Short Communication Report

IMPLEMENTATION OF A DATA AND COMPUTER SECURITY APPLICATION

*BIBU, G. D[1]. & CHUKWUEMEKA, B. B[2].

[1]Department of Mathematics,
[2]ICT Directorate
University of Jos, Nigeria
*gidadik@yahoo.com

As information requirements become more complex, users have adapted computer in almost all their daily endeavors. This has made a lot of users to be online and perform most of their businesses online. The basic data security utility applications that are provided by most operating systems and other application software is not strong enough to allow people to carry over the confidence found in the physical world to the electronic world. It does not allow people to do business electronically without worries of deceit and not being able to have personal information kept secret and secured from hackers and crackers. Data security has therefore become a major problem that will jeopardize the various electronic initiatives (e-initiatives) in business, administration, education etc if not properly addressed through all possible means (Syngress, 2008)

In this work, we design and implement security software which will enable users to protect their data using several data security techniques and approaches which are considered highly reliable. These security techniques include; improved encryption and decryption methods, improved folder protection techniques, improved computer system monitoring using key logger and camera video streaming (Thawte, 2008).

The proposed system: The existing system is based on the security utilities the basic operating system provides for all users. Users only have the option of making folders private, changing the files and folder attributes to either “**hidden**” or “**read only**” or by using the password utilities an individual application package provides.

In the case of making folder private which is provided by the basic operating system, once a user logged on, he automatically has access to all the folders that have been made private. This makes the users believe that making folders private or changing attributes of files and folders do not provide very reliable security. Making use of password utilities that other application software provides is still not reliable due to the fact that many hackers are used to some of these application software (Tsai *et al.,* 2006).

The basic operating system does not provide the user with monitoring software which will help the user to keep track of all the activities that are taking place on their systems. It also does not provide the user with file splitting functionality which is considered to be a very strong security method for storing archival files. This study is an attempt at addressing the noted issues and presenting the design (Fig 1).

The proposed system has a couple of security related features which enables it to perform the following basic operations.

1. Hide folders from the users, which avoid the user form knowing the existence of that folder and the folder content.
2. Unhide folders, revealing the folder and its content to the user.
3. Change the folder icon to another system icon, which even though the user sees the folder, will not be able to access the content of the folder.
4. Change the folder icon to the usual icon, which now allows the user to access the content of the folder.
5. Encrypt basic text using basic encryption algorithms like DES, RC4.
6. Decrypt the basic text which was previously encrypted by the user.
7. Allow the user to specify a file and a password which will be used to encrypt the specified file.
8. Allow the user to specify a file and password which will be used to decrypt the specified file.
9. Hash basic text using basic hashing algorithms like MD5, SHA.
10. Allow the user to specify a file and password which will be used to Hash the specified file.
11. Allow the user to specify the speed which will be used to perform security operations so as to avoid over using of the processor time.
12. Monitor the user’s computer using keylogger and a camera.

Implementation of the new system: The new security system involved the implementation of various cryptographic schemes which include RC2, RC4, DES, Triple DES, and Triple DES 112 (Menezes *et al.,* 2001). Hashing algorithms implemented include MD2, MD4, MD5, and SHA. The essence of having several algorithms implemented is to give users some flexibility in choosing an appropriate security scheme with which to secure his file. The interface was designed to make it easy to use by every computer

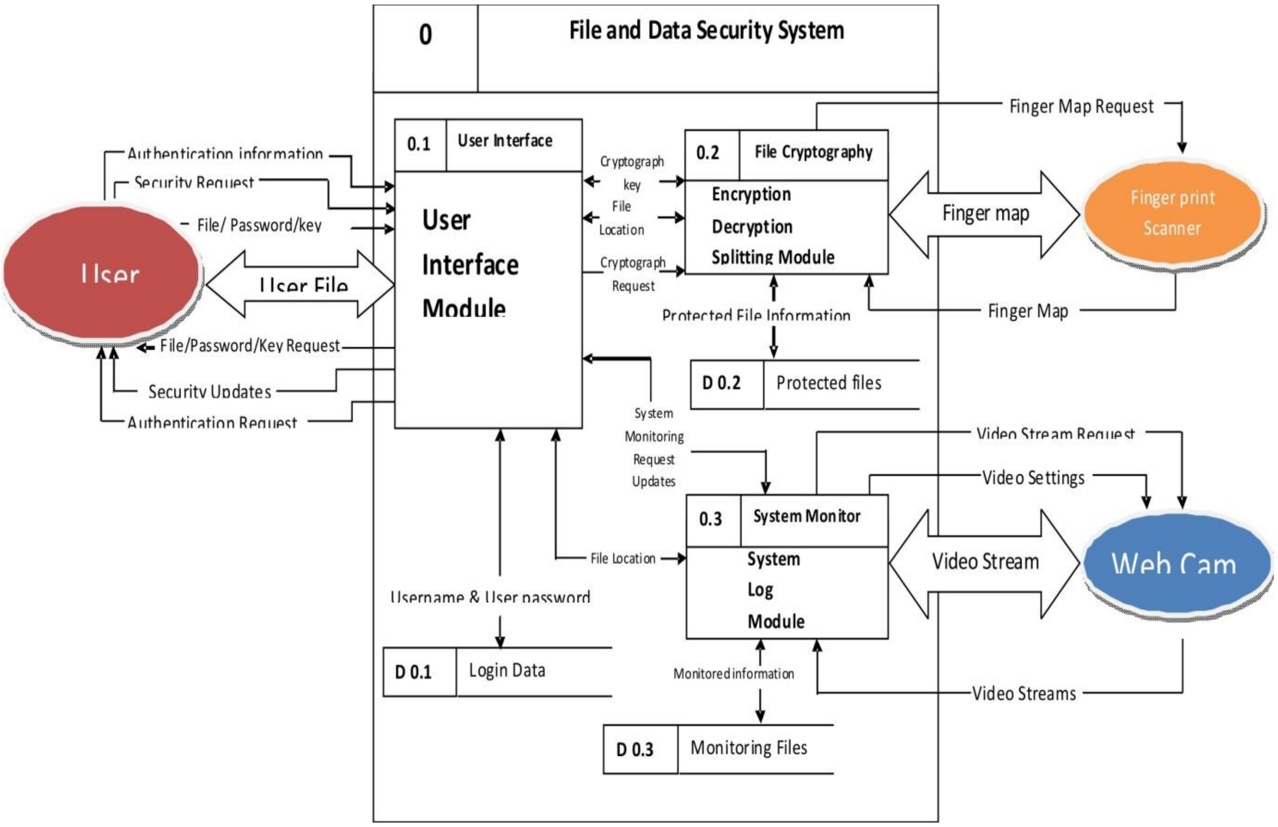
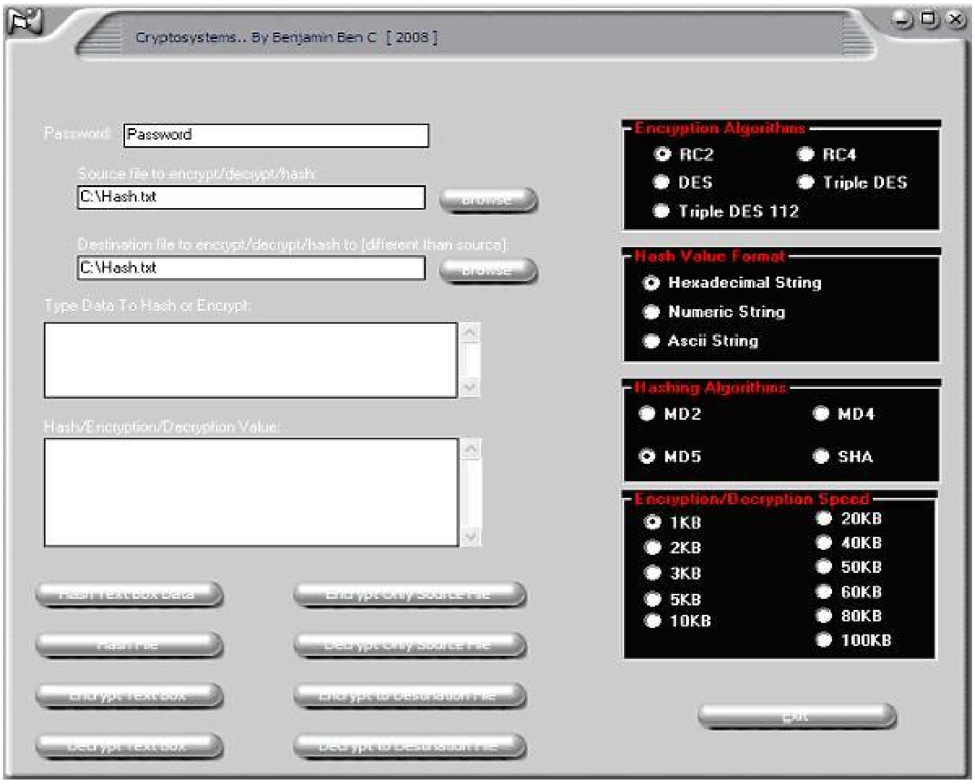


FIG. 1. DATA FLOW DIAGRAM OF THE PROPOSED SYSTEM.


Cryptosystems.. By Benjamin Ben C [2008]

Password: Password

Source file to encrypt/decrypt/hash: C:\Hash.txt

Destination file to encrypt/decrypt/hash to [different than source]: C:\Hash.txt

Type Data To Hash or Encrypt:

Hash/Encryption/Decryption Value:

Encryption Algorithms: ● RC2 ○ RC4 ○ DES ○ Triple DES ○ Triple DES 112

Hash Value Format: ● Hexadecimal String ○ Numeric String ○ Ascii String

Hashing Algorithms: ○ MD2 ○ MD4 ● MD5 ○ SHA

Encryption/Decryption Speed: ● 1KB ○ 2KB ○ 3KB ○ 5KB ○ 10KB ○ 20KB ○ 40KB ○ 50KB ○ 60KB ○ 80KB ○ 100KB

FIG. 2. THE SYSTEM MAIN MENU

Fig. 2 gives the user the following options:

Change login password: This enables the user to change the login password.

Secure Folder by hiding it. This enables the user to secure a folder by making it completely invisible and inaccessible to both the operating system and the general computer users.

Secure Folder by changing folder icon: This enables the user to change the icon of a folder to a reserved system icon like that of a control panel printer and so on. Once a user clicks on the newly changes folder icon, it triggers the equivalent system operation (e.g. popup the control panel page) rather than opening the folder. This allows the general computer users to see the secured folder but does not allow them to access it.

Encrypt/Decrypt File: This option enables the user to specify text data or files that will either be encrypted, decrypted or hashed. It provides the user several configurations for encrypting, decrypting or hashing of text data or files.

Split File: This option enables a user to split up a file into several fragments and a batch file. These file fragments will not be accessible by any user until they are combined back to the original file by the batch file which was produced alongside in the splitting process. This utility is useful to a user who wants to copy a file to another system and the file is larger than the available storage media. The user can split the file up into smaller fragments and transfer them to the other system after which they batch file can be used to combine the file fragments to get the original file.

Start Monitoring Camera: This option enables the user to start the camera monitoring aspect of the software. This captures videos of any detected movements around the users system.

Start Keylogger: This option enables the user to start the key logger utility of the security software application. This keylogger records the entire activity going taking place on the user's computer in a text format with time stamps. It gives the user the option of saving the logged files.

A lot of testing was carried out on the implemented system and several observations were made which showed that the security features of the proposed system are very reliable.

A sample data which contained the text string

"**This is to test the data encrypting feature of the new system**"

was used to test the system. Encryption was applied to this text using RC2 encryption algorithm with hexadecimal hash value format. This yielded a text data:

"**945115510AA674093488BD2852032722C6EEB152445973226BF97BA44E60977C27225582F01DECF96582D50256A1AA7917AF30F33185F5C6F12E69C2DFA183B1**"

From the above we can see that a user who comes across files containing this kind of data will definitely have no understanding of the content of this file.

The above operation took 0.0041 seconds to execute.

A second test was performed on textual data file which original content was

> "**I don't want any one to know about this.**
>
> **I have one million worth of naira in credit card.**
>
> **my credit card number is cc08M3499**
>
> **my password is ilovejesusalways**
>
> **I repeat no one should know this."**

After the encryption was done using Triple DES 112 encryption algorithm with hash value format of hexadecimal string and a password "**Benjamin**", the output was

"**1K————————————————g§.¶¼t×E1–Ü7!Â–^x©m**

————————————————————————

~mì_¢E¹¼ÏŠ*Ý•Ïá,¿(€¼Xa-¹_‡+±Ïgóo*—1h!äÝÎC2z™ä®□J□ˆ¿)‡€6í'Á•R]xâ×2LrI-6õâú‰"H□T§ätÖaŸYš…r‡0Œæ«•_8xÐŸ)ŠQªm1y,êQ□r□□fÍÚGîÖ*§ùIÊE]¬□Ðz□¯‡;ŒQ€œ°ˆ^0cÃ5S°G¢°·¾"

Clearly, it is seen that the encrypted data can not be understood by any user without decrypting the data with the correct password.

The above operation also outputted "Decryption Elapsed time: 0.015625"

The above test also was used to perform encryption over and over and returned successful. This implies that the several security features could be applied to the same data, depending on the user's choice.

REFERENCES

Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. (2001). *Handbook of applied cryptography*. CRC Press Inc.

Syngress, B. A. (2008). *IT Security Project Management Handbook,* Info Security, syngress Publishing

Thawte, M. S. (2008). *Secured Online Data Transfer, The value of Authentication,* Thawte Inc.

Tsai, C., Lee, C. & Hwang, M. (2006). Password Authentication Schemes: Current Status and Key Issues. *International Journal of Network Security*, 3(2):101-115.