhance the overall user experience. These remarks and recommendations were taken note of, and changes were implemented in the system based on the given recommendations.

V. Conclusion

Every project, no matter how well-executed, harbors room for improvement. PiFortify is no exception; it exhibits gaps in its graphical user interface, functionalities, and overall user experience. However, the completion of this project at its current stage is promising. It possesses the potential to be exceptionally beneficial for the intended users. As we continue to develop and enhance PiFortify, our goal is to broaden its reach and cater to an even wider audience.

References

[1] Yu,E. (2022). *Asia most targeted region in 2021, taking on one in four cybersecurity attacks.* ZDNET. https://www.zdnet.com/article/asia-most-targeted-region-in-2021-taking-on-one- in-four-cybersecurity-attacks/

[2] Basyir, M. (2021). Malaysians suffered RM2.23 billion losses from cyber-crime frauds. New Straits Times.

[3] Dosal, E. (2020). Top 9 Cybersecurity Threats and Vulnerabilities. Compuquip. https://www.compuquip.com/blog/cybersecurity-threats-vulnerabilities

[4] Nayyar, S. (2020). 5 Most Common Security Gaps Every Organization Struggles With. Spiceworks. https://www.spiceworks.com/it-security/security-general/guest-article/5- most-common-security-gaps-every-organization-struggles-with/

[5] Fruhlinger, J. (2020). Equifax data breach FAQ: What happened, who was affected, what was the impact? CSO. https://www.csoonline.com/article/3444488/equifax-data-breach-faq- what-happened-who-was-affected-what-was-the-impact.html

[6] Hartzog,W. & Solove, D, J. (2022). We Still Haven't Learned the Major Lesson of the 2013 Target Hack. Slate. https://slate.com/technology/2022/04/breached-excerpt-hartzog- solove-target.html

[7] https://www.nst.com.my/news/crimecourts/2021/07/708911/malaysians-suffered-rm223- billion-losses-cyber-crime-frauds

[8] Young, K. (2021). Cyber Case Study: Sony Pictures Entertainment Hack. Coverlink. https://coverlink.com/case-study/sony-pictures-entertainment-hack/

[9] Gençoğlu, M, T. (2019). Importance of Cryptography in Information Security. IOSR Journal of Computer Engineering (IOSR-JCE),21(1), 65-68.

[10] Samonas, S. & Coss, D. (2023). The Cia Strikes Back: Redefining Confidentiality, Integrity And Availability In Security. Jissec.

[11] Tan, C., Zhang, L., & Bao, L. (2020, October). A Deep Exploration of BitLocker Encryption and Security Analysis. In 2020 IEEE 20th International Conference on Communication Technology (ICCT) (pp. 1070-1074). IEEE.

[12] https://axcrypt.net/ Accessed on 23rd January 2023.