Project Name: Be Secure

*Developed using VB.NET*

Contents

[Introduction 4](#_Toc26659628)

[CIA concept 5](#_Toc26659629)

[Confidentiality 5](#_Toc26659630)

[Integrity 6](#_Toc26659631)

[Availability 7](#_Toc26659632)

[Client/Server chatting and file transfer system 8](#_Toc26659633)

[User manual 8](#_Toc26659634)

[Security features 24](#_Toc26659635)

[Data encryption and decryption 24](#_Toc26659636)

[Functionalities 25](#_Toc26659637)

[Advantages 26](#_Toc26659638)

[Impact 26](#_Toc26659639)

[AES, DES and Rijdael Encryption algorithm 27](#_Toc26659640)

[User’s records in hash value 28](#_Toc26659641)

[Functionalities 28](#_Toc26659642)

[Advantages 29](#_Toc26659643)

[Impact 29](#_Toc26659644)

[Checking Files Integrity 30](#_Toc26659645)

[Functionalities 30](#_Toc26659646)

[Advantages 31](#_Toc26659647)

[Impact 32](#_Toc26659648)

[Extra Features 32](#_Toc26659649)

[Email verification – Rushdi Eskandar 32](#_Toc26659650)

[Functionalities 32](#_Toc26659651)

[Advantages 33](#_Toc26659652)

[Impact 33](#_Toc26659653)

[Captcha – Haruna Abba Musa 34](#_Toc26659654)

[Functionalities 34](#_Toc26659655)

[Advantages 36](#_Toc26659656)

[Impact 36](#_Toc26659657)

[Hidden user’s records – Haruna Abba Musa 36](#_Toc26659658)

[Functionalities 36](#_Toc26659659)

[Advantages 36](#_Toc26659660)

[Impact 37](#_Toc26659661)

[Password Strength Verifier– Rushdi Eskandar 38](#_Toc26659662)

[Conclusion 40](#_Toc26659663)

[Appendices 41](#_Toc26659664)

[Progress report 41](#_Toc26659665)

[References 45](#_Toc26659666)

[Workload matrix 48](#_Toc26659667)

[Gantt Chart 49](#_Toc26659668)

# Introduction

The project team has aimed to achieve the aim of developing a chatting and file sharing system which will allow users to communicate and transfer data as desired. The target objective of building the system is to overcome the security problems that hinder people’s thoughts every day when it comes to data transfer, most of the chatting platforms nowadays in one way or the other have some security issues which makes users not to fully trust sharing data with the systems due to less security and could not provide a secure connection and encryption. The project main aim is to develop a system that will allow users to chat and at the same time transfer data to other parties. The application that is been used to develop the system is visual studio 2013 with using programming language of VB.NET which is known as Visual Basic and will be documented with Microsoft word.

# CIA concept

## Confidentiality

According to (Margret Rouse, n.d), confidentiality is ensuring that data or sensitive information is prevented from reaching the wrong people and making sure that the right those right people can get that information or data. The access to the data or sensitive information must be restricted to those that are authorized to access or view the data, data is categorized in accordance to the amount and type of damage that could be done when that sensitive information falls into the hands of wrong people. There are several methods used to ensure confidentiality, data encryption is a usual method. For example, when purchasing an item online, there is the need of inserting the card details like the card number, expiry date etc. then a transaction process follows, therefore encryption follows. The number is encrypted when transferring the card number to a transaction processing network which is where the confidentiality of data occurs, the data is being made private and secured with encryption and also by limiting appearance of the data in places like database, log files, backups, printed receipts etc. besides that, if a personal computer with sensitive information in it either about a company's employee or a secret documents stored in the pc is stolen or sold, there could be a tragic result in a breach of confidentiality. Moreover, giving out confidential information over the telephone might be a breach of confidentiality mostly if it is not a secured line. Therefore, it’s essential to know that confidentiality is necessary and important in securing sensitive data.

## Integrity

Data integrity refers to the protection of digital information to ensure that it can’t be modified only by authorized people. It involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Therefore, to maintain integrity, data must not be modified in transit and steps must be taken to ensure that data can’t be changed or modified by an unauthorized person or program ( [Rouse](http://www.techtarget.com/contributor/Margaret-Rouse), 2017). Integrity can be seen from different points of view as follows:

* **technology**
* **content**
* *Technology point of view*

From this point of view, digital information must be highly secured so it won’t be easily modified or corrupted, in any situation whether the data are being stored somewhere, or they are transferred between source or goal, or during the procedure of its elucidation in the frontend of its addressee. Integrity can be discussed from different types of views (as stated by Hanáček & Staudek, 2000), it can be discussed in terms of strength and weaknesses. Firstly, “weak” is when the security is used to protect against data modification due to commotion, randomness of the sequence etc. On the place where data are stored in somewhere else are controlling the checks are sued (e. g. CRC – Cyclic Redundancy Check) and amid the data exchange appropriate conventions are used (TCP – Transmission Control Protocol). “Strong” is from his point of view “weak” + means using the method for cryptography.

* *Content point of view:*

This part of view discusses about the loss of integrity when information was unintentionally altered or changed, despite of the fact from the technology point of view the integrity was not violated. In the situation if the integrity was breached and modified, then from the specific application which is processing the violated information different cases can be shown out (Drtil, 2013). In fact, there situation can be happened as follows:

1. Application failure (the data will not be processed)
2. Data will be partially/fully processed, but error message will be displayed)
3. All data will be processed (no error message will be displayed)

## Availability

Availability refers to a security procedural which to ensure that data and resources are kept to be only available for authorized use, especially during emergencies or disasters  [(Breithaupt](http://www.pearsonitcertification.com/authors/bio/9f269ea1-f45d-49dc-ae25-ce7def6e6307) and  [Merkow](http://www.pearsonitcertification.com/authors/bio/d45339cb-d931-4ef4-be06-f248be4952a6), 2014). In simple words, availability means all data and other resources which are critical must be accessed by authorized parties when as per their needs. Basically, there are three common encountered challenges which are usually faced be the Information Security Professionals. Firstly, The Denial of service (DoS) attacks which can be occurs intentionally. Second, loss of data system capabilities which can be happening due to this kind of attack. Third, equipment failure can occurs doing normal use.

There are 3 common challenges which is normally encountered by the information security professionals, they are Denial of service (Dos), loss of information system capabilities, and equipment failures. The DoS occurs caused by attacks that is done intentionally. It can also occur when weaknesses are undiscovered in implementation. Loss of information capabilities can emerge due to the impact of natural disaster. The third challenge that is commonly faced is equipment failures which surface during the normal use (Breithaupt, 2004).

# Client/Server chatting and file transfer system

Nowadays, people are using different chatting tools to communicate or share files. In fact, there are lots of socialized chatting system around the world and most preferable to be used by people are those Web-chatting systems. Hence there are lots of options provided to users to chat and share files, we came up with a new unique chatting and file sharing system which can allow different users to chat and transfer files. Along with the basic model, architecture and features of the system is supported with some additional security measures to enhance the security level and make it more reliable.

## User manual

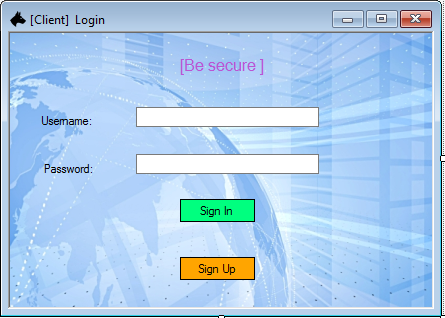


Figure 1: Prompting to enter login details

It is the main page for the system where the user needs to Sign in or Sign Up.

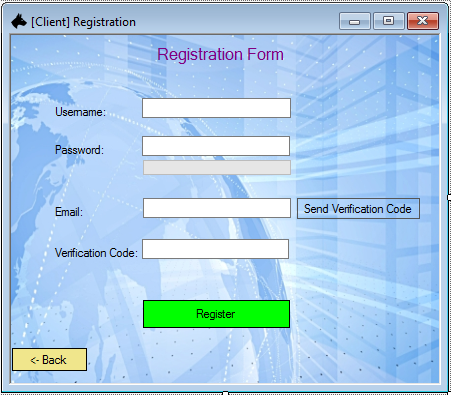


Figure 2: Signing Up to the system

When the user clicks on the Sign-Up button, he/she will be taken to this page for registration process. The user needs to enter his/her username, password and email address for verification and confirmation purpose. After that, the user needs to check the email and get the Verification Code to finish the registration procedural.

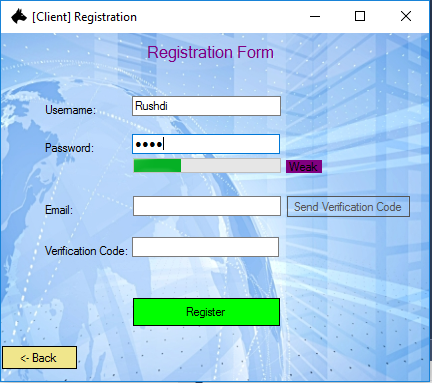


Figure 3: Registration Form

As shown in figure 3 above, if the user enters a password in the chatting system, the system will directly determine the strength of that password to let the user know about the security level for the given password. Therefore, the users would try to provide another password to have a better secure account in the system.

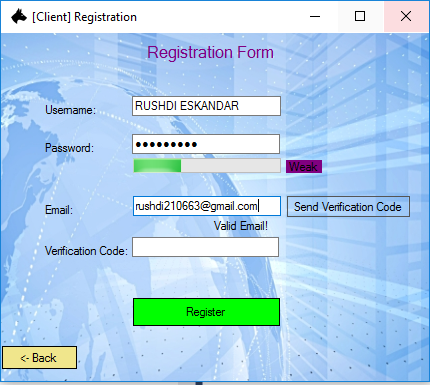


Figure 4: Registration Credentials entered

As shown in figure 4, the user has entered his e-mail address along with created username and password for the chatting system. Thus, a verification message will be directly send to his email address.

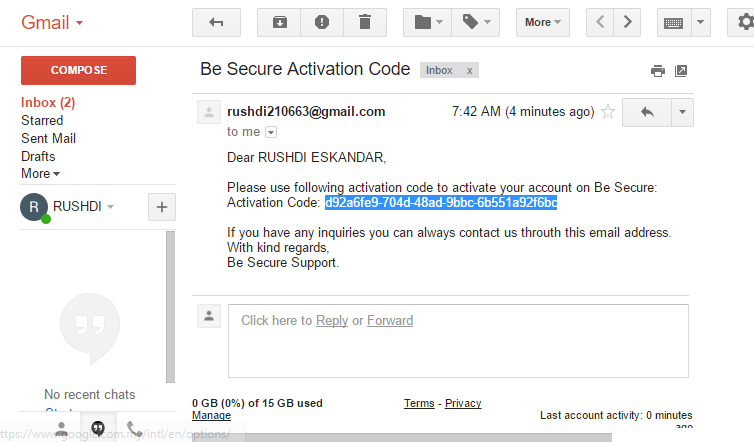


Figure 5: Verification E-mail sent

In the Figure 5 above, after the user has already click on the Verification button, he/she will receive a Verification code in his/her email. Therefore, the user needs to enter his email and check the received message to copy the Code and enter it in the system to be verified.

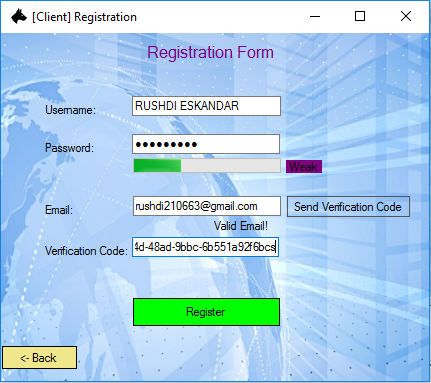


Figure 6: Checking Verification Code

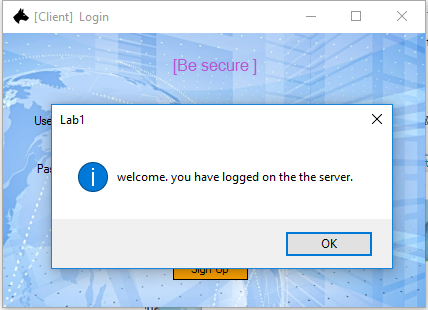


Figure 7: Registration Successful

Once the code has been checked successfully and the account have been activated successfully, then the user will be able to Sign In to the system. If the user enters the correct Username and Password, then a box message should pop up shown that the user Sign In successfully.

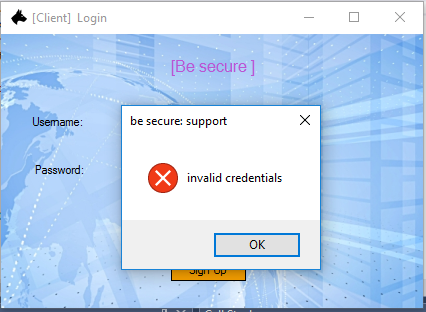


Figure 8: Login Page

As shown in the Figure 8 above, the user will receive error message when he/she enters wrong credentials to the system.

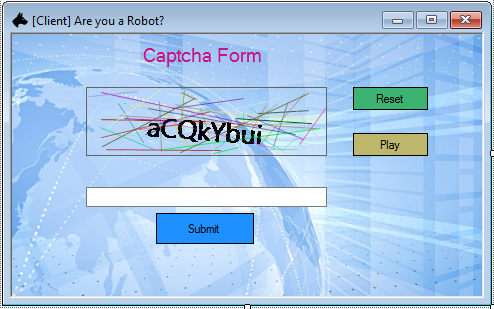


Figure 9: Captcha Verification for wrong credentials

The Figure 9 above shows when the user enters wrong credentials, repeatedly. Therefore, he/she will be driven to this form to enter the image letters as shown on the screen. This is procedural have been added to the system in order to verify the authentication user’s account to determine whether or not he/she is the one trying to access the account. Moreover, the user also can keep resetting the Captcha image in case if it is not clear to him/her.

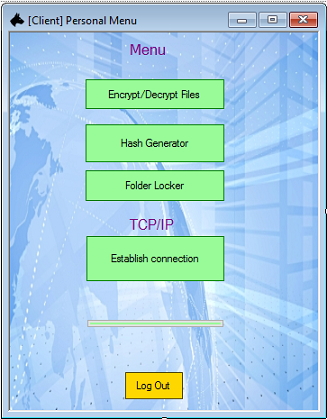


Figure 10: Main Menu

Once the user has successfully Signed In to the system, this is the main menu which will be shown after login, asking the user what to do next.

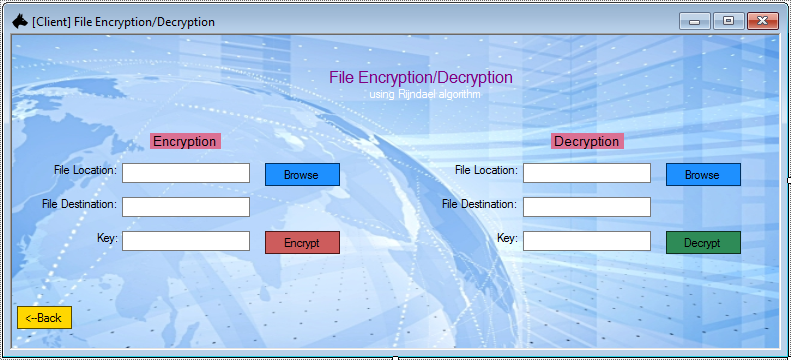


Figure 11: File Encryption/Decryption

If the user clicks on the first button “Encrypt or Decrypt files”, then this form would be shown. As show in Figure 11 above, the form will be provided with two sides; one for Encryption and the other for Decryption.



Figure 13: Encryption Completed

When the user needs to encrypt or decrypt a file, he/she needs to browse the file in the PC to be selected, then the user would press encrypt/decrypt button respectively. For encrypting a file, the user needs to select a file then enter the encryption key to proceed further. Once the user has keyed in the key for Encryption in the step above, as shown in figure 13, a box message will pop up appear to confirm that the encryption has been completed successfully.

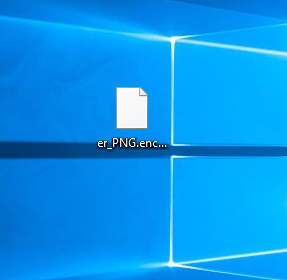


Figure 14: Encrypted File

As shown in figure 14 above, the encrypted file which the user had intended is being there. It has been stored in the same location which the user had specified earlier in Figure 13. The stored file will be in the format of a .txt file.

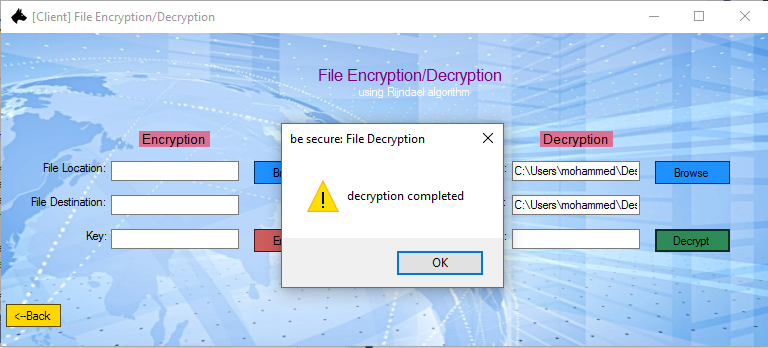


Figure 15: Decrypting a File

The figure 15 above shows the decrypting of the file which had been encrypted earlier. For testing purposes, the file which had been stored as “a”, has been tried to decrypt. The user must enter the same key which have been entered before while encrypting the file so the file will one be decrypted for authorized people.

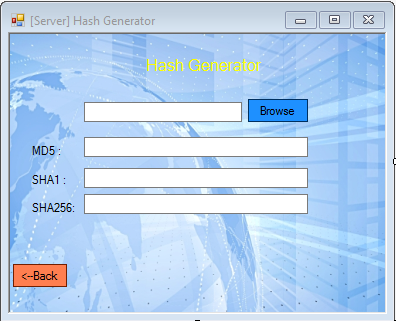


Figure 16: Hashing files

When the user click on the second option which is Hash Generator, this form will appear as shown in Figure 16 above. After the user has browsed to select the file for hashing some encryption methods will appear such as MD5, SHA1 and SHA256 encryptions.

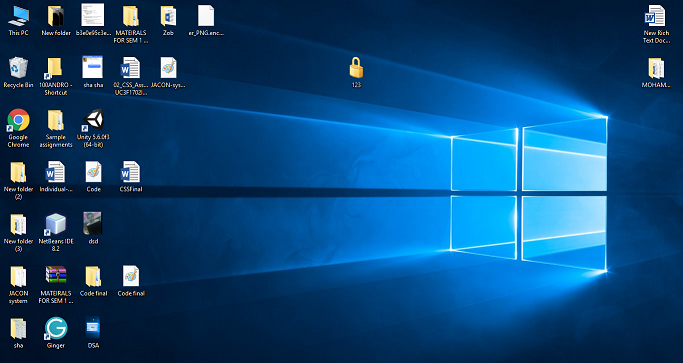


Figure 17: The decrypted file

As shown in the figure above, the Encrypted file which has been saved on the User’s desktop.

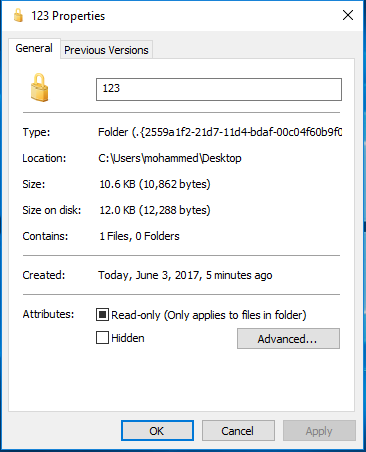


Figure 18: Decrypted file details

The figure 18 above, shows the details of the file which has been decrypted as it has now been decrypted, instead of hidden the file which provides access to the user to have been Read-only.

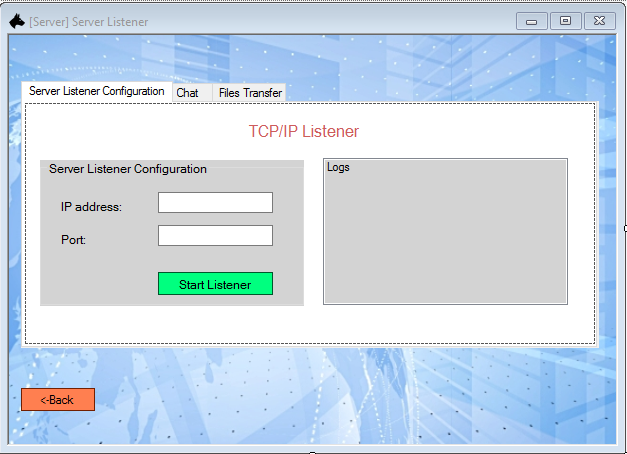


Figure 19: Server Listener

Figure 19 above shows the Server Listener side which the user will be directed when he/she clicks “Establish Connection” under TCP/IP.

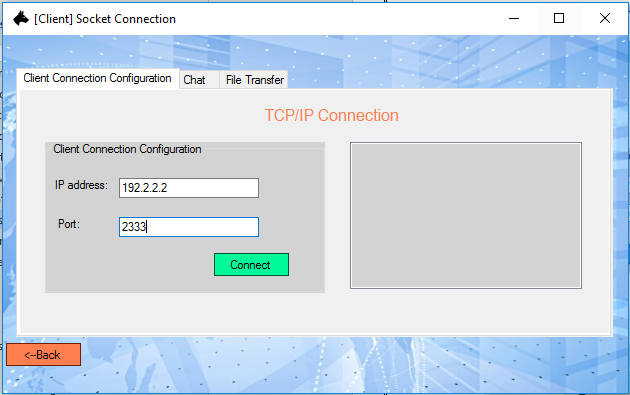


Figure 20: Server Listener Configuration

After that, the system would prompt to show tow box fields to let the user enters the IP Address and Port Number to establish the connection via using TCP/IP Protocol.

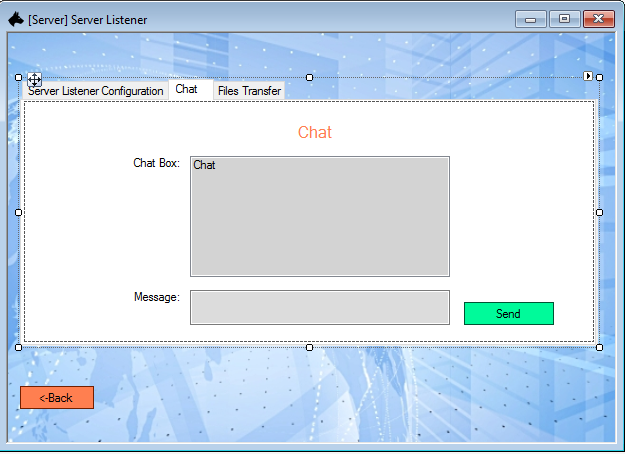


Figure 21: Configuration Complete

Next, as shown in figure 21, this form would be shown when the user has entered their IP Address and the available port number. Under the Server Listener Configuration tab, the user can edit his/her IP address as well as Port Number, whereas under the Chat bar, the user can connect and chat. Furthermore, the last tab of Files Transfer, would let the user to send and receive files, as shown in figures 22 and 23 below.

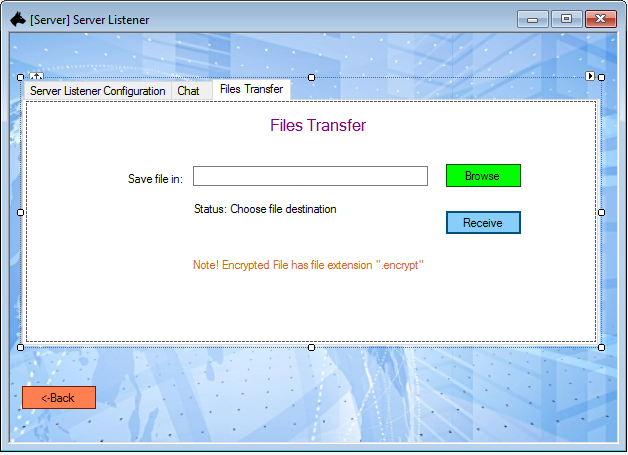


Figure 22: Receiving a file

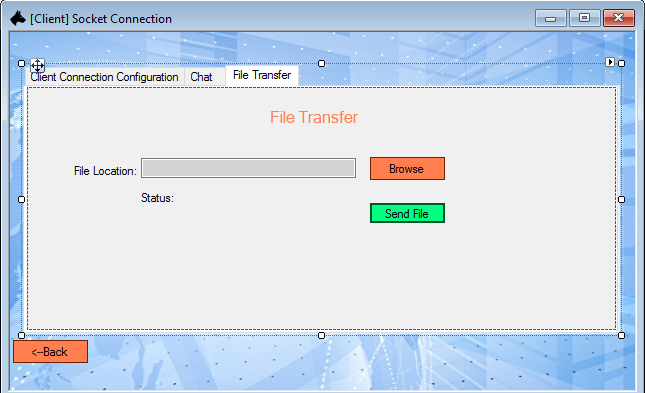


Figure 23: Sending a file

Figure 24 below shows the File Transfer taking a place; on left side, a file is being received, while on the right side a file is being sent by the user.

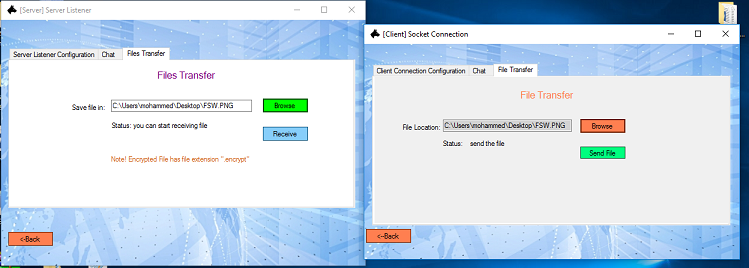


Figure 24: File Transferring

# Security features

## Data encryption and decryption

“Data encryption refers to the process for converting the electronic data to another form known as cipher text, which can’t be easily understood by other parties except authorized ones”

This security technique is used for making the data unreadable by unauthorized people who are not allowed to read or modify the information. A simple example can be taken here, when the data is transferred through the internet between two parties, it is possible that this data can be modified or changed by a third party which called “Man in the middle attack”, so it is dangerous if the attack happens during transferring important information, therefore, it is critical to Encrypt files before sending them through the network. Basically, there are various data encryption algorithm which can be used and most of them are based on mathematic formulas. In fact, encryption is a formula which creates a cipher key and add it to the plaintext or primary data. Therefore, the original data will be modified to look something different. Thus, only authorized receiver will know the specific encryption algorithm then he/she can decrypt that to plain text. Therefore, the encryption algorithms are used so messages will be highly secured to be cracked or decrypted by unauthorized parties. (WhatIsMyIPAddress.com, 2016)

Asides from that, decryption is the process of converting/decrypting the encrypted data to the original format “plain text”, which can only be understood by the authorized parties. Basically, decryption requires a secret key or password. (Webopedia.com, 2016)

In this project, the developed system used Rijindel algorithm. Rijndael will begin to supplant the Data Encryption Standard (DES) then later Triple DES over the next few years in many cryptography applications. “The Rijndael algorithm is a symmetric block cipher which supports a [key](http://searchsecurity.techtarget.com/definition/key) sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks but in excess of AES criteria, the block sizes can mirror those of the keys.” (SearchSecurity, 2007)

### Functionalities

The proposed system has a function which can encrypt and decrypt any files stored in user’s computer/USB/cloud drive. When the user clicks on the “Encryption and Decryption files” button, he/she will be taken to the form where he/she can encrypt or decrypt files. The user needs to select a specific file and its destination in order to encrypt or decrypt files. More on that, the system has been provided with extra feature to allow for selecting a specific key for encryption of the file, which means that the file will be encrypted using private key of the user and the encrypted file will be decrypted only by using that key.

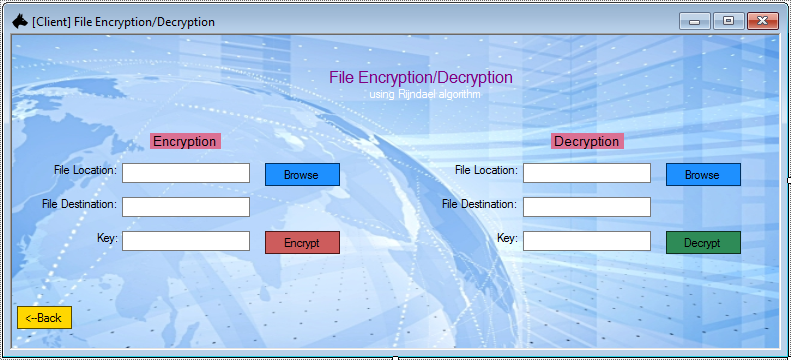


Figure: Encryption and decryption of the files



Figure: File is encrypted using Rijndael algorithm

When the file is successfully encrypted, it will be stored in the chosen folder with another file extension such as *“. encrypt”*. Example is shown on figure below:

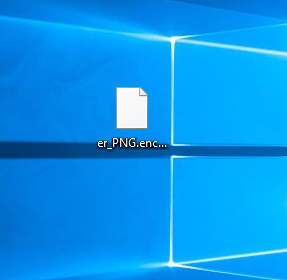


Figure: example of encrypted file

### Advantages

There are few main advantages of encryption files which play the essential role in this system.

Nowadays, the price of private information grows day by day because cybercrime expends their borders to new sectors of IT infrastructure. One of the weightiest argument that user can encrypt his/her private data and be sure that it can’t be read by unauthorized parties. Moreover, the data can be decrypted via using private key. Decryption function implemented in the same system that make it easier for users.

### Impact

If the system doesn’t have the function of the data encryption, the system will not be enough secured. As the security technology is always in progress, there are also many ways to steal, modify or sniff user’s private information. Therefore, if the user’s private information (such as bank details, business contracts, debenture stock etc..) is not encrypted it can be read by anyone who has that data, as a result, it will be dangerous if a hacker gets that digital information and he/she can blackmail and threat owners of the information.

## AES, DES and Rijdael Encryption algorithm

**DES**

Data encryption standard (DES) is a symmetric-key block cipher that was published by the national institute of standards and technology (NIST), it encrypts message and decrypts message with the same key and it is an implementation of feistel cipher which uses about 16 rounds feistel structures and has block size of 64-bit. Moreover, DES has an effective key length of 56-bit, because 8 of the 64-bits of key are not used by the encryption algorithm. The federal government originally developed DES encryption for over 35 years ago in order to provide cryptographic security for all government communications. The idea was to ensure government systems all used the same, secure standard to facilitate interconnectivity. To show that the DES was outdated and vulnerable to attacks, it should not be used in important systems anymore, a series of challenges were brought together to see how long is it going to take to decrypt a message. Two organizations played key roles in breaking DES: distributed.net and the Electronic Frontier Foundation (EFF) (Michael Cobb, n.d).

**AES**

The advanced encryption standard was developed by the national institute of standards and technology (NIST) in 1997 to be the successor to the data encryption standard (DES) due to it vulnerability to brute-force attacks. Brute-force attacks is trial and error method that is used by applications in order to decrypt password or data encryption standard. The advanced encryption algorithm was meant to be implemented easily in software and hardware and also in restricted environments so as to prevent various attacks techniques. Advanced encryption standard has some features that enables the standard algorithm of block cipher which is capable of containing 128 bit blocks with the use of key sized 128, 192, and 256 bits. The advanced encryption standard includes important aspects like security, implementation, cost etc. Moreover, uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block. The original DES designers made a great contribution to data security but it is said to be the aggregate effort of cryptographers for the AES algorithm has been far greater (Margret Rouse, n.d).

**Rijndael**

Rijindael is an algorithm that has been selected by the national institute of standards and technology (NITS) as a candidate of advance encryption standard (AES) in order to supplement the data encryption standard in the next few years. The rijindael encryption algorithm is a new generation of symmetric [block cipher](http://searchsecurity.techtarget.com/definition/block-cipher) that supports [key](http://searchsecurity.techtarget.com/definition/key) sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, the AES design criteria, uses the block sizes that can mirror those of the keys. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows for example,for 9 rounds, if the key/block size is 128 bits, 11 rounds if the key/block size is 192 bits, and 13 rounds if the key/block size is 256 bits.

Moreover, Rijndael is a substitution of linear transformation cipher, not requiring a Feistel network. It uses triple discreet invertible uniform transformations (layers). These are Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to the security (Margret Rouse, 2015)

## User’s records in hash value

Hashing is the transformation of a string of [character](http://searchcio-midmarket.techtarget.com/definition/character)s into a usually shorter fixed-length value or key which represents the original string. Hashing is implemented to index and retrieve items in a [database](http://searchsqlserver.techtarget.com/definition/database) because it is faster to find the item using the shorter hashed key than to find it using the original value ([Rouse](http://www.techtarget.com/contributor/Margaret-Rouse), 2017).

In simple words, hashing is a method of taking data, encrypting it, and creating unpredictable, irreversible output.” Basically, there are number of different hashing algorithms such as MD2, MD5, SHA, SHA-1, SHA-256, SHA-512 and many others (eTutorials.org, 2017). The proposed system has implemented MD5, SHA-1, SHA-256 hashing algorithms. And here MD5 will be taken as an example to justify its benefits and impact.

### Functionalities

The proposed system uses hashing algorithms to encrypt different types of files. By default, when the user register into the system he/she must his/her username and password which will be later used to Sign in into the system. Each user has his/her own record to allow for logging to the system and those records contain user’s information (username, password), which is used to login to the system. Each user record should be saved in a text file in a hashed form.



Figure: Hashed user’s records

The function of the verification and comparison of username and password is shown below:

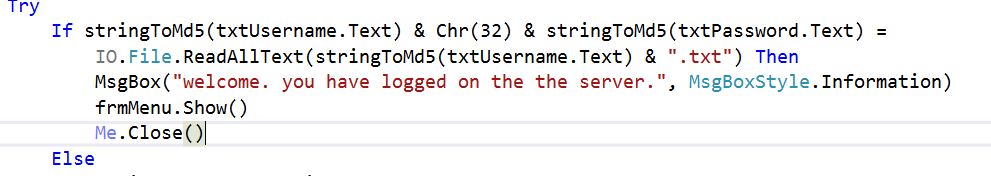


Figure: Hashing using MD5

### Advantages

Hashing is one of the common security considerations which must be implemented when designing any application that accepts username and passwords from users. If hashing is not used and the database got hacked by a hacker, then all the user’s records will be stolen and compromised. Therefore, the hashing algorithm must be used in the system for user’s records as it assists to increase security level and make it difficult for attackers to predict the original password. (Php.net, 2016)

### Impact

If the application doesn’t utilize the hashing algorithms for username and password, the system much vulnerable and risks will be increases. In case if the data is not being hashed and an attacker get the chance to access to the user’s login information, it will be very simple for him/her to use that unencrypted information.

## Checking Files Integrity

To ensure the integrity of a file is essential, it need to be maintained and must make sure that the data is accurate and consistent over the entire lifecycle. Moreover, integrity checking plays a vital role in the security aspects by ensuring the quality of a received data is not poor.

.

### Functionalities

MD5

MD5 algorithm which is known as message digest algorithm is a one-way cryptographic function that accepts data/message of any length as an input and returns it as output for a fixed-length digest value that can be used to authenticate the initial message. The MD5 encryption algorithm was invented by Ronald Rivest, it is implemented to verify the data integrity by hashing random data that can be presented in any length and size as an input then the output will be presented as fixed size generated hash value, what so ever the input size is, the algorithm will always generate a fixed size MD5 hash that is represented in 32-digit hex. The below figures show the example of MD5 implementation where the hashed files are shown in message1.txt and message 2.txt. moreover, both files have different sizes, but they all got the fixed hash value which is 32-digit hex as it is supposed to be represented.



Figure: MD5 hash value

SHA1

In cryptography, SHA1 which is secure hash algorithm is a cryptic hash function that is designed by the united states national security agency and is also a united states NIST that produces 160-bit (20-byte) hash value that is known as a message digest. It appears to be the most common utilized algorithm that is applied in various huge projects which are related to security. SHA1 is normally utilized in cryptographic environment and applications which require high data integrity. In the developed program. For this application, we have implement the SHA1 algorithm. Below is the sample of a file with the hash value produced by utilizing SHA1.

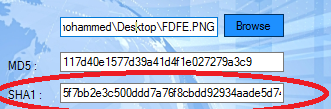


Figure: SHA1 Hashed Value

SHA256

SHA256 is among the SHA2 set which consist of SHA224, SHA256, SHA384 and SHA512 of cryptographic hash functions that was designed by the U.S. national security agency (NSA) and was published in 2001 by the NIST for the U.S federal information processing standard (FIPS).

SHA256 is a type of cryptographic hash that generates an almost unique signature for a text. The hash functions of cryptographic that operate on digital data are mathematical operations. People can identify and analyze the integrity of a data by doing comparison between the computed hash to a recognized hash value. The below figure shows the implementation of SHA256 in the application.

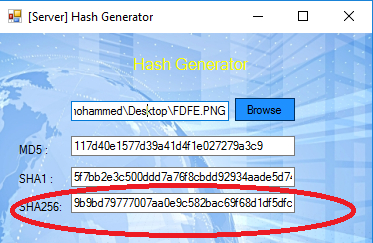


Figure: Utilization of SHA256

### Advantages

The advantages of utilizing hash functions in the application is to ensure the integrity of the sent and received messages, it is important to avoid any data inconsistency during the process of message distribution until the messages are received by the authorized receiver. The inconsistency or inaccuracy of either sent or received messages can occur as the impact of data loss due to instability of secured or private internet connection, malicious actions performed by attacker, and virus infection.

### Impact

Hashing is an important which when not implemented in the application will be difficult for authorized users to identify the integrity of the sent and received files and if there is any disruption that happens willingly or unwillingly, the users will face a difficult time to identify the corrupt files that is sent or received.

# Extra Features

## Email verification – Rushdi Eskandar

Email verification is one of the methods to protect registration process from massive… this method consists of few steps: (1) receiving user’s email address, (2) sending email to this address with unique code that user required to enter, (3) verify validity of the entered code.

Upon registration user is required to enter his/her valid email for further verification. It is important that user has access to entered email and can easily receive verification code.

### Functionalities

Email Verification is particularly used to avoid robot users and check user’s validation. In fact, it is mainly implemented to increase the level of protection for both users and application. Email verification would be used in case if users forget their passwords, so it can assist to recover them back. In case if a user has lost/forgotten his/her password, he/she can use the email to get the password back. The system ensures to send new password to the registered email particularly. Asides from that, email verification can prevent the system from any registrations of fake emails and bots which can use multiple accounts automatically. Additionally, email verification prevents double registration, which means each user must have only one account registered within one used email. This will assist to prevent creating multiple accounts and which will be inactive.

Figure below demonstrate how the system sends verification code to the user’s email.

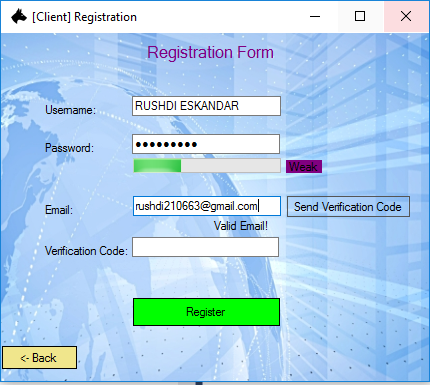


Figure: Send verification code

Once the verification code has been sent, the user will receive email with verification code.

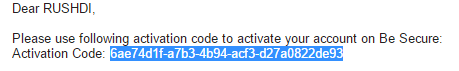


Figure: Verification code

### Advantages

* Users verifications “System will be used only by real users”
* Password recovery
* Prevent double users’ registrations
* Increase security level

### Impact

Assuming in case if the system doesn’t have email verification function, there might be several scenarios of harmful events. One of the situation might happened if someone tries to make the system down and use bots. Bots may create multiple accounts at the same time which will have some impacts over the system. Thus, the system might be overloaded if there is a huge bots attack.

## Captcha – Haruna Abba Musa

A CAPTCHA (“Completely Automated Public Turing test to tell computers and Humans Apart”) is a program that ensures protection to websites against bots by generating and assigning a small task or test of asking the user to rewrite a short text so as to verify if it is a human using the system or a computer (Tim Schiesser, 2013). For example, humans can read text while current computer programs cannot read. Few years back, people tried to use websites in an inappropriate way for profit, gradually the abuse became profitable and the scale of abuse grew using automated software (which sometimes is referred to as bots) To prevent the bots from overloading website with spam, fraudulent registrations, fake sweepstakes. Due to the abuse, captcha was invented to avoid the misuse of websites and now over 3.5 million sites globally implemented CATPCHA.

### Functionalities

CAPCHA functions during a system login, it is an authentication function that verify username and password when entered. When one of the username and password is wrong, the system will display notification message “Be secure support” as shown below:

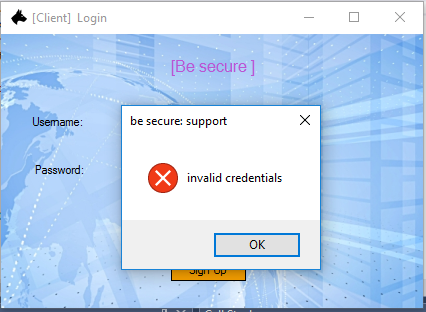


Figure: Invalid user credentials

Once the user selects “OK” the system will display Captcha form to check that the user is not a robot.

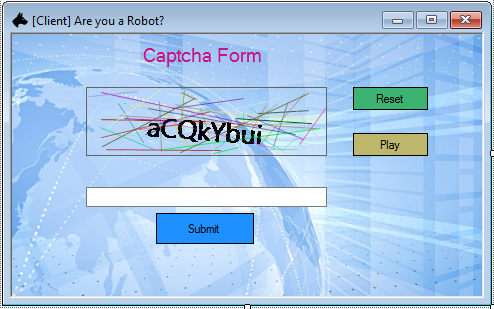


Figure: Captcha form

The source code of the captcha function can be found below:



Figure: Captcha function

### Advantages

Captcha function play an important role in this application. Firstly, captcha function increases level of the security and prevent the system from the bots’ attack that is quite common important nowadays. Secondly distinguishes between a human and a machine.

### Impact

Websites that don’t have the CAPTCHA function are vulnerable to the type of robots and bots that does spamming to harm the system. But if websites implement the CAPTCHA function, it will surely stop spammers from registering into the system, the spammers and bots cannot read the letters and presented by the captcha, therefore it prevents attacks to sites.

## Hidden user’s records – Haruna Abba Musa

Windows platforms have the ability to hide users’ files and folders, which means a user can choose to hide his/her sensitive data from other users. Moreover, the hidden files or folders can ensure privacy especially for the people that uses public devices.

### Functionalities

In the system, the application hides a user’s data when the user chooses to do so, then the system hides that particular data automatically and can be set to hide new data when created automatically.



Figure: File attributes options

### Advantages

Hidden users’ records are very important to the application and it is something that other application will wish to have because it increases the rate of security in applications but in this scenario, the application there won’t be the need to use database because the application is developed for small amounts of people which means text files will be used to store data.

### Impact

Developers spend huge amount of time to find a possible way to improve applications with advanced security strategies but implementing the hidden function in application will definitely increase the rate of security in applications.

## Password Strength Verifier– Rushdi Eskandar

The proposed system has been supported with the password strength checker function. This function can determine the strength of the entered password’s characters in the password field when the users do the signup process. The password strength function is applied to let the user know regarding the strength of the inserted password. This feature can measure the strength of the passwords by analyzing the entered characters which should be created based on the combination of symbols, numbers, capital letters, and small letters to generate a stronger password. Moreover, the more characters entered, the stronger password will be. The strength status of the password will be shown on the right side of the entered password field as shown in the figures below:

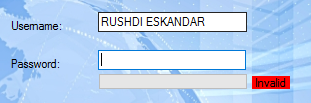


Figure: Status shows ‘Invalid’ when the field left blank.

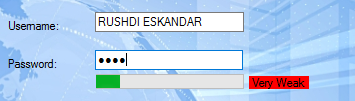


Figure: Status shows ‘Very Weak’ when the number of characters entered is too less or not vary.

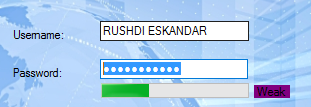


Figure: Status will show ‘Weak’ when the number of characters entered is too less or less vary.

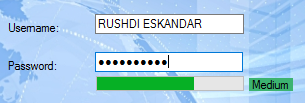


Figure: Status shows ‘Medium’ when the characters entered is vary.

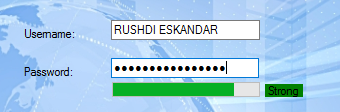


Figure: Status shows ‘Strong’ when the characters entered is long and vary.

# Conclusion

To conclude, the developed system application wan mainly focusing on creating a chatting system which was developed/built for users to have a better and reliable source of communication as well file sharing system. Most chatting systems in these days provides users with chatting platforms which are not enough secured, therefore, this chatting system has been created and supported which extra security features to protect the information while being transferred from both the client and server side. These features are E-mail verification, Captcha, hiding users’ records which would ensure data encryption, checking the password strength upon registration and Folder Locker which allows users to lock their files and give authorized access to authorized people.

# Appendices

## Progress report

|  |  |  |
| --- | --- | --- |
| **Names:** | | Rushdi Eskandar Mohammed Thabit |
| **1** | **Proposed System** | |
| **1.1** | **Title:** Be Secure | |
|  | Chatting and File Sharing System | |
| **1.2** | **General Description** | |
|  | It is a Chatting and file sharing System, which allows people to communicate with each other and share files. It is a client and server-based application for windows platform.  The application has the ability to Encrypt and Decrypt data in order to provide secure chatting environment. | |
| **1.3** | **Main Components** | |
|  | * User registration * Password strength verification * Captcha Form * Login authentication * File Transfer through the Socket * Chatting System through the Socket * Email verification upon registration * File Encryption and Decryption (AES algorithm) * Hash sum verification | |
| **1.4** | **Design: (Use Case/Flowchart/….)** | |
|  |  | |
| **1.5** | **Techniques:** | |
|  | 1) Confidentiality:  Using AES encryption algorithm  2) Integrity:  We will use MD5, SHA256 hashing algorithms  3) Availability:  We will use username and password which have been verified by email | |
| **1.6** | **Extra Features:** | |
|  | 1. Email verification 2. Captcha 3. Password strength 4. Hidden user’s records | |
| **2** | **Requirements** | |
| **2.1** | **Hardware/software/tools** | |
|  | Asus A10; Core i5, 4 Gb RAM  Development tool: Visual Studio 2017 | |
| **2.2** | **Programming language** | |
|  | VB.net | |
| **2.3** | **Database** | |
|  | Data will be saved in text files | |

# 