in collaboration with

Softwarica College of IT & E-commerce | Coventry University

Locking and unlocking files and folders to provide security with Fernet (Symmetric encryption) in python to improve the personal security sector.

Department of Ethical Hacking and Cybersecurity

STW303COM Individual Project

Submission deadline: Aug 23, 2022

Submitted by:

Niraj Sangraula

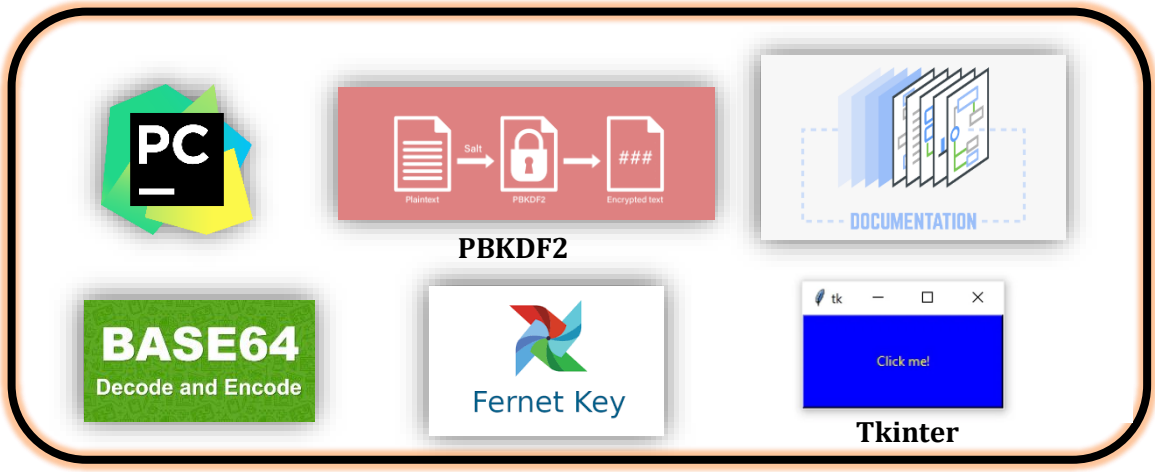
CUID: 10176391

Submitted to:

Mr. Manoj Shrestha

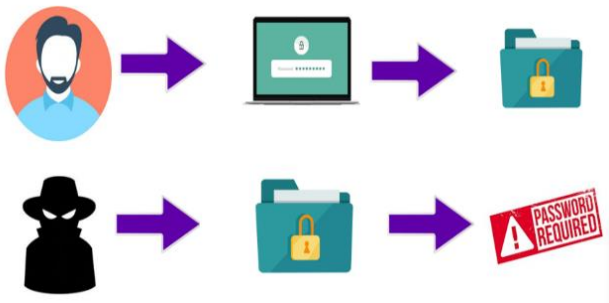
Project Supervisor

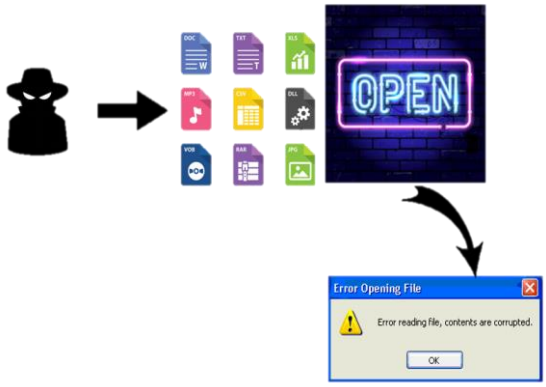
Concept Page



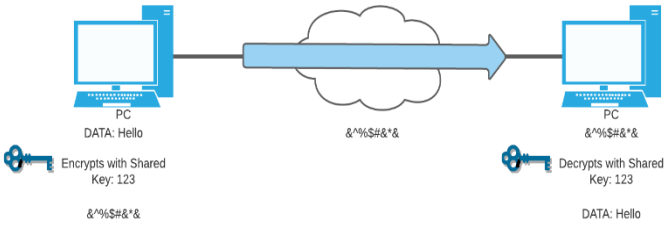
PBKDF2

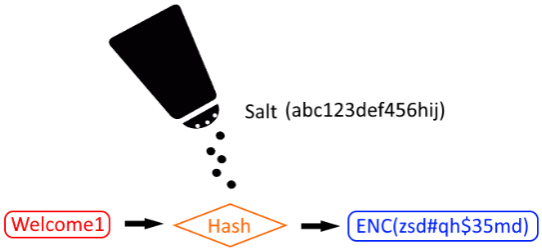
Tkinter





F&F Security





Abstract

The product falls under the personal security sector. In the personal security sector, security is provided by a person or an organization using various tools and technologies to safeguard vital property. With the growth of technology, it has also become easier to breach the privacy and security of an individual. So, securing files and folders in an individual device has become a vital task. So, in this documentation, there are case studies of companies like Microsoft, Viber, and others, who use similar functionalities as this product. Moreover, PESTEL analysis is also done to determine the factors that will affect the product launch. Different things like how the user and attacker interact with the product, GUI demonstration of the product, Agile methodology, future works, risk analysis, scope of the project, issues log, ethical view, Gantt Chart, revenue generation model, and so on are also discussed in this project. To do this documentation, Office 365 tools are used. The tools and technologies behind the product can encrypt and decrypt files and folders, make them inaccessible, and provide security and privacy. The tools and technologies that have played a vital role in doing this project are Python, Fernet, PBKDF2, base64, and others.

Keywords


PBKDF2
Encryption
Security
Authentication
Modification
Individuals protection
Fernet
Personal Security Sector
General Data Protection Regulation
Files and Folders protection
Privacy
Password Protection
The Electronic Transactions Act
Password and Salt
Real world cases
Decryption
Product

Table of Contents

List of Figures

List of Tables

Introduction

Personal security is that sector that helps an individual to protect their online accounts and devices from cyber threats. Individuals or organizations can also improve their security by integrating different personal security solutions like this product **Files and Folders (F&F) Security** in their system. The personal security sector mainly focuses on minimizing the harm that can be done to assets and protecting them from being damaged, theft, and compromised by providing them with different means of security like encryption, password protection, stenography, authentication, and others. (Protective Security Requirements, 2022). In addition, many companies work and provide security solutions in the personal security sector, such as NewSoftwares LLC, IO bit Protected Folder and Microsoft, to improve an individual or organization's security.

With the growing need for technology, security and privacy have become essential in the modern world. Nowadays, there is much information transferred via the internet daily. Moreover, securing files and folders in an individual device has become a vital task in an era where almost all communication is carried out through electronic means, whether through email or e-commerce. Furthermore, privacy and security are needed to transfer personal or sensitive data between two parties. However, there have been significant setbacks, whether in the case of people, businesses, or the military, where they suffered from data breach scenarios and faced a loss of millions of dollars. (Rosenthal, 2022). So, the need to lock files and folders on one's PC prevents them from being seen by prying eyes and prevents unauthorized access. Therefore, this application is the best choice as it can solve the case of privacy and security field. Furthermore, this application is not simple as the user can also lock files by setting a password to transfer them to another party securely. Even in between, if the third-party gains access to those files, they cannot edit or view them as a robust encryption mechanism is used here.

(This product **Files and Folders (F&F) Security** is a GUI-based desktop application made only for windows OS using python.)

Figure 1 General functionality of the product

Aim

This project aims to lock and unlock files and folders to provide security with Fernet (Symmetric encryption) in python to improve the personal security sector.

Objectives

- To lock and unlock files and folders using encrypt and decrypt, respectively.
- To password protect the files and folders and make them inaccessible.
- To provide additional security by hashing the password through PBKDF2.
- To select multiple files at a time and a folder to provide them with security.

Justification

In this section, we will discuss the problems people and businesses face in transferring data securely, mainly due to not locking files and folders. Moreover, we will also discuss mentioned problem's solutions here. Finally, the past issues companies and people have faced will also be addressed relating to this project.

Problem

The project focuses on the personal security sector. In the personal security sector, security is provided by a person or an organization using various tools and technologies to safeguard the vital property of the person. For example, suppose there are some files and folders inside the PC that people do not want anyone to see or find except themselves. Unfortunately, there is no built-in software on windows that password protects such data. Moreover, sending and receiving files between two parties are generally done in a plain text format, and those plaintext files are not encrypted. So, people are compromising their security and privacy.

Individuals and businesses suffer from weak security if they do not lock files and folders. For example, in 2020, the biggest chipset provider Intel suffered from a data breach scenario where an employee shared data on MEGA (data sharing platform) was leaked. This leaked data contained 20GB of files and folders containing yet-to-be-launched designs of various chipsets. (Hope, 2020). Likewise, in 2019 records containing sensitive information about patients' mental health were accidentally sent to the wrong person via email by an employee working under National Health Service (NHS). Due to this, the attackers leaked the information, and a data breach scenario occurred. In a recent story, it was found that 800 emails (organization containing 1000 employees) are misdirected and sent to the wrong person by an employee working in an organization every year.

If there had been a reliable tool or technology to save the problem currently faced by individuals and businesses, it would have been an enormous relief. However, the problem can be reduced if individuals or companies use this product.

Solution

Many files and folder locker applications are available in the market, but this product is simple to use, bugs-free, and supports old and new versions of Windows OS. All problems have been discussed in the above section. Therefore, in this section, only solutions will be discussed.

To explain how this product operates, the user first enters their preferred password and salt, then browses to lock the files or folders of their choice; Files or a folder are then encrypted after the user has chosen their option. After that, if a third party tries to access those locked files or folders, they cannot do it as the files and folders are not accessible and cannot even be viewed.

The data breach scenario would not have caused much damage, and the patients' leaked sensitive information could have been prevented if this product had been deployed to NHS. Additionally, even if documents from Mega containing yet-to-be-released designs of various Intel chipsets were leaked, but the documents had been secured using this product, it wouldn't have resulted in such a major catastrophe for Intel, as the incident response team could have avoided that major catastrophe by creating strong plans and policies before the attackers were able to breach the security provided to those documents.

Many people are facing problems related to files and folder security. For example, some files or folders on the hard drive are essential and contain personal information accessible to anyone using the PC. So, to solve this problem and give people their privacy and freedom by letting them keep personal information on their PCs, this product secures files and folders for windows.

Research questions

1. How to lock and unlock files and folders through encrypt and decrypt using symmetric encryption called Fernet?
2. How does PBKDF2 do hashing, and how is it different from the regular type of hashing?
3. How does this product affect the legal and ethical aspects?
4. How can this product do business and generate revenue?

(The four research questions will each have a dedicated section of the text devoted to their response. It will be made very obvious at the beginning of that topic in whatever section it is explained. Therefore, findings will not be presented in this document.)

Scope

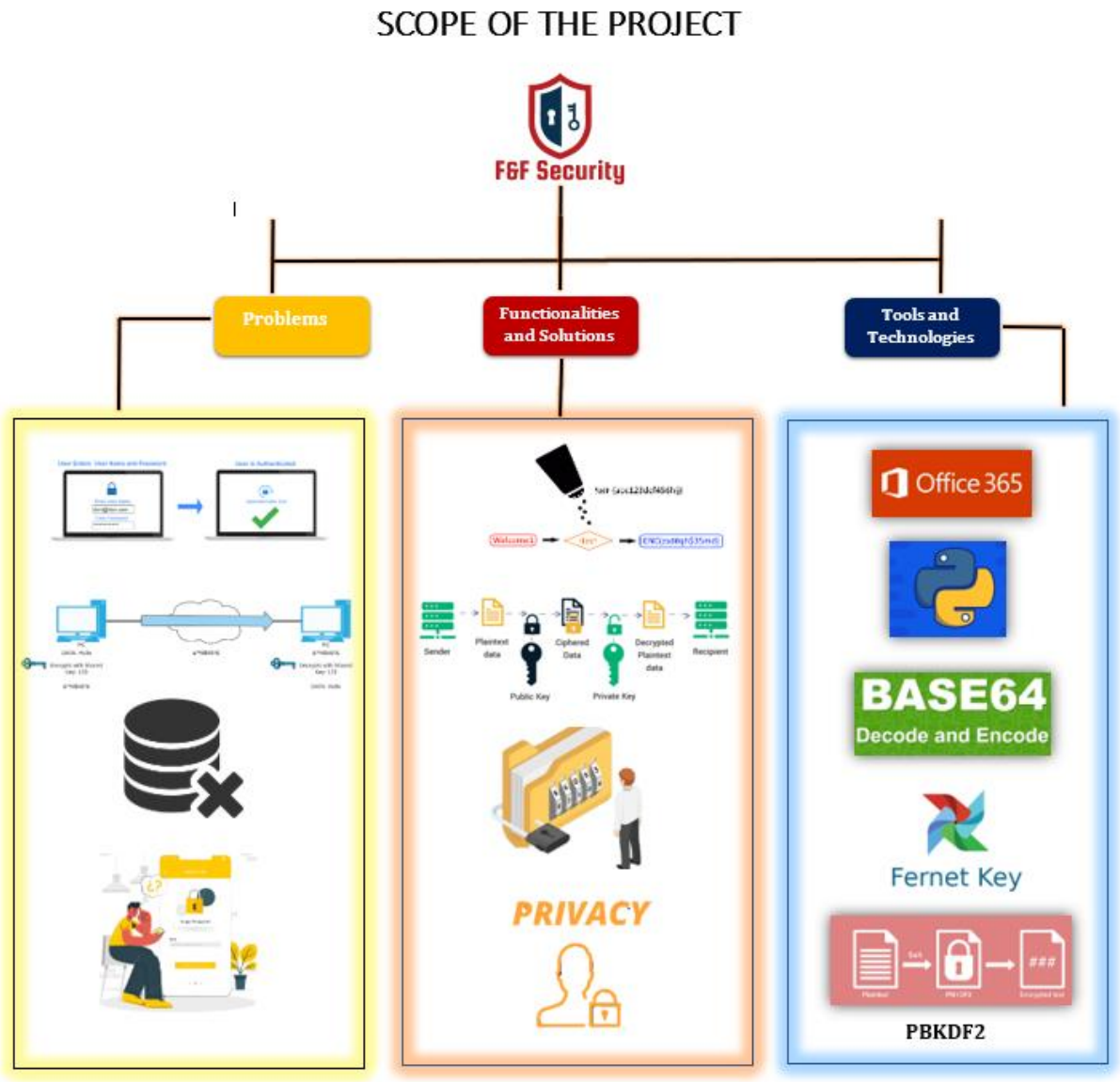


Figure 2 Scope of the project

Ethical and Legal Consideration

(There are four research questions. The third research question's answer is in this section.)

Ethical and legal aspects are well considered when documenting and writing the code. So, from the start of this project to the end, whichever tools were used were free and open source. So, no pirated tools have been used. The author has made the Majority of the infographics used in the document. Those that the author did not create are appropriately cited, and the original author is given credit. The resources and knowledge outside the knowledge criteria are taken from the internet. Furthermore, proper citation is also done in the reference section. This product complies with the GDPR (General Data Protection Regulation.), so the confidential data from users will be encrypted and stored on the server when collecting data. So, the collected data will not be used for personal benefit. Moreover, the user is the valid owner of their data, so when collecting data, they will be informed and given 100% rights over their data. They will also have complete control over it.

This product Files and Folders (F&F) Security is also protected by Article 44 of (The Electronic Transactions Act (ETA), related to Pirate, Destroy or Alter computer source code. So, if people or a company steals, pirate, destroys, or modifies this product's source code, they will be subjected to this act with a punishment of 3 years in prison or two hundred thousand Nepalese rupees or both. Moreover, a complication related to law, privacy, and copyright issues might arise. However, for now, there are no such complications.

Figure 3 ETA Representation and GDPR logo

Is it ethical?

In the above section, we have mentioned that users' data will be collected. Many people may find it unethical and wrong, but this product and other products collect individuals' data. If the collection is done within a limit, it is ethical; if it is done over the limit, it is unethical. So, suppose the company or product collects users' private information, such as their password, credit card information, mental health information, and others, with or without permission from the user. In that case, it is unethical and punishable by law.

So, a company should only view and collect information such as users' email, OS version, etc. Moreover, the sensitive and private information of the user stored in the server should be encrypted and not be accessed in any way. So, the personal data collected by this product will be encrypted and will not be accessed by this product. Collecting data is necessary to improve user experience, see how and where this product is being used, and prioritize a strategy for further product development by managing the result.

Figure 4 Ethical representation

Literature Review

We use devices and online accounts like email, social media, banking, and others, which are vulnerable to cyber threats. So, personal security is that sector that helps an individual to protect their online accounts and devices from cyber threats. Both individuals and organizations can improve their security by integrating different personal security solutions like this project Files and Folders (F&F) Security in their system. The personal security sector mainly focuses on minimizing the harm that can be done to the assets and protecting them from being damaged, theft, and compromised by providing them with different means of security like encryption, password protection, stenography, authentication, and others. In addition, many companies work and provide security solutions in the personal security sectors, such as NewSoftwares LLC, IO bit Protected Folder, Microsoft, and Viber, to improve an individual or organization's security.

Desk based research

Writing a dissertation is a complicated task, unlike coursework. Before attempting to write it, detailed research and investigation are needed. Moreover, a predefined topic and assignment briefs are not given to students like in coursework. Instead, they have to research on their own and come up with a topic they want to write about and are interested in. Furthermore, specific guidelines mentioning what font size to choose, what font style, what structure to follow, or other instructions are not given to students; they need to choose their writing style. However, it has to be consistent. Mistakes such as writing with one font style and size on one section and choosing another in a different section

should be avoided. Moreover, legal and ethical aspects should also be included in the dissertation. (Scribbr, 2022).

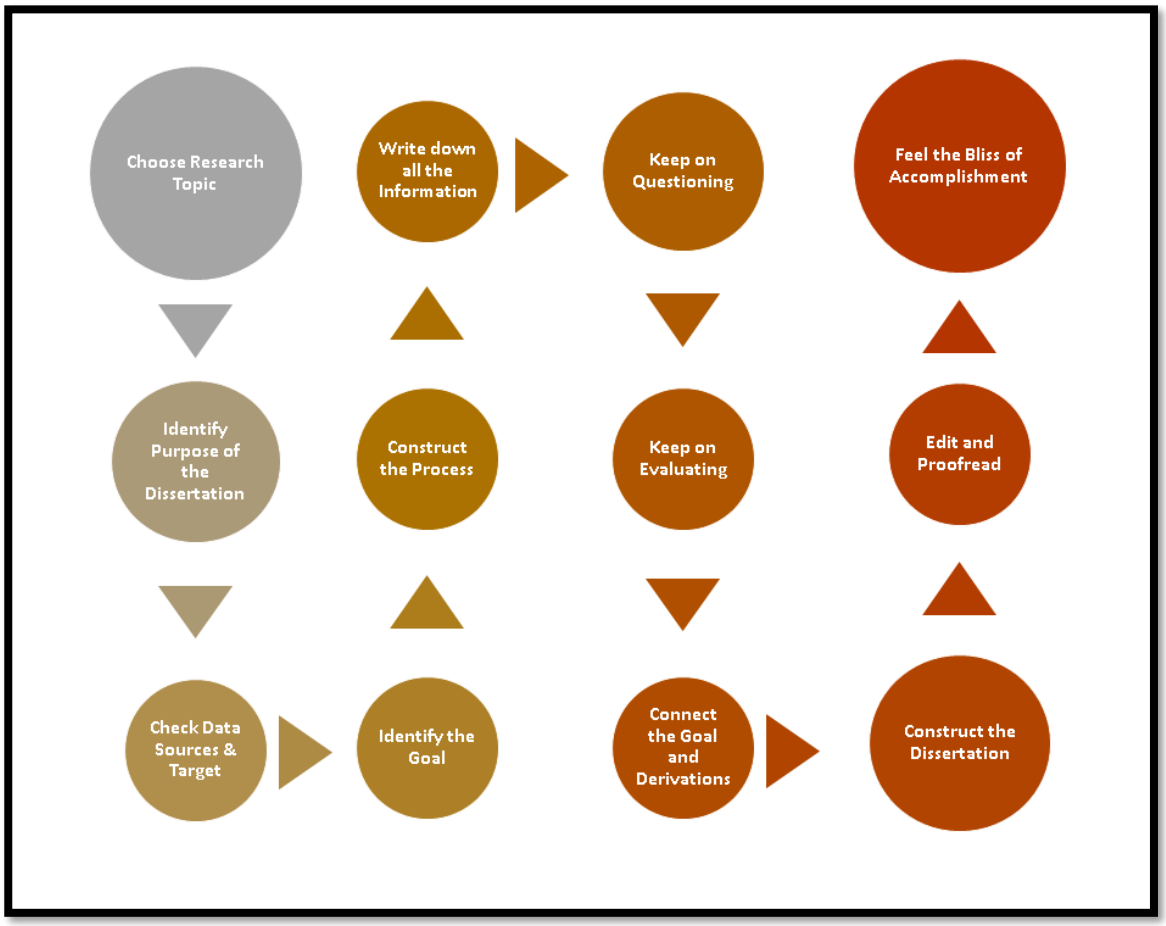


Figure 5 Dissertation writing process

NewSoftwares LLC: How does it password protects the files?

NewSoftwares LLC is a data security company that has existed since 2001, even before Facebook. Moreover, they provide security solutions in information security to clients, partners, and customers. They work daily to improve and create new products using the latest technology available in the market. Their primary focus is on data privacy and encryption. Furthermore, like this product, this company has made various products like folder lock, USB lock, copy protect, veracrypt, and others. These products are similar to ours as their primary function is to provide security to files and folders. (NewSoftwares, 2022)

Nowadays, people have different errands and forget what is important and should be given attention to. Since the internet has become one of the important factors in people's lives, it has become easier, better, and faster to connect, access, and store data in a device. Moreover, people can now store terabytes of data on their hard drives like videos, audio, photos, files, and other file formats. However, easier information technology access has also led to different security threats. In simple words, data stored in the hard drives are not safe. The attacker can wipe and steal the private data stored on the victim's PC within seconds. Nevertheless, this problem can be solved with an outstanding solution. Software by the name 'Folder Protect' by NewSoftwares can help users protect their important files, drives, extensions, programs, folders, and so on. With the use of folder protect, an outsider cannot access, view, delete and modify the legitimate user's files and folders. Moreover, this application not only password-protect files and folders but can also encrypt them using AES 256-bit encryption, which can be exchanged between two parties securely through a communication line. This software is compatible with Windows 10/8/7/Vista and many more. Folder protect covers and provide security to wide range of extensions some of them being .bmp, *.mp3, * .wmv, * *.avi, *.gif and so on. Moreover, this software cannot be uninstalled; only genuine users can delete this software using the set password.

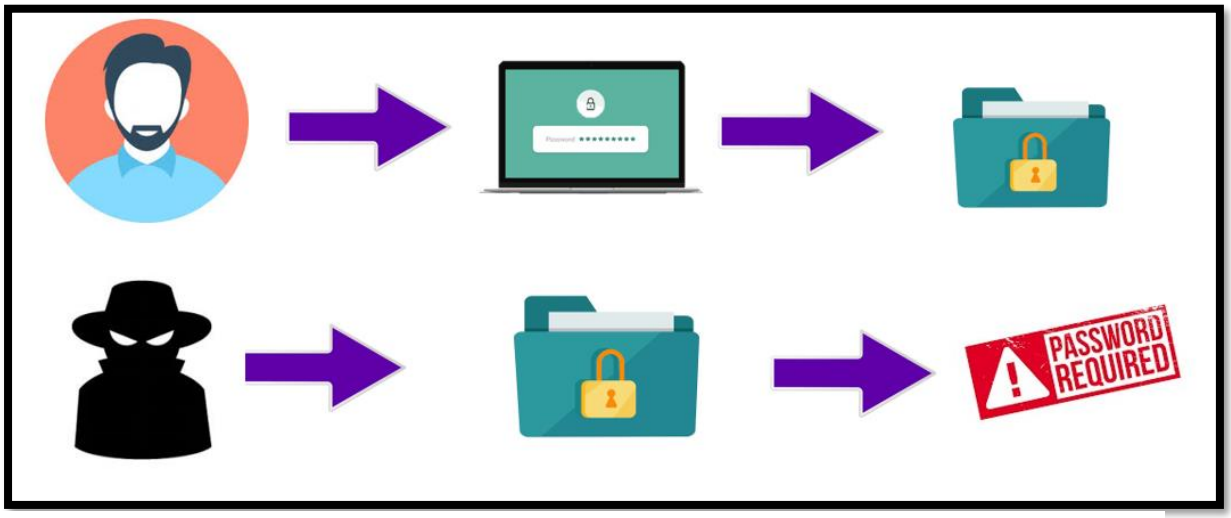


Figure 6 Password protecting the files

IO bit Protected Folder: How does this lock files and make them inaccessible?

IO bit company, founded in 2004, works mainly to provide security software for PC to enhance their performance and security. It is not entirely safe to store private data like spreadsheets, patient data, HR data, and so on the PC without providing protection. So, software from the IO bit, 'protected folder,' safeguards private files and makes them inaccessible if anybody other than the owner tries to access them. Moreover, in this modern era, password protection to private files should be done even if a close one wants

to access the PC. Malware like a virus, trojans, etc., threaten private files and damage them, making them corrupted. (IO bit, 2022)

For instance, in May 2017 WannaCry ransomware attack took place through which the victim's money was extorted. Through the WannaCry attack, the attacker can encrypt the victim's data or files and demand ransomware. Mainly Microsoft windows OS was targeted by the attackers. As a result, 230,000 computers globally suffered from the 2017 WannaCry attack. The first victim of this attack was a Spanish company called Telefónica. (What Is Wannacry Ransomware?)

Moreover, NHS hospitals were also the victim of this attack, and many surgeries were canceled due to data theft from attackers. It was estimated that due to this attack, $4 billion in financial loss happened across the world. However, with Protected Folder, people and an organization can safeguard their private data or files by locking files stored on their PC through which the attacker cannot steal or encrypt the user's data, and the user will not have to pay ransomware to get the data. (What Is Wannacry Ransomware?)

IObit Protected Folder not only password-protects private files but also saves them from unwanted use. There are other features too provided by this software like it can hide images, data, documents, videos, and other file formats on PC, which nobody can search, view, or access. Even if the unauthorized person gets access, they cannot view it or see their thumbnail. Moreover, the unauthorized person cannot run, copy, or read the file's content. So, there are no chances of modification done to the files.

Furthermore, the attacker cannot delete the files without unlocking them with the password. No one can move, delete or modify the file's content without the owner's permission. So, the only way to access those files is with the password provided before locking it. It is a good software through which a person or a company can save millions as it prevents data theft. This software is from a trusted company that is safe and secure and does not contain viruses, adware, and spyware.

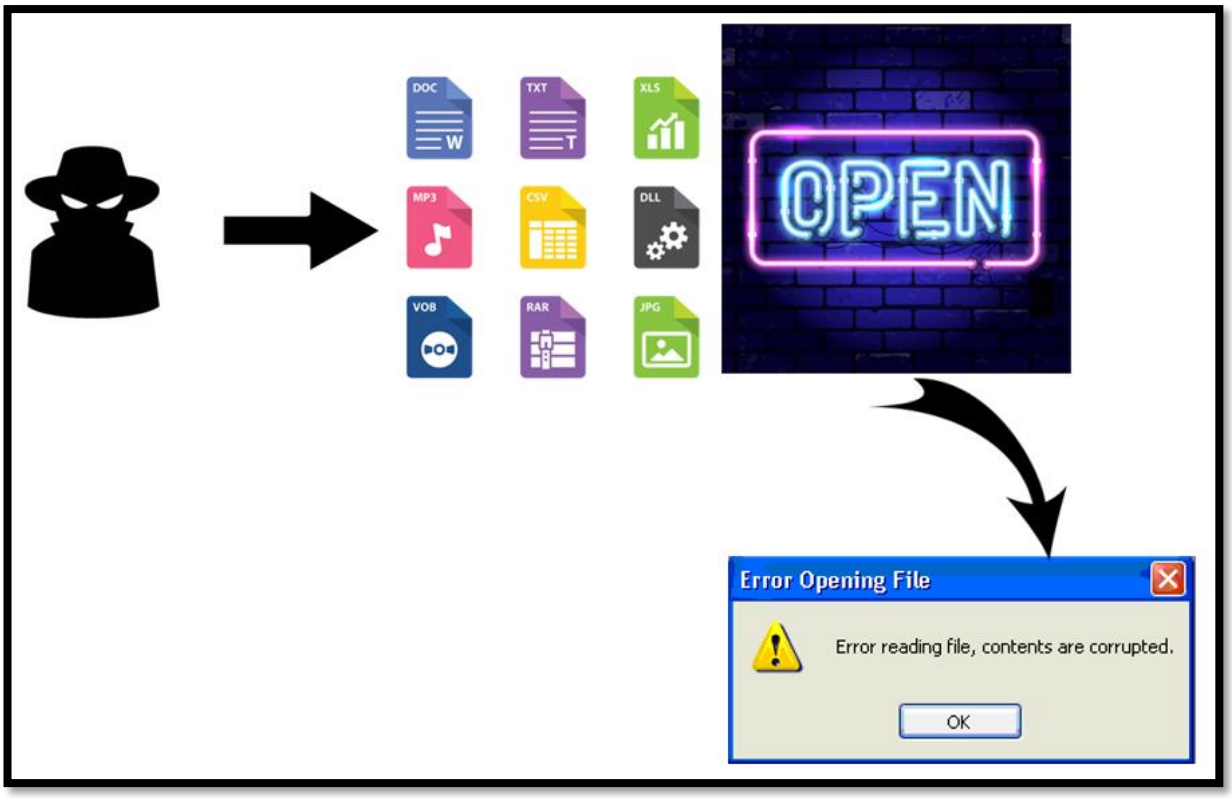


Figure 7 Locking files and making them inaccessible

Microsoft: How does this company provide robust email security?

Private information such as patient health information, spreadsheets containing company financial records, employee sensitive information, legal contracts, sales contracts, and others are shared daily within or outside the company. Therefore, the mailboxes can become a massive target for attackers to quickly get private information through which situations like blackmailing and data breach scenario may occur. So, it is crucial to encrypt or password-protect email contents before sending them.

Late in 2020, it was discovered that foreign hackers monitored the email accounts of US government officials. Furthermore, the activity the attackers did was not only monitoring. This cyberattack was labeled as SolarWinds hack. This cyberattack did not affect only Microsoft because this attack targeted thousands of other organizations. SolarWinds provides infrastructure and network monitoring solutions, technical services, and many more services to their partner and customer. Microsoft was also their partner and had been using its product, SolarWinds Orion. Attackers gained access to Microsoft's network, systems, and data through Orion, as the installation of malware compromised its security during an update. After exploiting the vulnerability, the attackers gained access to Microsoft's users and accounts. Through that intrusion, victims were also spied upon whether they were sending email, accessing their private files, or doing other things.

Moreover, high-level government officials and Microsoft Office 365 accounts were also breached. This intrusion was only detected in 2020, but it was later discovered that it was starting to happen in 2019. [(Oladimeji and kerner, 2022)]

With Office 365 Message Encryption, all the problems mentioned above can be solved. This 365 encryption can be easily implemented when sending emails to another person. Through this service, people can encrypt their email messages and send them to people working within or outside the organization. This service works with Gmail, Yahoo, Outlook, and other email services. Through this service, only the intended receiver can view the message. [(Message Encryption, 2022)]

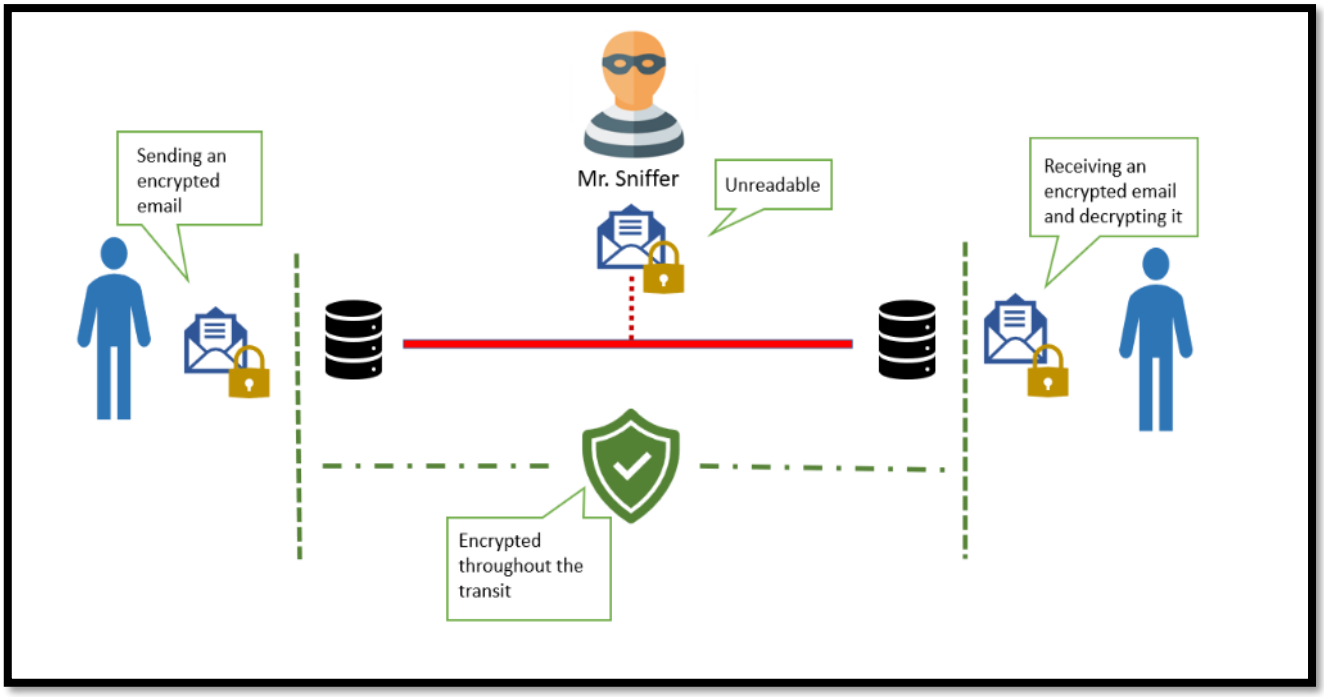


Figure 8 Encrypted email

Moreover, suppose the government officials encrypted their email when sending it or the employees working under Microsoft encrypted their email. In that case, a man-in-the-middle attack can be prevented. No one can view the files attached to that email except the intended receiver, and nobody can modify it. So, a strong layer of security can help a company or an individual to be saved from humiliation and ransomware attacks. Through this simple process, data breach scenarios can be prevented. Moreover, implementing two-factor authentication, keeping a strong password, and avoiding phishing scams can help safeguard Microsoft accounts.

Viber: Why is end-to-end encryption implemented?

Messaging apps have made it easier to communicate with others from all around the world. But with the new ways of communication that are developing every day, it has also become easier to breach the privacy and security of an individual. Moreover, the private messages or data sent between a sender and a receiver can risk being seen and controlled by an unauthorized person, the messaging app company, internet service providers, and governments. So, it is crucial to implement end-to-end encryption on those messaging apps through which no one except the sender and intended receiver can read the messages and make changes to the data in the form of audio, videos, files, and so on. Unfortunately, popular apps like Instagram, Facebook Messenger, Snapchat, and others have not implanted end-to-end encryption in their system. However, in the case of Viber, they have implemented end-to-end encryption in their app through which private sharing, messages, calls, and so on are secure, meaning no third party can access it.

Moreover, the unique feature of Viber is that every chat has its color-coded-based encryption. Green represents the person as a trusted source and encrypted communication line. Grey represents the encrypted communication line, but the source is not to be trusted. Red means the communication line is not secure, and the contact is not from a genuine source either. Moreover, Viber does not only provide an end-to-end encryption feature but also chats with PIN access and destructing chats after some time feature. (G, 2020)

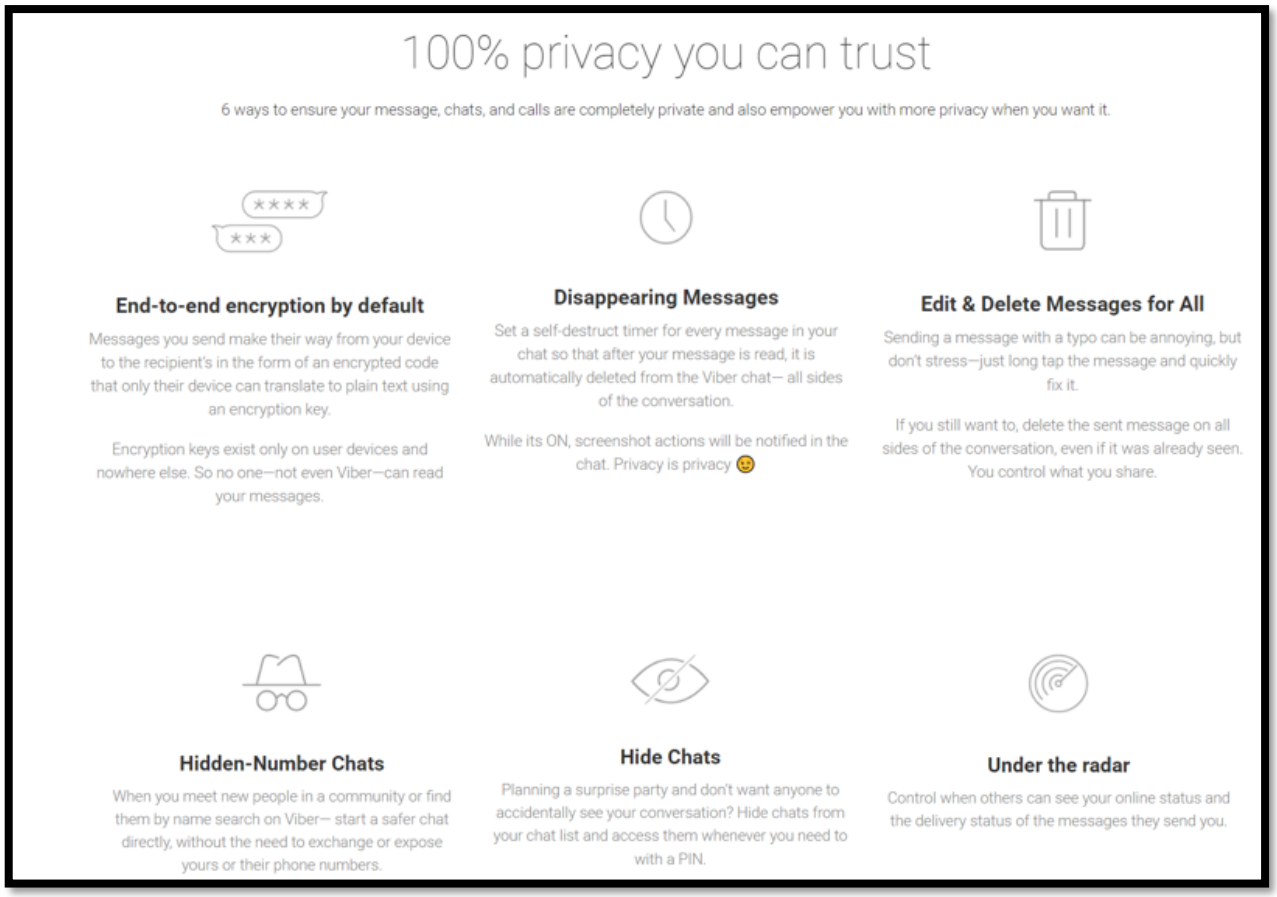


Figure 9 Viber advanced encryption

Facebook Case: Why not end-to-end encryption like Viber?

As discussed earlier, popular apps like Instagram, Facebook Messenger, Snapchat, and others have not implanted end-to-end encryption in their system. However, among the company or apps, facebook's case is taken to be discussed here. It was announced on April 3rd, 2021, that 533 million Facebook users' data had leaked. The data was leaked in a low-level hacking forum. The leaked data contained private messages between users, their phone numbers, emails, files, locations, etc. Facebook claimed that the leaked data happened through a vulnerability patched in 2019. (Ray, 2021) Now that the data has been leaked, cybercriminals can use the leaked data and impersonate legitimate users to perform scams, blackmail, and even sell the legitimate user's details to the highest bidder. If security features like end-to-end encryption are implemented, Facebook can reduce the chances of data leaks. Furthermore, the attackers cannot intervene between a sender and receiver; the files and chats exchanged between a sender and receiver will have reliable means of protection and will not leak in a low-level hacking forum.

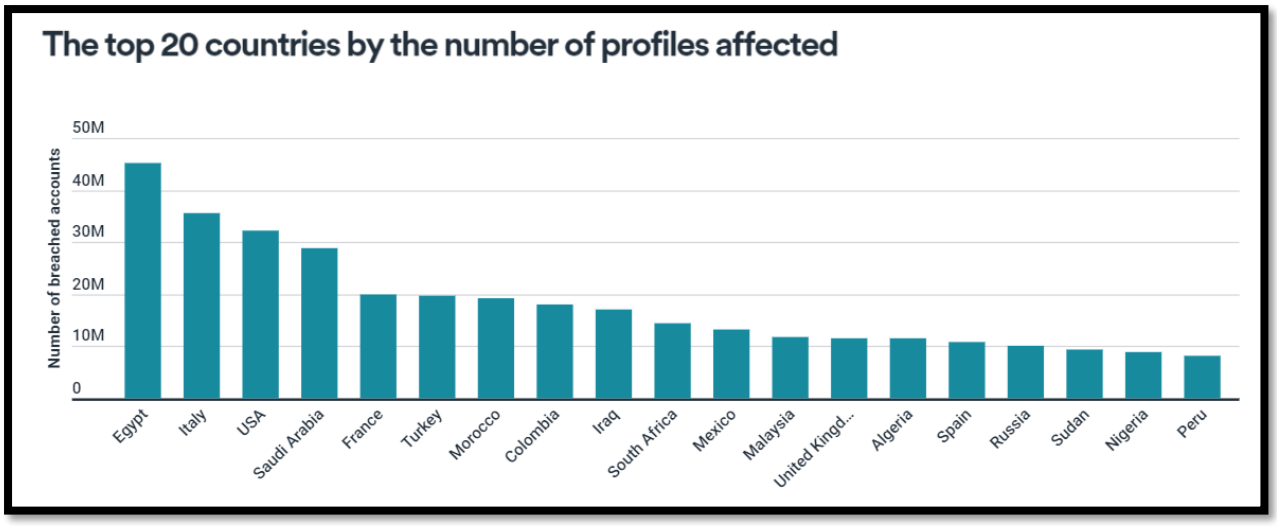


Figure 10 The Top 20 countries that suffered due to the data leak

In 2019 Facebook, now Meta, announced that they do not have any plan to implement end-to-end encryption until 2023. It is rumored that the reason behind this is for public safety. If Facebook implements the end-to-end encryption system, it will be difficult to track the criminal, unethical and illegal activities and so on done through the platform. So, Facebook wants to design and implement such a system that will not obstruct from detection of abuse. Moreover, the tech giant also wants to ensure that after implementing end-to-end encryption, it doesn't come in the way when investigating illegal activities. ["Facebook Messenger, Instagram chats will not get end-to-end encryption until 2023", 2021).

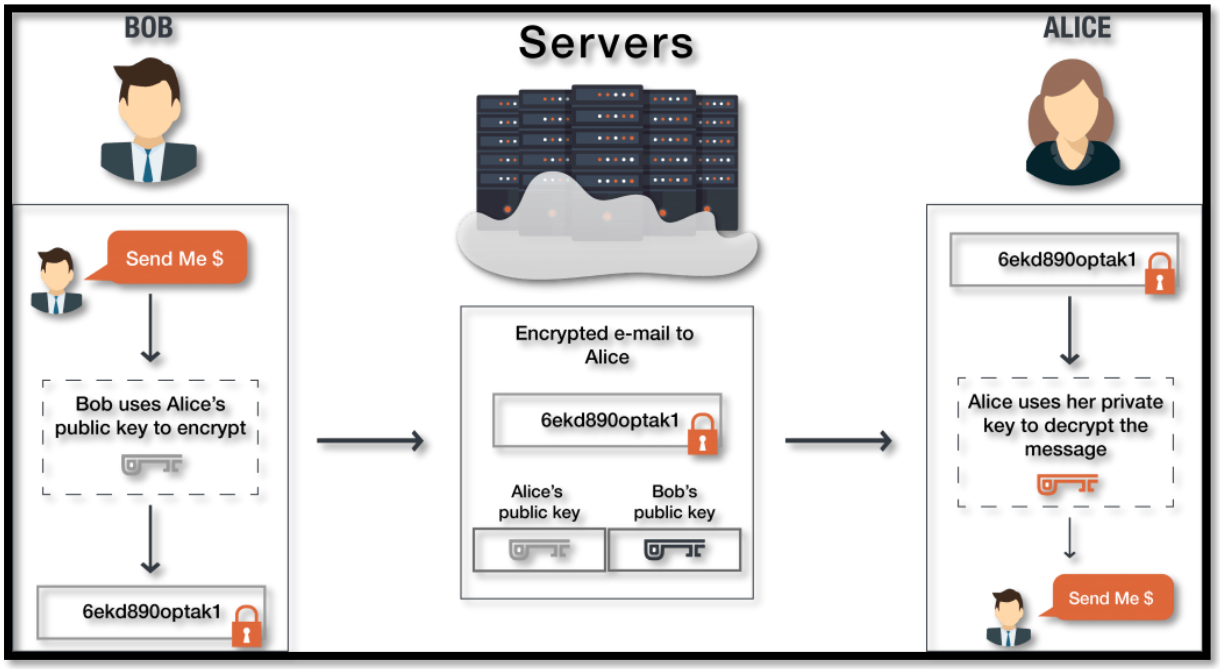


Figure 11 End- to- End encryption between a sender and a receiver

Methodology

Agile Model

All software or projects must go through certain phases to become a successful product. Each product has its requirement to be fulfilled, which needs to be analyzed when making or implementing a product. A client's requirements are only fulfilled, and a successful product can only be made by following a particular framework. Therefore, this project has used the agile model as the framework. Unlike the waterfall model, the agile model follows different approaches where large projects are broken down into smaller tasks, completed in a small-time interval, and delivered to the client. For example, suppose a company got a contract to make a messaging app by following the waterfall model. In that case, the final product is only delivered to the clients after one year or at a specific time. So, the app will not have the latest technology integrated, but with an agile model, the updates or a small product form are made and delivered weekly to clients. So that all client's needs are satisfied and they get the latest update available in the market integrated into their product until completion. Almost all company, military, universities, and others are shifting and adapting the agile model as it gets work done faster, fulfill clients' requirements, change project sections and optimize workflow. So, the agile model will be followed.

This project follows the Agile Software Development Life Cycle (SDLC) model. This life cycle organizes a series of phases a product experiences from beginning to end. Moreover, it mainly focuses on customer satisfaction, rapid delivery, rapid update, and process adaptation. The stages are concept, inception, iteration, release, maintenance, and retirement. (Wrike, 2022) The setting may vary depending on the agile methodology designed by the team. The life cycle that a product goes through are:

1. **Concept**

   In this phase, the product owner or stakeholders decide the scope of the product. Then, they will list certain things when making the product in a document and give them importance. After that, the product owner will discuss with the clients to outline the essential thing in the document, which means what features to add, what not to add, and so on. Moreover, keeping the requirements low will be advised so that unnecessary things in later stages could be removed. Detailed analysis of the client's needs will also be done to ensure the work can be done. After that, the time and cost also will be determined.

   So, by following the concept phase, the topic was researched in a detailed manner to make sure that this product could be made successfully, what features to add and what not to add were also determined, and time and cost were also estimated to make the product run successfully.

2. **Inception**

Once the concept phase is completed, a software development team will be assembled to work on the product. First, the best people who fulfill all criteria or skills required to make the product will be picked. Then, the necessary resources are allocated to them. The team then will create a prototype user interface and design the outline of the product. Client feedback will also be addressed if a change in a particular product section is required. Moreover, regular checks will be done on the product to fulfill all requirements.

So, first of all, this product was made by the author entirely, and a development team was not assembled. Following this phase, a structure or layout was designed for this product to work on them individually. Then, the author arranged the necessary resources like tools, books, and other things to work on the product officially.

3. **Iteration**

A working prototype product will be delivered to the client in this phase. A successful product completed after the first iteration will be delivered to the client. It is probably the most extended phase in the life cycle where developers combine all designs, product requirements, customer feedback, and features to turn them into code. Time after time or iteration after iteration, a new product version will be delivered to the client.

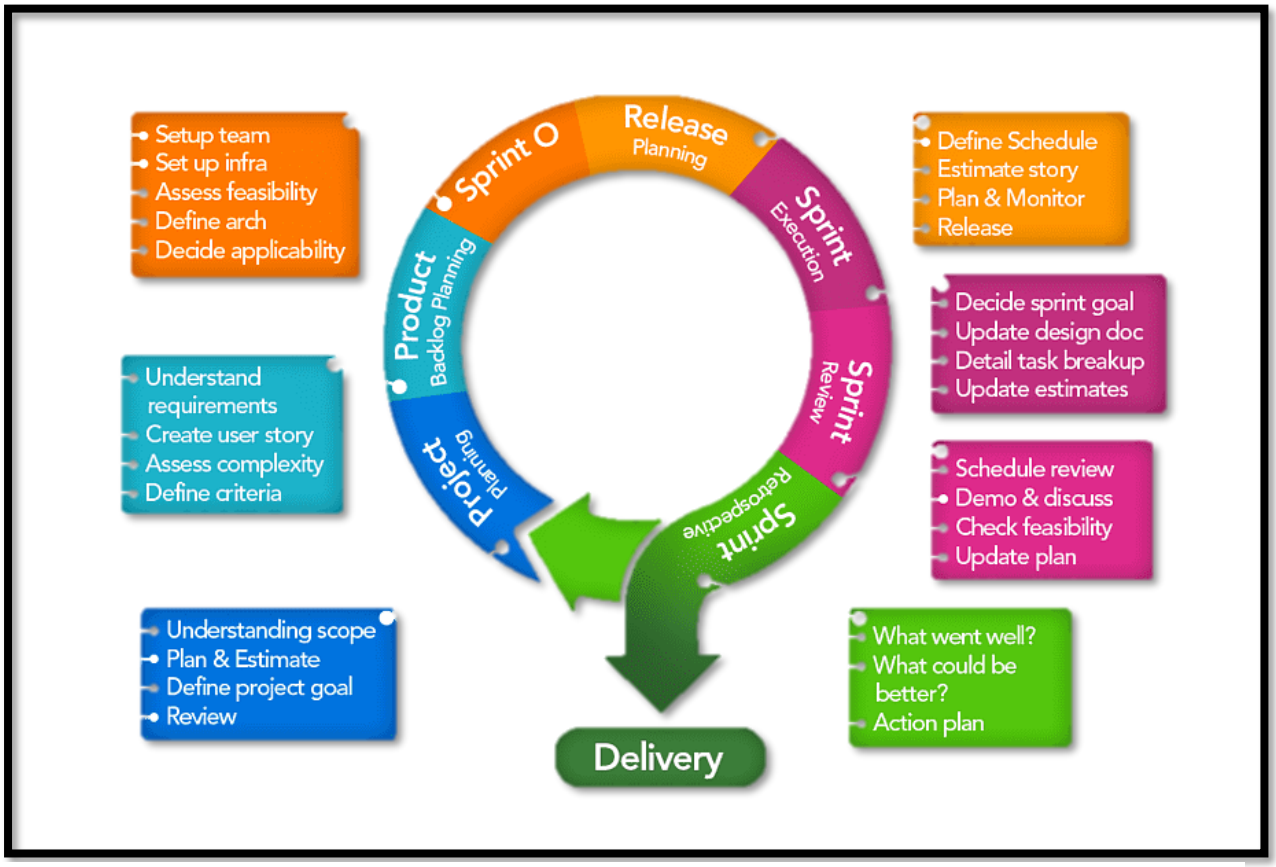


Figure 12 Agile iteration process

So, by following this phase, this product was tested just after completing a small section or functionality of the code to check whether or not the selection of the code could run successfully. Moreover, the product's initial design during the inception phase was turned into code.

4. **Release**

   After all, iteration is completed, the product will be made ready to be launched in the market. Before launching the product, different sections of the code will be re-checked to find if there are bugs and defects. After running the product and testing out all functionality provided, it will be determined whether the product is working successfully or not. Moreover, documentation will also be prepared on how to use the product.

   So, by following this phase, it was determined that the product was running successfully without bugs. Moreover, after all, iteration was completed, functionalities were also tested, which was found to be precise and accurate as it was intended when writing the code. A video on how to use this product is provided in the appendix section.

5. **Maintenance**

   After solving all errors in the product, it will be launched in the market. After launch, the product may face different cyber-attacks, so the product will be checked and upgraded to protect from the attacks. This work is done so that the product will continue existing in the market and run smoothly. From time to time, through new iterations, security features will be added. Non-technical users will be given a hand-to-hand demonstration on how to use this product in this phase.
   So, following this phase, if this product is launched in the market, it will be maintained from time to time and upgraded with new security features after every iteration. So, this product will continue to exist in the market.

6. **Retirement**

   When the product is not doing well on the market and generating low revenue, it is often replaced with another product providing the same functionality, or the product will be removed from the market permanently. Before doing so, the users will be notified that the product is retiring from the market. If there is a product replacement, users will be migrated to the new system.

So, following this phase, if this product is not doing well in the market, it will be replaced or removed altogether.

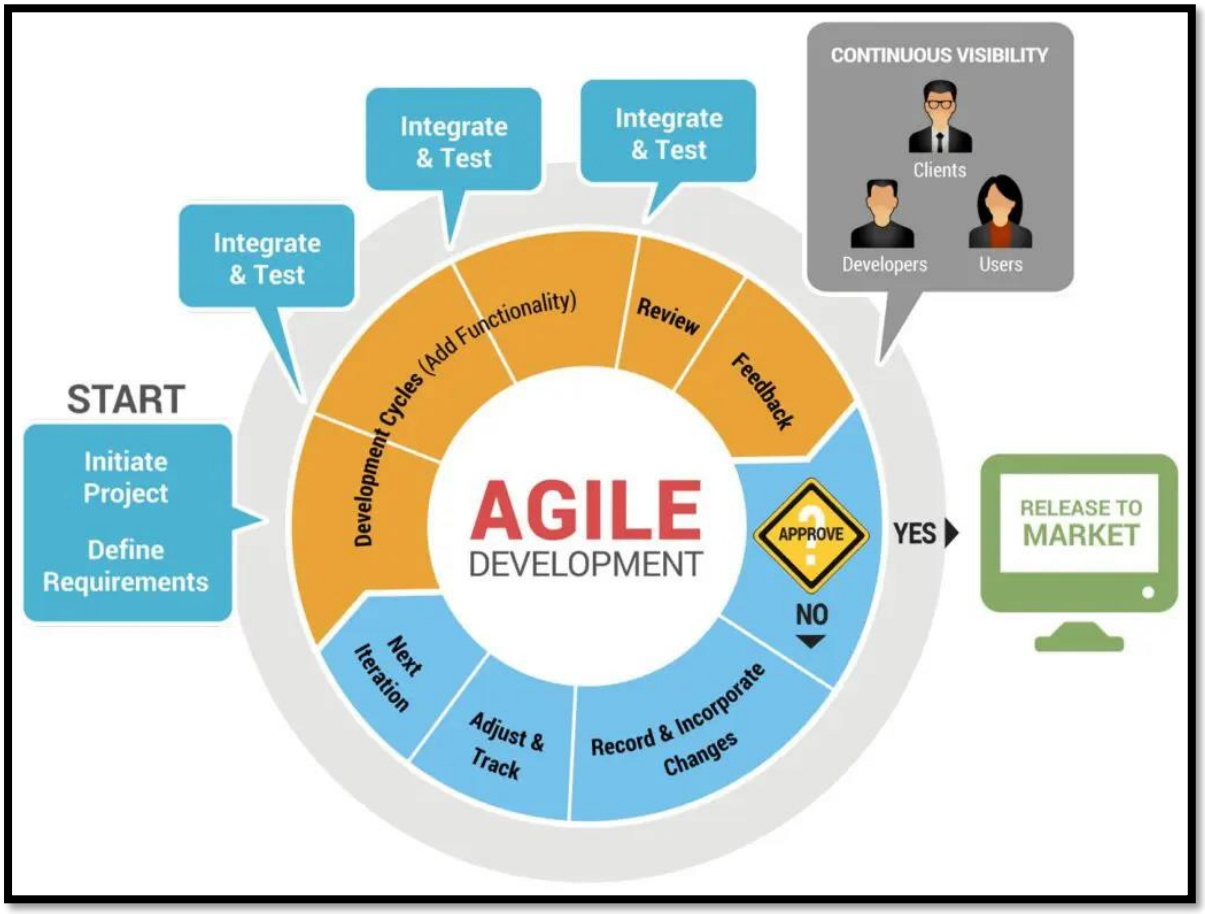


Figure 13 Agile development methodology

Tools and Technologies

These are the various tools and technologies used when creating this product.

Office 365

There are two versions of Microsoft Office 365 offline and online. The offline version is installed on the desktop and can be accessed through a web browser. In our case, an offline version of office 365 was used to write the document. Specifically, out-of-office 365 packages Microsoft Word, Microsoft Excel, and Microsoft PowerPoint were used. Through Microsoft word, tables, flowcharts, and on were made. This document, too, is written using the word. Through PowerPoint, certain graphics have been used. Moreover, when writing this document in word, Cambria font is chosen, justify is used, and line spacing of 1.15 is done in A4 size paper. For referencing CU, Harvard style is followed.

Python and PyCharm

PyCharm is one of Python's IDLE (Integrated Development and Learning Environment). Python is one of the most famous programming languages in the world through which we can develop websites and software, automate tasks, perform testing, analyze data, and do other things. So, this project is entirely programmed using python as it is easy to use and has been learned and implemented since our first semester. More specifically, python 3.9 (64-bit) is used and integrated into the PyCharm environment. PyCharm supports a wide range of tools and, according to our requirement, different encryption algorithms, the Tkinter module for GUI, and cryptography library modules like fernet, hashes, and PBKDF2 by importing them in PyCharm.

Tkinter

Usually, Tkinter is used to create a Graphical User Interface (GUI) for desktop applications. It is one of the modules which can be imported and utilized through PyCharm. Since this product is a desktop application and Tkinter is one of the famous packages it has been used.

Fernet (symmetric encryption)

Fernet is like symmetric encryption, where the same key is used to encrypt and decrypt a piece of data. However, after fernet encrypts the piece of data, it cannot be opened, modified, or manipulated. Fernet is used in this product to make it secure and free from manipulation. Moreover, fernet also provides one-way authentication.

Base64

The problem with a general encoding process is that the binary data or special characters might be lost during the encoding process. Nevertheless, with Base64 encoding, we can convert binary data or special characters into base64 plain text string, which can then be sent over the communication line. After it reaches its destination, that string can be decoded using the base64 decoder. So, the base64 ensures that no data is lost, and the receiver can get the exact data without changes that the sender sends in the first place. Base64 is used in this project to encode the generated key.

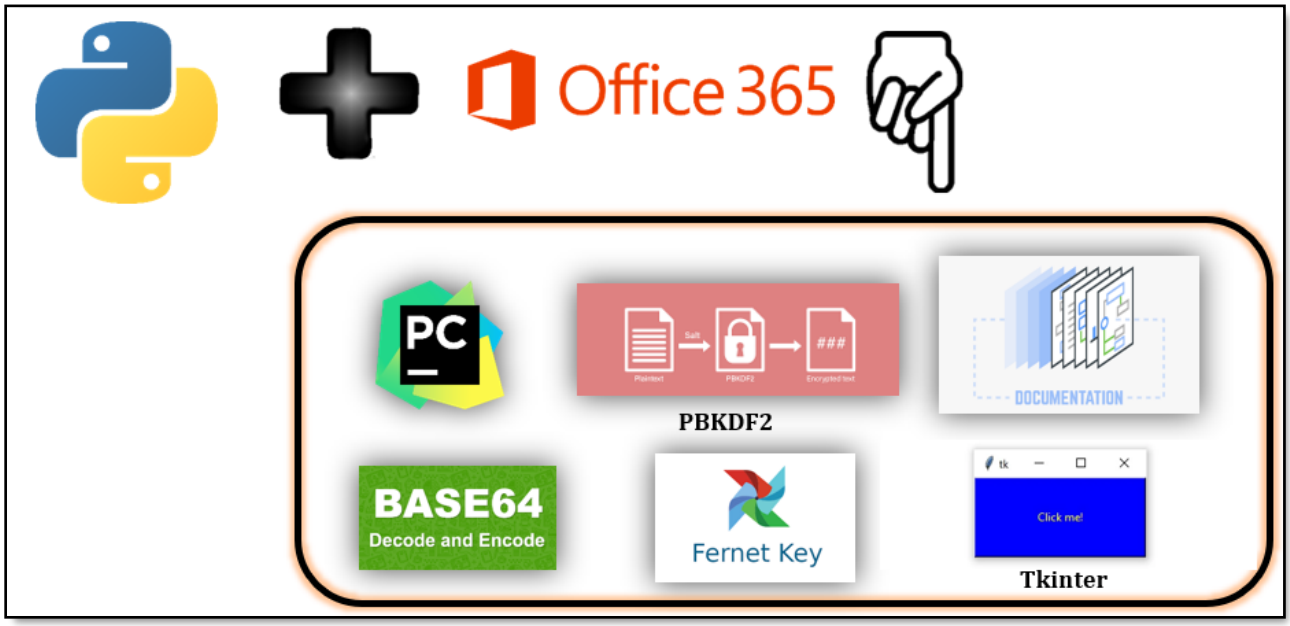


Figure 14 Tools and Technologies

Techniques

All the techniques used when creating this product have been discussed here. In addition, multiple techniques that have been used are listed below.

Hashing

When it comes to storing the password and safeguarding it, we use hashing. In the hashing process, we generally take a piece of data or plain text and use different hashing algorithms like MD5, SHA256, and so on to convert the plain text to an unreadable hash value. This generated hash value contains a password but in an unreadable format. If only a slight change in the plain text is made, we will get a different hash value. Moreover, in the encryption process, we can encrypt a piece of data and later decrypt it using the key to get the original data. However, it is irreversible in the case of hashing, and we cannot get the actual data from the generated hash value.

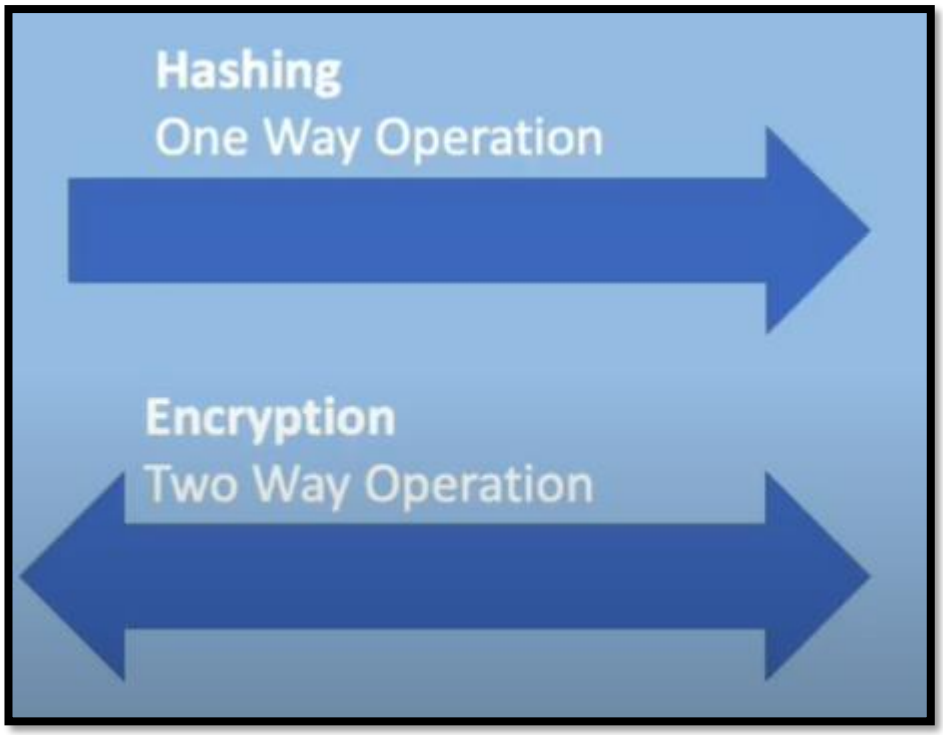


Figure 15 Hashing

Nevertheless, hashing has several vulnerabilities that can be used to get the original data from the generated hash value. One vulnerability is brute force attack. For example, if a password is hashed and stored in a database, the attackers can try millions and billions of combinations of passwords until they get the one that matches the hash stored in the database. It can be done using tools like hashcat or other online tools. Another vulnerability is the dictionary attack. For example, the attacker makes or downloads a huge pre-computed dictionary containing password and their hashes and matches the hashed password from the dictionary with the one stored in the database until they get the one.

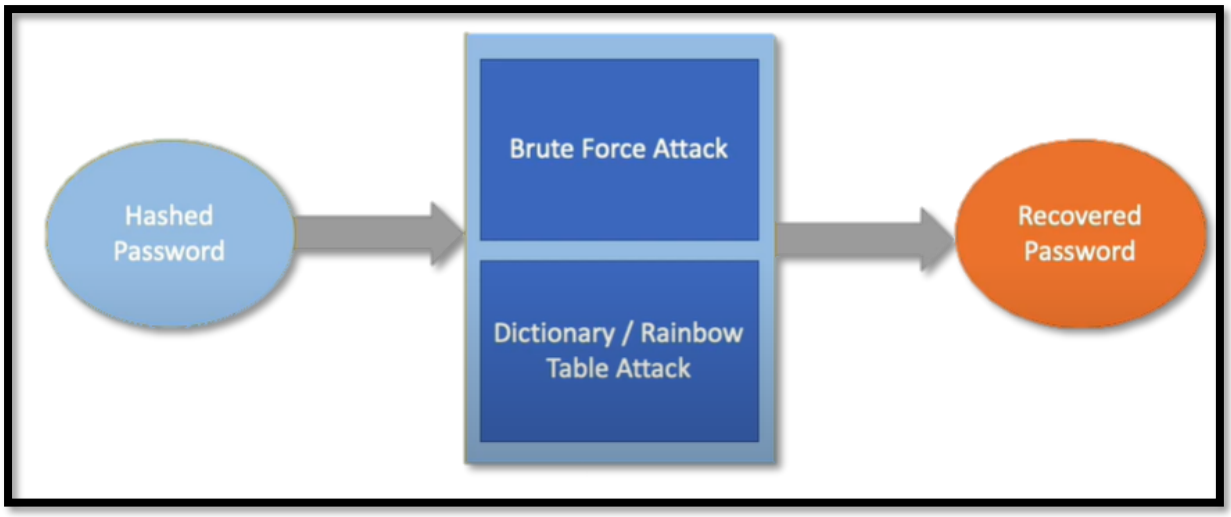


Figure 16 Brute force and dictionary attack on the hashed password.

Salting

A common way to mitigate against brute force and dictionary attacks is by adding salt to the password. It means you take a piece of random data called salt and append it to the password. After this, the password is hashed. This method provides more security, and the attacks have much more difficulty cracking the password. Moreover, the user needs to store the hashed password and salt in the database as they need the same salt to be able to hash the same password. (Triveni, 2021)

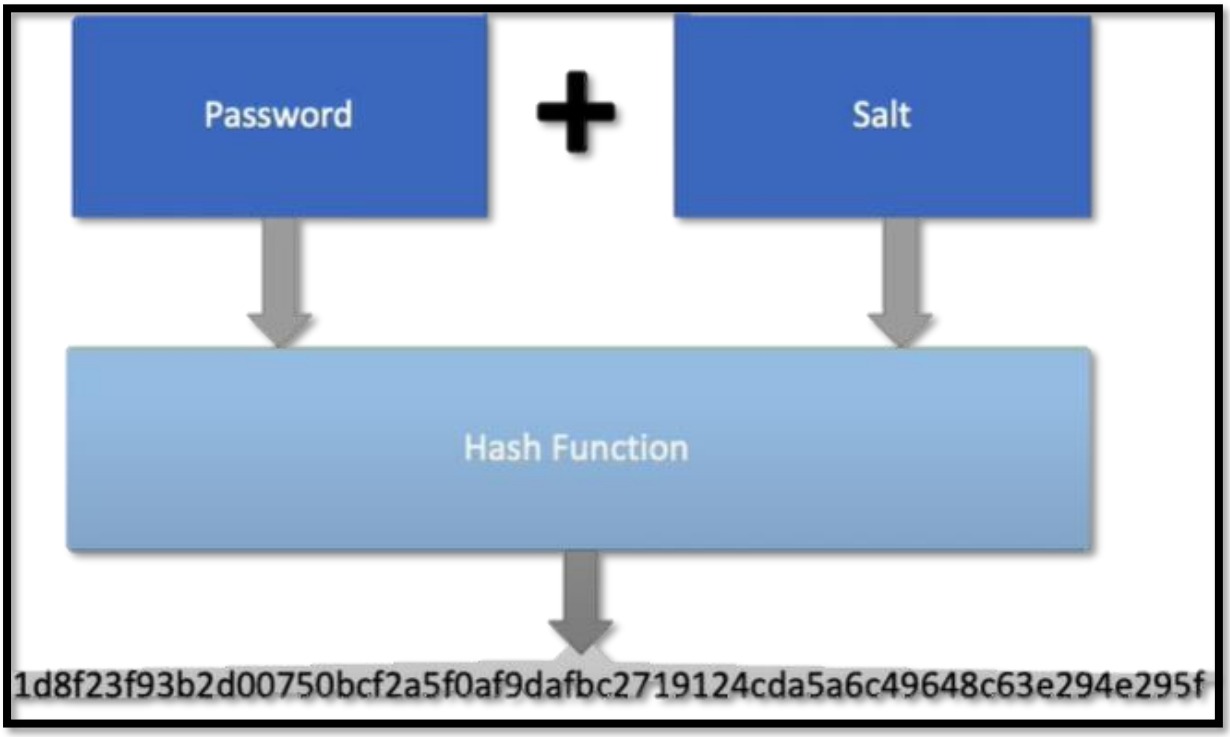


Figure 17 Adding salt to your password to make it more secure

Password-Based Key Derivation Function (PBKDF2)

However, the problem here is that with Moore's law and the CPUs and GPUs getting faster each day, the salt and password combination might be cracked in 5years. Nevertheless, it is safe for now. So, to solve this, we have a new technique called Password-Based Key Derivation Function (PBKDF2). (Cryptosense, 2015).

It is the new generation of password hashing used when making the product. PBKDF2 is not complicated. For example, A salt is appended to your password, and that password is hashed based on the number of iterations provided. If the user passes 20 as the number of iterations value, the password will be hashed 20 times. Furthermore, if the user passes in 10000 as the number of iteration values, the password will be hashed 10 thousand times. This new technique provides unbreakable security against brute force and dictionary attacks.

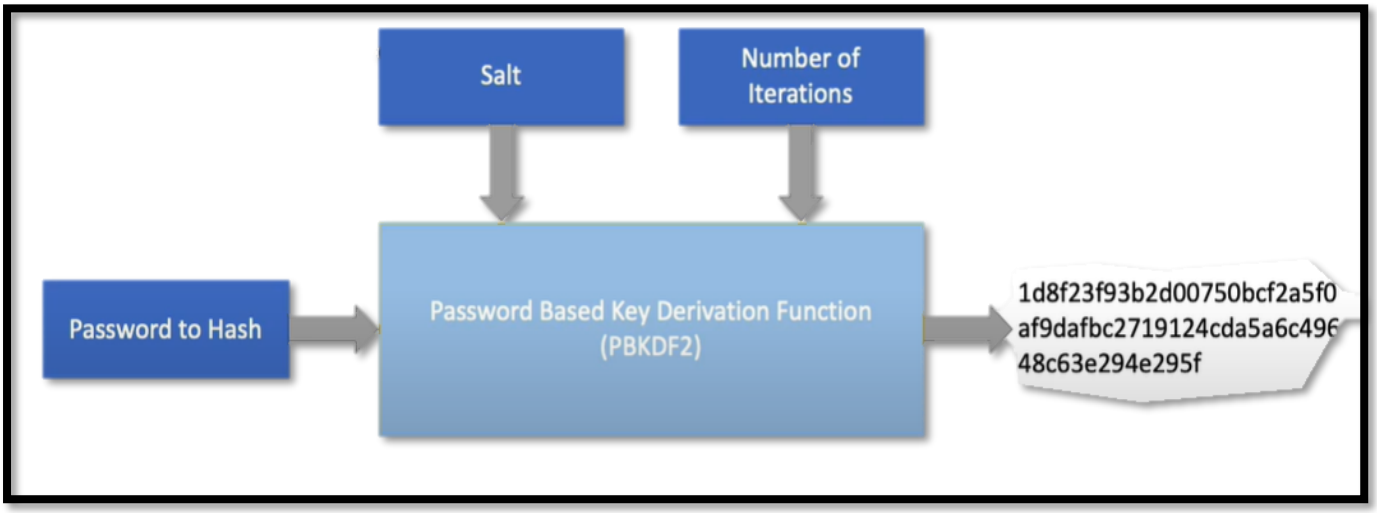


Figure 18 Password-Based Key Derivation Function (PBKDF2) iterations

Integration

(There are four research questions. The First and Second research questions answer is in this section.)

This section discusses how the tools, technologies, and techniques are integrated into the product. For a detailed and clear explanation, an activity diagram of the project is provided below, which we will discuss.

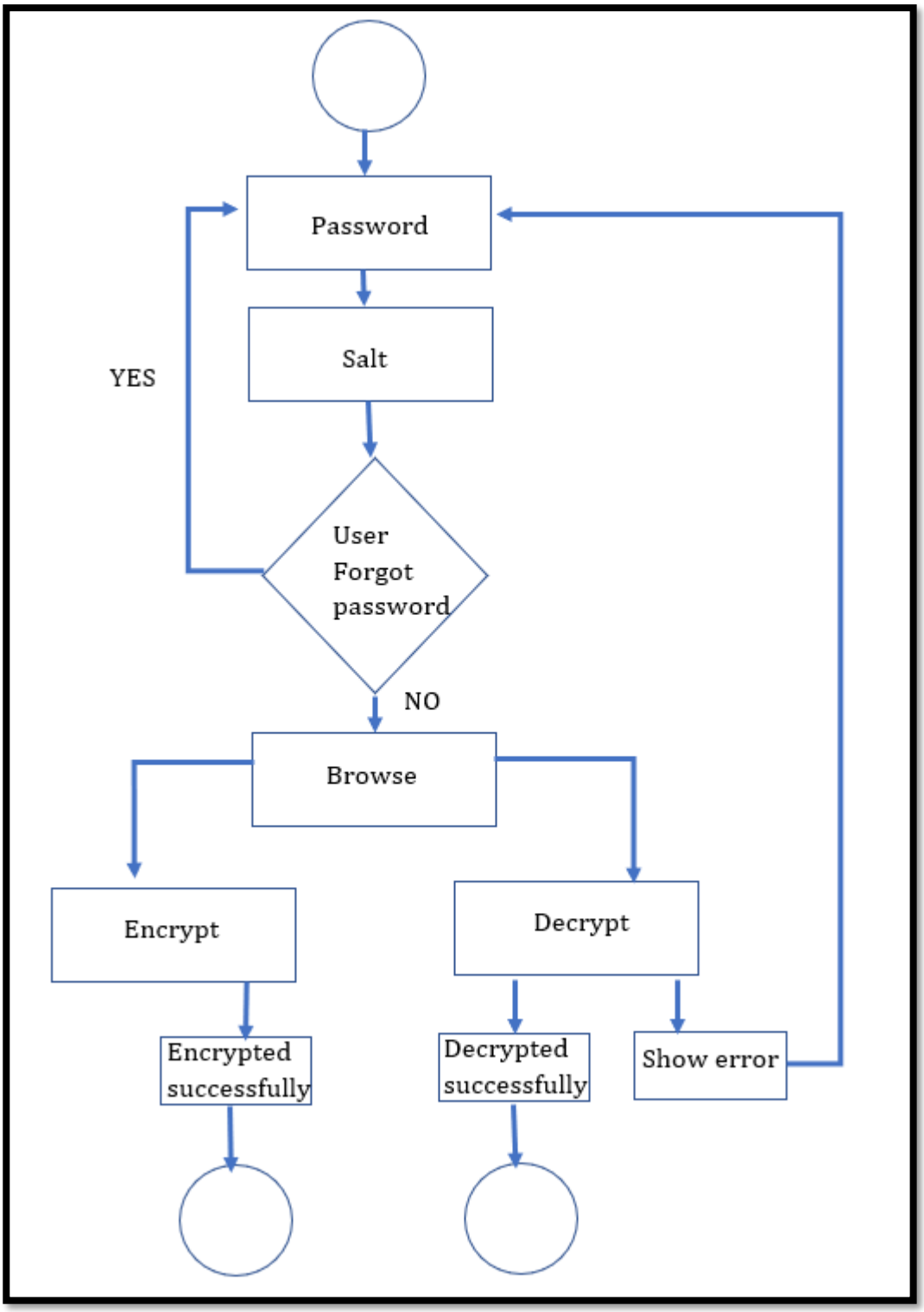


Figure 19 Basic activity diagram of the product

In the encryption phase, first of all, the user views a file or folder to which they want to provide security. After that, a password and salt of their choice is provided in the GUI of the product. If the password is only hashed, then it is prone to brute force and dictionary attacks. So, a salt is added to the password to enhance the security feature of the product further. The password and salt are hidden behind asterisks for security purposes, so users may sometimes forget their set passwords and salt. So, if they forget, they need to start again by giving the password and salt in the GUI app. The salted password is hashed using the Password-Based Key Derivation Function (PBKDF2), setting the number of iterations to 100000. This means the password will be hashed 100 thousand times. Moreover, users can browse files or folders to protect them if there are no mistakes. The user can also select multiple files at a time and a folder to lock them.

Through fernet, the hashed password and salt are used as a medium to generate a key. The selected files or folders are locked and encrypted using the key. Fernet is used, so no amount of manipulation can be done to files and folders. If a third person other than the legitimate user tries to open the file, it will not even open. Moreover, even the thumbnail of that file will be locked and cannot be seen by the third person. Through the base64 encoder, the generated key will be encoded. Moreover, if the legitimate user wants to access the files (In the decryption phase), first of all, the password and salt should be provided in the GUI of the product. After the password and salt match with the legitimate source, the same key generated earlier will decrypt the file, and we can finally access that file.

Interaction of legitimate user and attacker with the product (layman's terms)

This section is written using Use Case Diagram as a reference. This section includes things that the product must do, how a user can interact with the GUI of the product, what the product cannot do, how actors such as legitimate users and attackers interact with the system, and so on. Moreover, this section provides a simplified version of how this product works so that even lay people or non-technical personal can understand the product. Here, the legitimate user is the person who sets a password to a file, and the attacker represents the third person with access to a legitimate user's PC. So, we will see the legitimate user interaction with the product and the attacker interaction on what they can access and what they cannot from their view.

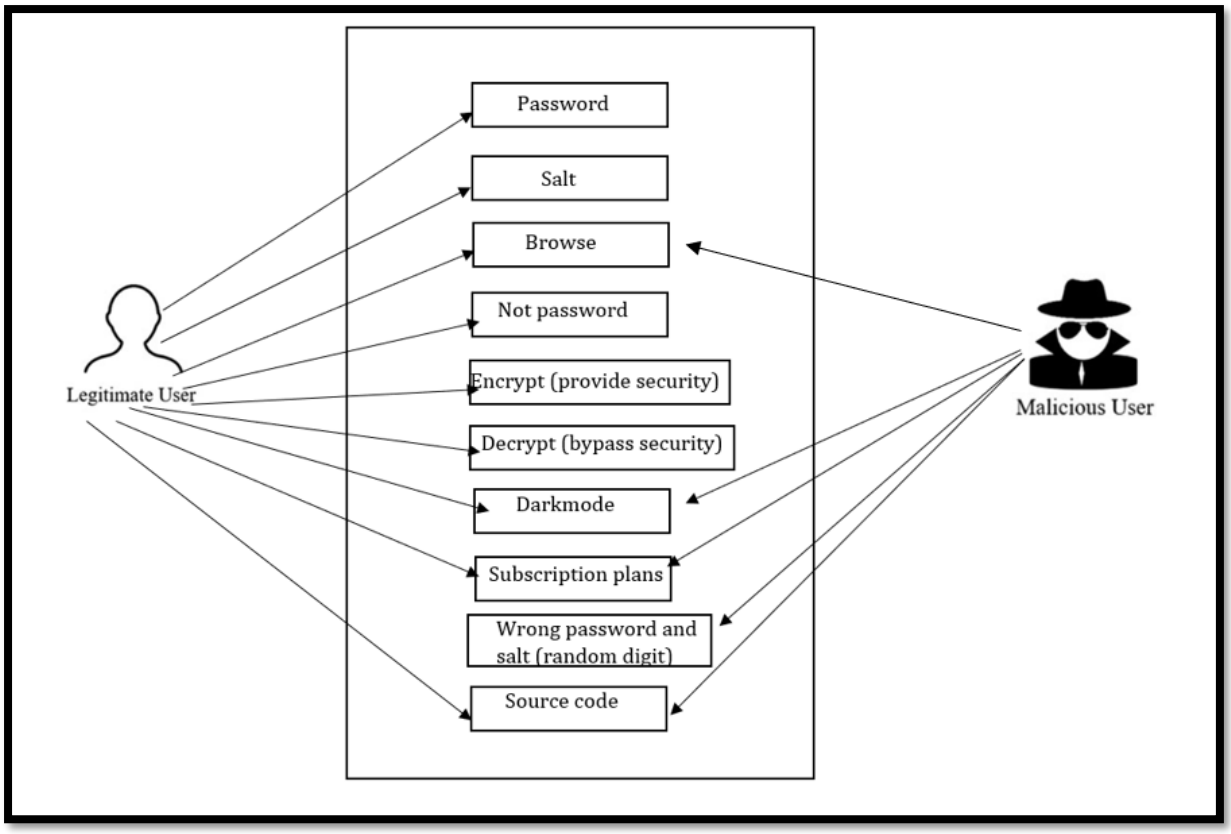


Figure 20 Interaction of user and the attacker with the product

Table 1: Interaction with password and salt

Name:	Password and salt (random digit)
Actors:	Legitimate user
How is it used? • The password and salt are provided by the legitimate user, and the attacker cannot have access to it. • If the legitimate user provides only salt but not the password in the product, then it will show an error telling the user to provide the password. • If the attacker tries to access the files locked by the legitimate user by entering a random password and salt, then they can't get access, and an error box will be shown.	
What can it do? • Files are provided security with a password. Salt means adding random digits like 1234 in the password. • So, salt is added to the password to provide more security and be safe from hacking attacks.	
Drawback	

• With each passing day, new forms of technology have been developing all around the world. • Password and salt might not be secure in the coming future, and the attackers can have access to your files.

Table 2: Interaction with browse

Name:	Browse
Actors:	Legitimate user, the attacker
How is it used? • Users can browse files and folders from their PC to lock it by providing a password and salt of their choice. • Multiple files and a folder can be browsed and selected at a time to provide security. • Attackers can browse the files and folders using the product but cannot get access to them as security is provided to them.	
What can it do? • The browse option is added to the product to select and lock files and folders from their PC according to user choice.	
Drawback	
• Attackers can also have access to the browse feature.	

Table 3: Interaction with encrypt and decrypt

Name:	Encrypt (provide security) and Decrypt (bypass security)
Actors:	Legitimate user
How is it used? • After the user selects the password and salt of their choice for files, they have to select encrypt to lock the files to make them appropriately protected. • If the user wants to get the file contents, they have to select decrypt after providing the password and salt. • Attackers cannot encrypt and decrypt.	
What can it do? • By encrypting the files, we are password-protecting them. This means a password and salt are required to open it. • By selecting Decrypt, we can have access to files.	
Drawback	

• To provide security to the files, symmetric encryption is used. Asymmetric encryption = High security Symmetric encryption= Low security compared to Asymmetric encryption

Table 4: Interaction with Darkmode

Name:	Darkmode
Actors:	Legitimate user, the attacker
How is it used? • Turn on and Turn off the dark mode feature available in the product. • Both the attacker and the user can turn off and on the dark mode feature according to their preferences.	
What can it do? • Turning on dark mode is helpful for your eyes, especially at night time. • Turning on the dark mode can reduce blue light exposure and help to prevent eye strain and headaches. • Dark mode means changing the white background into a dark background.	
Drawback • White background enables a more accurate view of text and interfaces as compared to the black background in our case.	

Table 5: Interaction with subscription plans (for future)

Name:	Subscription plans (For future)
Actors:	Legitimate user, the attacker
How is it used? • The subscription plans section is included in the menu bar. The user and the attacker can view it.	
What can it do? • Subscription plans do not have any functionality. • This product is only a prototype, and the subscription plans are made for future purposes when it will be full-fledged or ready for market. • It is included in the menu bar section for marketing purposes.	

Table 6: Interaction with Source Code

Name:	Source Code
Actors:	Legitimate user, the attacker
How is it used? • It is included in the menu bar where the GitHub link to that source code is provided. • Both the attacker and users can view it as the code as the source code is made public.	
What can it do? • With source code, we can run this product and see its interface. • The source code is free from bugs and viruses. • If the attacker steals the source code and uses it for their personal benefit, then they will be subjected to Article 44 of the Electronic Transactions Act (ETA), related to Pirate, Destroy or Alter computer source code.	
Drawback • The only drawback is that in later dates, the product will be changed to closed-source software, by which many vulnerabilities and bugs may arise.	

The interface of the product- How does this product work? (Final results)

In this section, this product's GUI screenshots will be taken, and these screenshots will be described in detail for readers who want to know more about the product. In addition, the screenshots will contain a different section of the product so that reader can visualize the GUI and understand more about how this product functionality works. So, a simple demonstration will also be given.

Main Interface

As can be seen, there are two different sections after opening the product: the Files section and the Folder section. Using the files section, the user can select multiple files at a time and encrypt them. Using the folder section, the user can choose to encrypt only one folder at a time. There are other sections, too, which will be discussed individually.

The files and folder are encrypted and decrypted in the same way, and common steps are followed. The only difference is that when selecting files, multiple files can be chosen at a time, but only one folder can be chosen at a time to encrypt and decrypt.

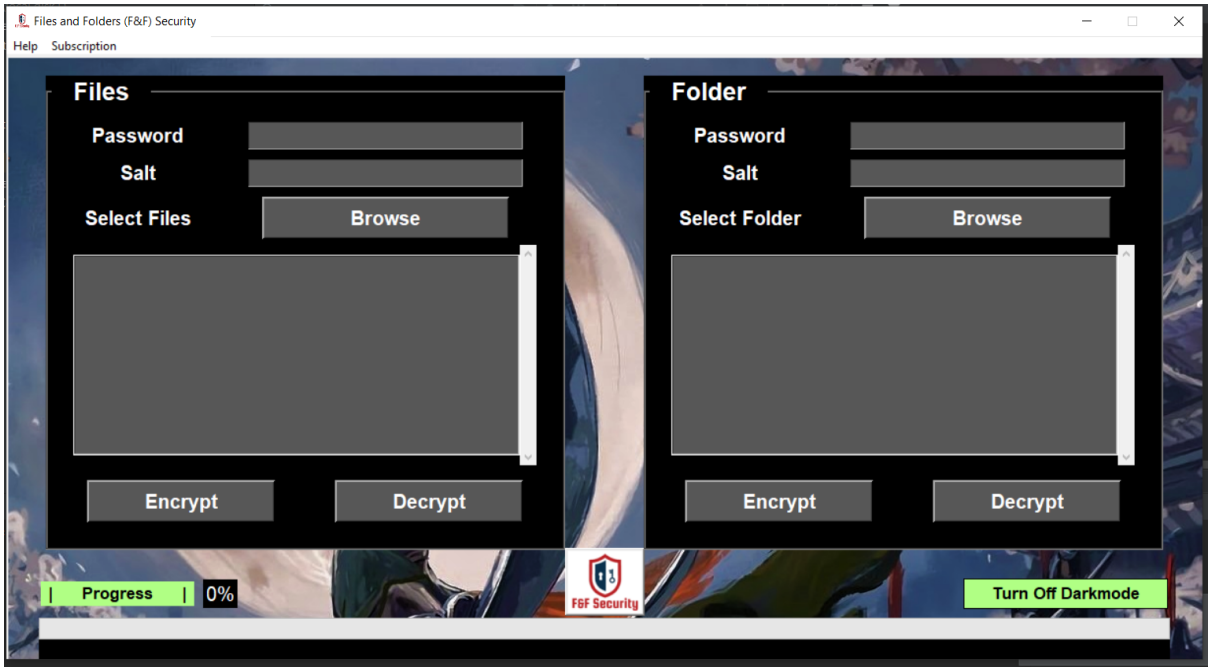


Figure 21 Main Interface

So, the functionalities and how this product works will be explained through these steps:

Files encryption and decryption

Step 1: No login is required when using the product, and the user can directly enter the password and salt of their choice after opening the product. The password and salt are hidden behind asterisks for security purposes.

Step 2: After placing the password and salt, another thing to do is select a file or a bunch of files the user wants to encrypt. In this case, the user has selected six files to encrypt.

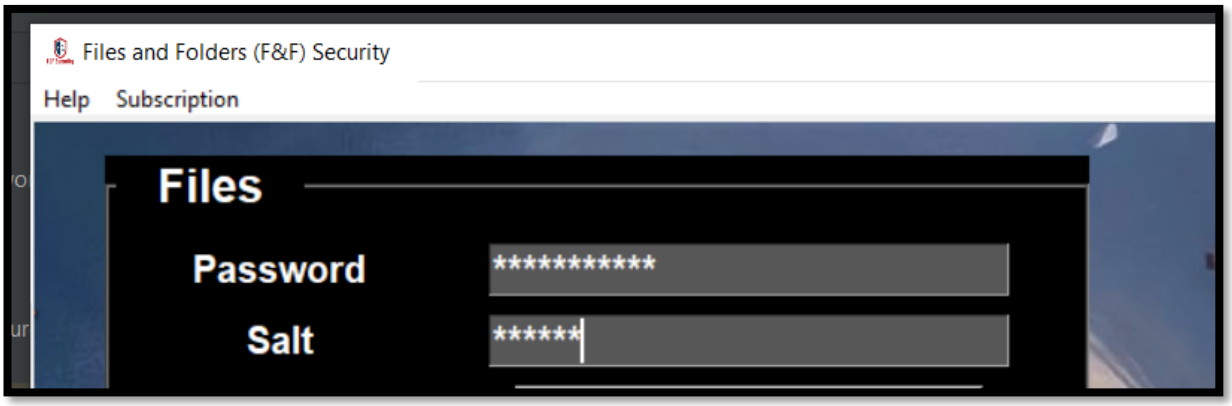


Figure 22 Entering password and salt

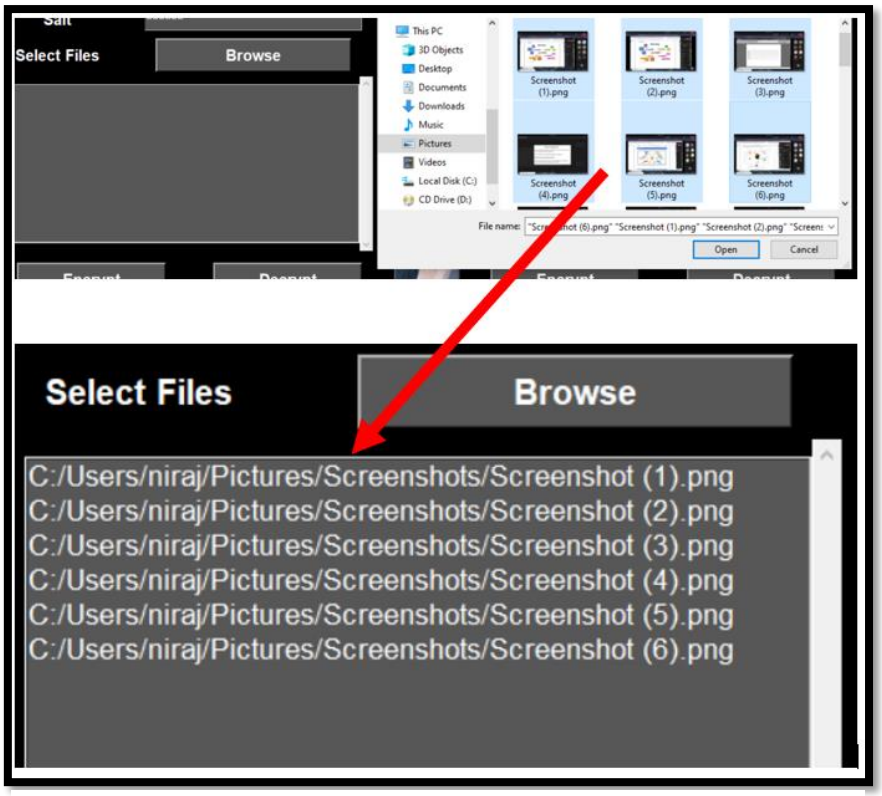


Figure 23 Browsing for files

Step 3: All files will be encrypted simultaneously after the user hits enter. If another person other than the user wants access to the encrypted files, they cannot open the file. In this demonstration, an image file is taken and encrypted. Image files and files in different formats such as pdf, docx, mp3, mp4, and other file formats can also be encrypted. The files, after being encrypted, can also be sent to other parties through email or message; in between, no other third party can view it without a password and a salt.

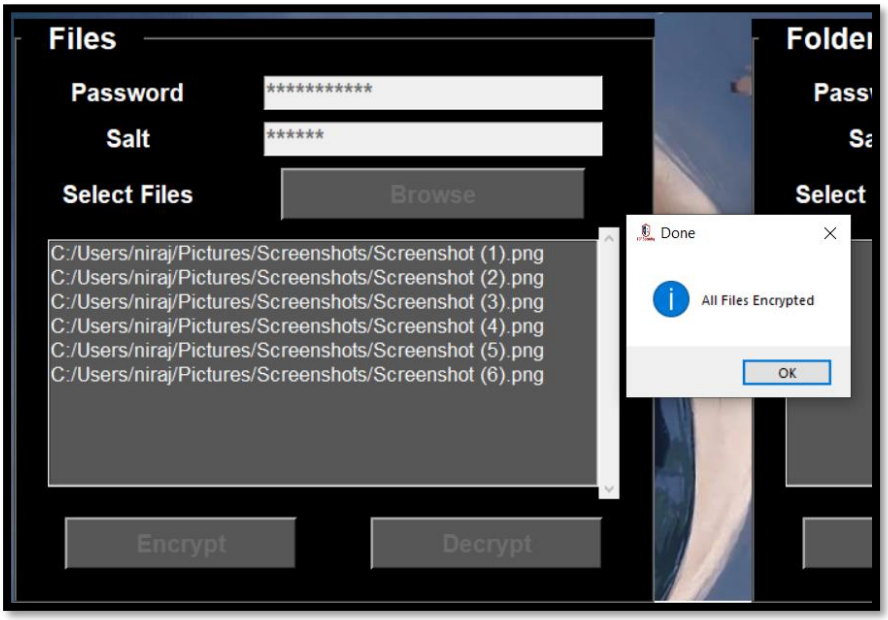


Figure 24 Files encrypted successfully

After encrypting, the file cannot be opened without a password and salt. In this demo, the user had previously encrypted from files one to six. So, even the thumbnails of files one to six are not showing. This way, the product provides security.

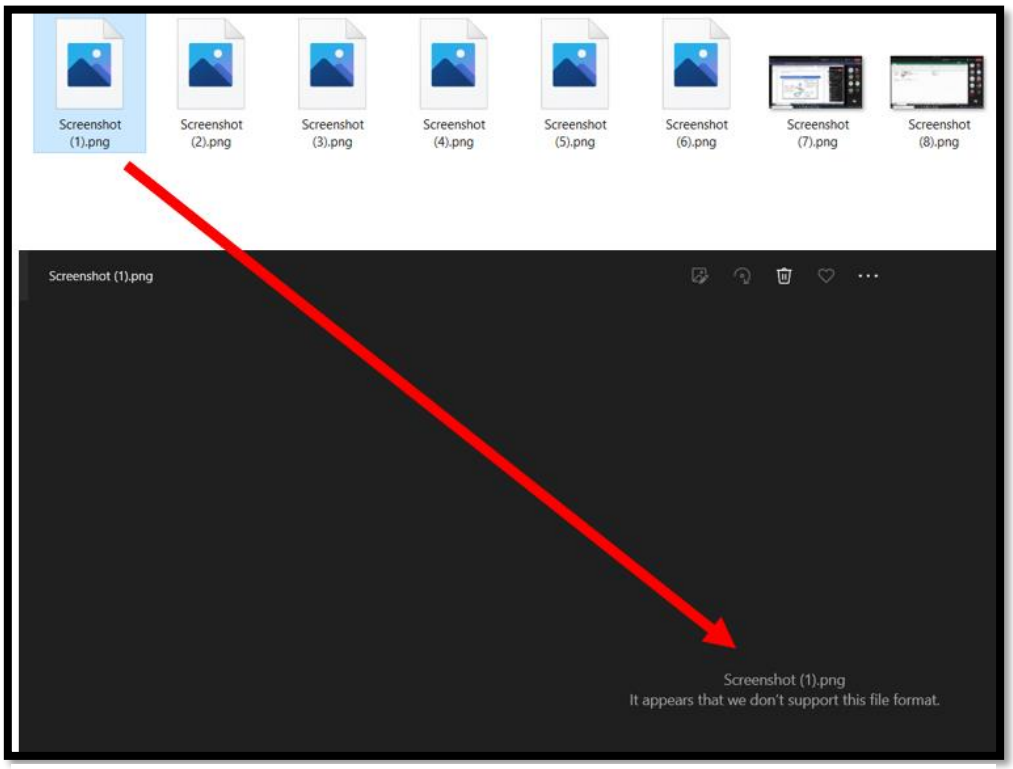


Figure 25 Files not accessible anymore

Step 4: If the user wants to decrypt the files, they need to enter the password and salt they previously used when encrypting them, as shown in the first picture. As shown in the second picture, the user selects files they once encrypted to decrypt them. After providing the correct password and salt, the files are decrypted successfully. Moreover, like in the third picture, the user can now view the file content, and the thumbnail is not hidden like previously.

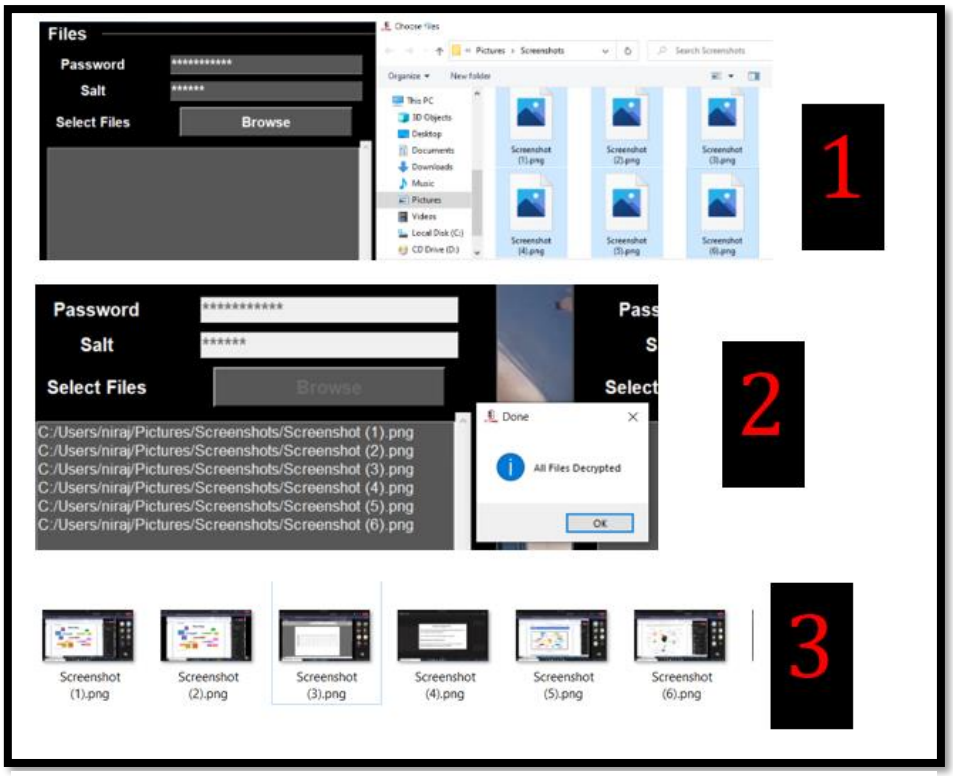


Figure 26 Files decryption process

Folder encryption and decryption

From steps, one to four, file encryption and decryption demonstration is provided. The folder encryption process also follows the same steps as file encryption. When selecting files from the files section, only files can be selected, and no folder can be selected. Moreover, only folders can be selected, encrypted, or decrypted from the folder section. Unlike the files section from the folder section, only one folder can be selected at a time to encrypt or decrypt. A simple demonstration is provided here. The user first enters the password and salt of their choice. Then, they choose a folder that they want to encrypt. In this case, the user has selected a folder containing a pdf and a video file. After the encryption is successful, the pdf and video files cannot be opened, as shown in the third picture, through which others cannot access the user's private files and folder. However, they can be sent to others through email or messaging platforms by maintaining security. If the user wants to see the file contents, they will provide the password and salt, and the content will be decrypted.

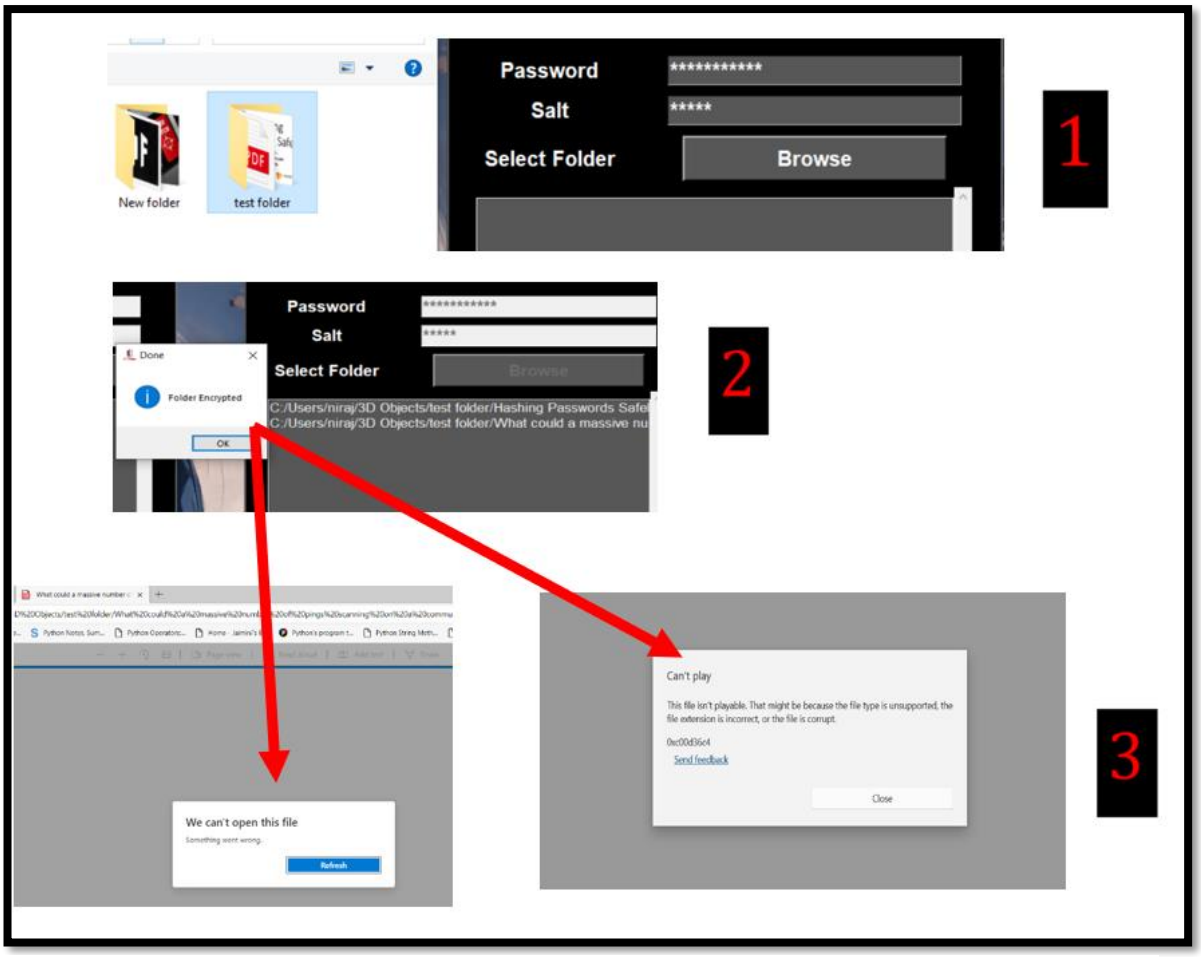


Figure 27 Folder encryption and decryption process (Just like files process)

Progress bar and Dark mode GUI

Progress bar

A progress bar widget has its advantages. First, it shows the progress of a long-running task. For example: if a user uploads 100 files at a time in the product to encrypt and if the progress bar was not integrated into the product, then the user cannot get the exact time the files will be encrypted and then cannot be sure if all files are encrypted or not. With a progress bar, the progress goes from 0% to 100% after putting a file or a folder in the product so the user can watch the whole process and ensure the files are encrypted successfully.

So, in short, they will know that something is happening after their click, and they need to wait in response to get the result.

Figure 28 Progress bar

Dark mode

Users can turn on and turn off dark mode in the product according to their choice. However, it is recommended to use dark mode, especially at night, as it is helpful for the eyes. Moreover, turning on the dark mode can reduce blue light exposure and help to prevent eye strain and headaches. (Healthline, 2021).

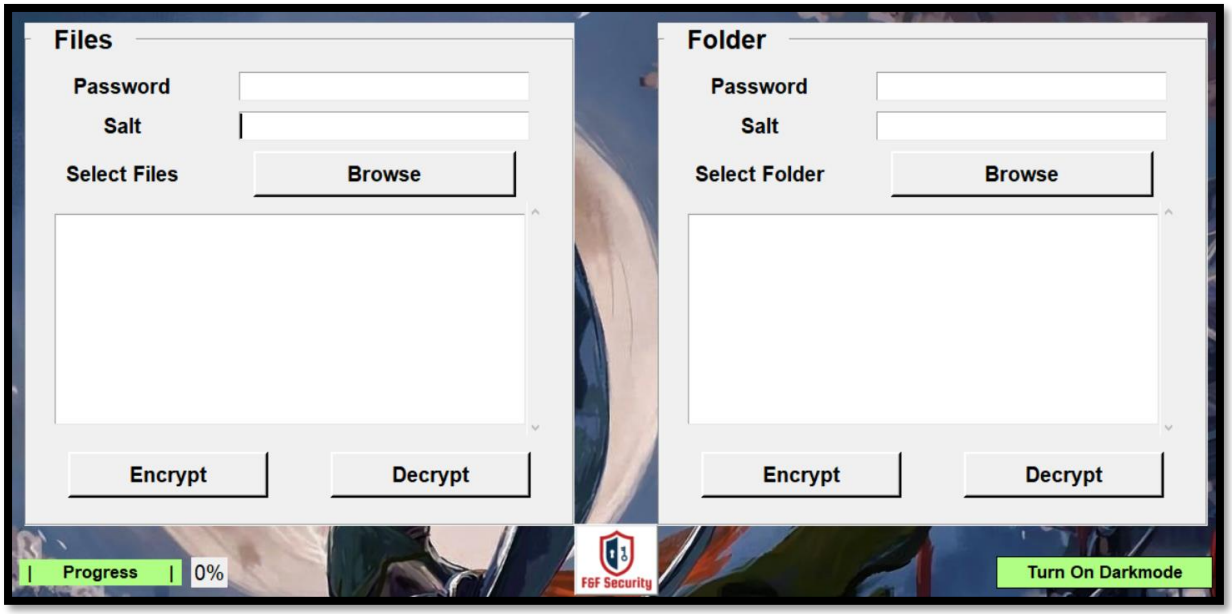


Figure 29 Dark mode off

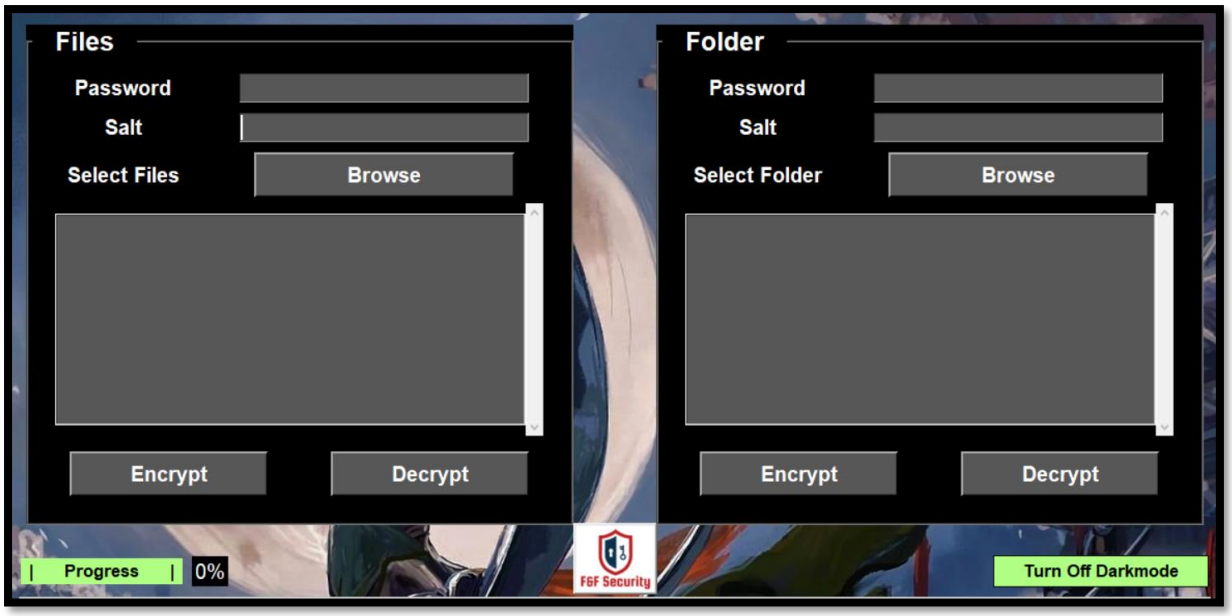


Figure 30 Dark mode on

PESTEL Analysis

Marketers or a company do PESTEL analysis before launching their product in the market. It helps to form a strategic plan that benefits the product. Moreover, PESTEL stands for PESTEL stands for political, economic, social, technological, environmental, and legal factors. So, PESTEL is generally done to know how these factors affect the product launch and how the product affects the aspects. However, it is not done regularly and only after a certain period as the factors keep changing. (Oxford, 2021).

Figure 31 PESTEL analysis

The different aspects are explained below:

Political Aspect

The product is free from any political viewpoint and is not affiliated with a political party or made for a political party. All users are equal and will be treated equally in the future whenever they use this product. Moreover, all user's viewpoints will be noted equally, and necessary upgrades and updates will be installed in the product in the future to enhance the development.

Economic Aspect

The product is only a prototype and is not full-fledged. Revenue from the product will be generated with the subscription-based model in the future. So, the product is created having commercial viewpoints in mind. Although much work is needed to be done to make this product market ready, after the work is completed, it will positively affect the company's financial statements. Since this product is scalable and simple, a basic structure is followed, so the maintenance price will be significantly reduced in the future.

Social Aspect

This product falls under the private security sector. So, with this product, people can provide security to their confidential files and folders and save from any manipulation from hackers. So, this product will enhance the private security of people, and their quality of life will also be improved.

Technological Aspect

This product is easy to use, and prior knowledge of technical things is not required. Moreover, with this product, people will have security in their private files to protect them from any ransomware attacks. This way, people in Nepal will use other security products, leading to modern life and technological development in Nepal. Moreover, the product size is not large and can be easily installed on windows OS.

Environmental Aspect

Electronic Hardware components contain mercury, lead, and lithium, if improperly disposed of, can harm the environment. However, since this product does not have any hardware components and is software-based, so this product does not harm the environment.

Legal Aspect

The product is protected from Article 44 of (the Electronic Transactions Act (ETA), related to Pirate, Destroy, or Alter computer source code. So, if people or a company steals, pirate, destroys, or modifies this product's source code, they will be subjected to this act with a punishment of 3 years in prison or two hundred thousand Nepalese rupees or with both. This product, too, will follow GDPR (General Data Protection Regulation) and will not violate other people's privacy; otherwise, we will be subjected to this act.

GANTT Chart

Tasks	Start date	End date	Duration
Project Proposal	5/29/2022	6/1/2022	3
Framework and design	6/2/2022	6/5/2022	3
Initial coding	6/6/2022	6/29/2022	23
Algorithm	6/30/2022	7/3/2022	3
Interface	7/5/2022	7/12/2022	7
Integration	7/15/2022	7/21/2022	6
Testing	7/22/2022	7/24/2022	2
Final coding	7/25/2022	7/29/2022	4
Literature review research	7/30/2022	8/1/2022	2
Documentation	8/2/2022	8/13/2022	11
Infographics	8/14/2022	8/15/2022	1
Future work	8/16/2022	8/17/2022	1
Final documentation	8/18/2022	8/20/2022	2

Figure 32 Gantt Chart

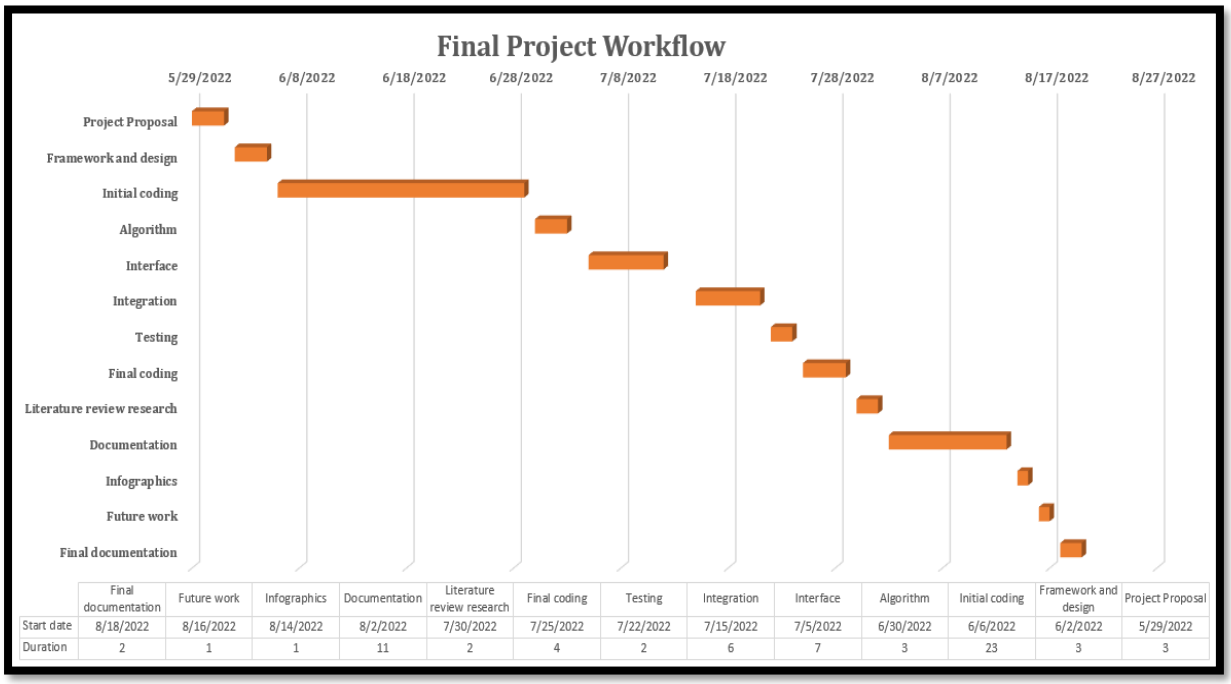


Figure 33 Graphical representation of the workflow

Risks Analysis

When managing a product, risk will arise. There is not a single product in this world without risk, so rather than trying to eliminate all the risks from the product, following a risk management framework is a better way to mitigate the risks. In general, we can follow the National Institute of Standards and Technology (NIST) Risk management framework for risk analysis through which we can identify, eliminate and minimize risks. In this project, too, various troubles have been encountered, or the user may face different risks while using the product they are:

- The owner may forget their password and salt through which the locked files and folder might not be accessible anymore.
- There is no database, so login cannot be done.
- The attacker may delete the locked files and folders.
- Since there is no login system, the attacker might lock the owner's essential files and folders.
- Two-way authentication to the owner is not provided.

Figure 34 Risk assessment

Issue Log

Many issues originated during the development phase of this product. These issues I faced from the beginning to the end are listed below.

Figure 35 Issues handling process

.

- Code not running due to bugs.
- Encryption and Decryption keys were not generating.
- When selecting multiple files to encrypt simultaneously, one or two files were not being encrypted.
- When selecting multiple files to decrypt simultaneously, one or two files were not being decrypted.
- General problems like how to do this project, what format to follow, what to write, what to include, what not to include, how to fulfill the criteria of word count, out of ideas, what logo to make, and others.
- A new window was not popping in the GUI of the product.

Future works and Limitations

This product that we have made is just a prototype and is not market-ready. Even products such as YouTube, Facebook, and other security-related tools like Anti-Spyware Software, Anti-virus software, Steganography-related software, Wireshark, password management software, and others are not perfect. These products or tools have existed for over a decade but still, need updates and upgrades to make them more perfect and enhanced. Similarly, this product has some limitations that need to be fixed in the future to make it more excellent and eventually launch it to the market. So, this product's limitations need to be fixed in the future, and some plans for this product are mentioned below.

- **Lack of two-factor authentication and the proposal to solve this**
  This product only has somewhat one form of authentication. So, the product can provide that one form of authentication to the users through the set password and salt. So, in the future, we will integrate two-form of authentication by introducing a login page and an OTP or email verification to authenticate the user.

- **No database and the proposal to solve this**
  This product does not have a login page, so the product cannot store users' information. However, as this product grows, so do the users. So, we need to keep up with the growing number of users and maintain high importance on their privacy by even introducing three-factor authentication. So, making a database to save users' information is a must. So, we will use the MYSQL database to store users' data. Moreover, the MYSQL database will protect users' private information through encryption.

- **No login page and the proposal to solve this**
  The login page also provides one-way authentication, but we have not used it in this product. So, in the previous section (Lack of two-factor authentication section), we mentioned that the product provides one-way authentication to the users through the set password and salt. A database will be used to store login information, and the information will not be stored on a file.

- **Lack of Marketing and the proposal to solve this**
  We will generate revenue from this product through a subscription-based model included in the product's menu bar section. To correctly market, we need to make a website dedicated to this product. So, in the future, we will make a website dedicated to this product and will also advertise this product using Facebook, YouTube, Instagram, and other social media platforms.

- **Use of Symmetric encryption and the proposal to solve this**
  Symmetric encryption called fernet is used in this product. So, there is only a need for one key to encrypt and as well as to decrypt. However, the attacker can easily

gain the password and salt and crack the key using keylogger software. So, in the future asymmetric encryption like RSA will be used. Moreover, with asymmetric encryption and two-factor authentication, we can be safe from keylogger software and other security attacks.

Moreover, time-to-time upgrades and updates will also be done to ensure that the latest security trends are used in this product, and that the users can be safe from attackers.

Our Subscription Plan and revenue generation method (For future)

(There are four research questions. The fourth research question's answer is in this section.)

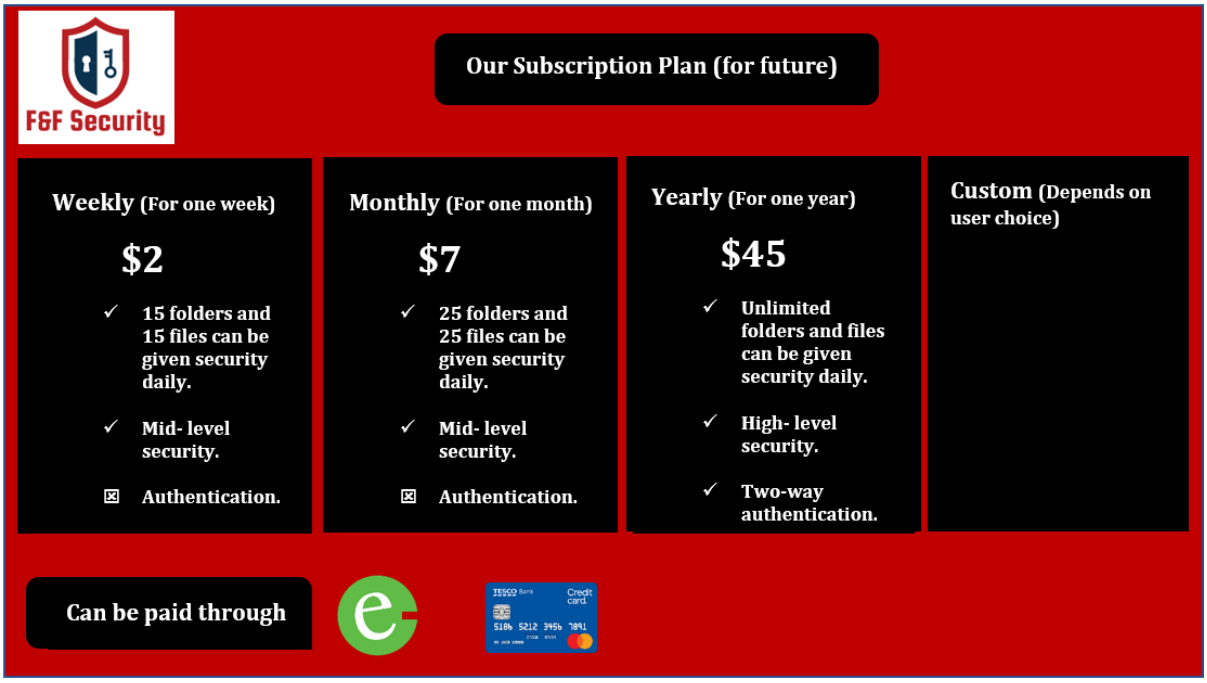


Figure 36 Subscription plans for future

This product is only a prototype, and the subscription plans are made for future purposes when it is full-fledged or ready for market. Moreover, we will generate revenue from the product using a subscription-based model. A subscription-based model is one of many revenue generation models where an individual, a company, or a subscriber pays a certain amount of money to use the vendor's IT services for a certain amount of time. These subscription plans are not functional but are included in the product's menu bar section.

It is also included in the menu bar for marketing purposes. After integrating two-factor authentication into the product, a test trial will be conducted. A YouTube tutorial will be made on how to use this product, and a link will be included in the description that directs to my GitHub. In GitHub, the product will be provided freely without cost for a certain amount of time. (Code will not be provided as it is our intellectual property.) So, when using this product, the users will view the subscription plan and know about the pricing. After a certain period, the free version will be locked, and the user cannot do any activities they were doing previously and must purchase the subscription to use this product. They will pay for a subscription as they got used to using the product for locking files and keeping security on their end.

The pricing can be seen and understood from the picture clearly. The custom-based subscription is taken when users use the product on uneven days. Like three days, for thirteen days which does not have a fixed number of days compared to other subscription sections. The subscription-based model is not generated randomly; instead, the author has followed the subscription-based model of AxCrypt company which is similar to this product and provides a similar type of function used by this product. This company has been existing since 2001 and is still relevant and popular in today's world. Moreover, they also work in the field of providing security to files, folders, and password management.

Conclusion

So, a working product or a GUI-based desktop application is successfully made, performing all the functionalities intended when writing the code. This product secures files and folders and protects them from manipulation. So, the third party cannot change, modify or access the files and folders stored on the hard drive. Moreover, sending and receiving files between two parties are generally done in a plain text format, and those plaintext files are not encrypted. So, people are compromising their security and privacy. However, the sender and receiver can exchange encrypted files with this product. The document mentioned that private files are leaked online after a data breach scenario. Attackers can blackmail the file owner by demanding ransomware. Still, this situation will be somewhat delayed with the use of this product. The incident response team can solve the data breach scenario when attackers are trying to decrypt the encrypted files. So, this product is worthwhile. However, no product is perfect; they need constant upgrades, updated security, and improved functionalities. Similarly, this product has some limitations already discussed in this document. After the limitations are solved, we will eventually launch this product on the market.

Bibliography

Why Personnel Security Matters | Protective Security Requirements (2022) available from https://protectivesecurity.govt.nz/personnel-security/why-personnel-security-matters/#:~:text=Personnel%20security%20protects%20your%20people,being%20lost%2C%20damaged%2C%20or%20compromised [May 30th 2022].

Rosenthal, M. (2022) "Insider Threats Examples: 17 Real Examples Of Insider Threats". [2022] available from https://www.tessian.com/blog/insider-threats-types-and-real-world-examples/ [June 5th 2022].

Hope, A. (2020) *Massive Data Breach Exposes Intel'S Intellectual Property For Its Flagship Cpus And Spacex Sensors* [online] available from https://www.cpomagazine.com/cyber-security/massive-data-breach-exposes-intels-intellectual-property-for-its-flagship-cpus-and-spacex-sensors/ [June 8th 2022].

NHS Data Breach Exposes 24 Staff Data In Scotland (2019) available from https://www.grcworldforums.com/privacy-and-technology/nhs-data-breach-exposes-24-staff-data-in-scotland/396.article [June 17th 2022].

Electronic Transactions Act (2008): Kathmandu: Nepal Government

General Data Protection Regulation (GDPR): Regulation (EU): 2018

Base, K. (n.d.) *Dissertation Archieven* [online] available from https://www.scribbr.co.uk/category/thesis-dissertation/ [June 21th 2022].

What Is Wannacry Ransomware? (n.d.) available from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry [June 27th 2022].

Oladimeji, S. and kerner, S. (2022) *Solarwinds Hack Explained: Everything You Need To Know* [online] available from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [July 4th 2022].

G, T. (2020) *10 Most Secure Messaging Apps - Best Encrypted Chat App Solutions* [online] available from https://getstream.io/blog/most-secure-messaging-apps/ [July 7th 2022].

Ray, G. (2021) *A Deep Dive Into The Leaked Data Of 533 Million Facebook Users* [online] available from https://surfshark.com/blog/a-deep-dive-into-the-facebook-leak-data [July 17th 2022].

What Is Salt And How Does It Provides An Additional Layer Of Security? | Triveni Global Software Services LLP (2021) available from https://triveniglobalsoft.com/adding-salt-to-passwords-for-extra-layer-of-security/ [July 21th 2022].

The Agile Software Development Life Cycle | Wrike Agile Guide (n.d.) available from https://www.wrike.com/agile-guide/agile-development-life-cycle/ [July 30th 2022].

Steel, G. (2015) *Blog - Parameter Choice For PBKDF2* [online] available from https://cryptosense.com/blog/parameter-choice-for-pbkdf2 [August 1st 2022].

Fernet (Symmetric Encryption) — Cryptography 38.0.0.Dev1 Documentation (n.d.) available from https://cryptography.io/en/latest/fernet/ [August 3rd 2022].

Thompson, B. (2022) *20 BEST File & Folder Locker Software For Windows 10 PC* [online] available from https://www.guru99.com/file-folder-locker-windows.html [August 7th 2022].

Facebook Messenger, Instagram Chats Will Not Get End-To-End Encryption Until 2023 (2021) available from https://www.indiatoday.in/technology/news/story/facebook-messenger-instagram-chats-will-not-get-end-to-end-encryption-until-2023-1879501-2021-11-22 [August 9th 2022].

Barrington, R. (2022) *What Is A PESTEL Analysis?* [online] available from https://blog.oxfordcollegeofmarketing.com/2016/06/30/pestel-analysis/ [August 20th 2022].

Case, J. (2021) *Is Dark Mode Better For Your Eyes?* [online] available from https://www.healthline.com/health/is-dark-mode-better-for-your-eyes#:~:text=The%20default%20setting%20on%20most,comes%20with%20prolonged%20screen%20time. [August 19th 2022].

Library.sacredheart.edu. n.d. *Research Guides: Organizing Academic Research Papers: 7. The Results*. [online] available from https://library.sacredheart.edu/c.php?g=29803&p=185931 [August 13th 2022].

Newsoftwares.net Blog. n.d. *Four Solid Reasons Why You Should Lock Folder & Files*. [online] available from https://www.newsoftwares.net/blog/four-solid-reasons-why-you-should-lock-folder-files/#more-1821 [July 19th 2022].

Viber. n.d. *Security | Viber*. [online] available from https://www.viber.com/en/security/ [July 20th 2022].

Axcrypt.net. n.d. *axcrypt*. [online] available from https://www.axcrypt.net/ [August 17th 2022].

Software Testing Help. 2022. *10 Best Folder Lock Software (Folder Locker) For Windows PC*. [online] available from https://www.softwaretestinghelp.com/folder-lock-software/#1_Folder_Lock [July 25th 2022].

Docs.microsoft.com. 2022. *Office 365 Message Encryption - Microsoft Purview (compliance)*. [online] available from https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide [July 29th 2022].

Iobit.com. n.d. *The Best Files Protection Tool - IObit Protected Folder Windows 10*. [online] available from https://www.iobit.com/en/password-protected-folder.php [August 10th 2022].

Tutorialspoint.com. n.d. *Base64 Encoding and Decoding*. [online] available from https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_base64_encoding_and_decoding.htm [August 18th 2022].

NewSoftwares.net. 2022. *Data Security & Protection Software - NewSoftwares.net*. [online] available from https://www.newsoftwares.net/ [July 31th 2022].

Aumasson, J. (2018) *Serious Cryptography*. 1st edn. San Francisco, CA: No Starch Press.

DELFS, H. (2016) *INTRODUCTION TO CRYPTOGRAPHY*. 3rd edn. Bavaria: SPRINGER-VERLAG BERLIN AN.

Appendix

GitHub Link – Source code

https://github.com/nirajsangraula/Final-semester-project-code.git

Google Drive Link – Demonstration of the product

https://drive.google.com/file/d/18t7iI204hNIQi6JUSCykNQ-iY6rUJ-q5/view?usp=sharing