A Secure Memo for Mobile Application using Blowfish Encryption Technique

M.S. Suhaimi[1], H. Nahar[1], M. Zulkiflee[1], A. Hassan[1]
[1] Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
haniza@utem.edu.my

Abstract— Nowadays people are looking for a reliable and secure memo mobile application which avoid their data from being stolen. Mostly, people choose to back up their data in cloud storage which later can be accessible anywhere. However, the privacy of the data is at risk as the data also can be accessed by other party. In this study, the main objective is to develop a prototype of secure memo mobile application by applying Blowfish Encryption technique. This application was developed using Android Studio software and the data are stored in an online database called Firebase. The effectiveness of the prototype has been measured by benchmarking three (3) metrics: Response Time for encryption, Response Time for decryption and Memory Usage. Based on our findings, it proves that the system works effectively in terms of provides the fastest Response Time during encryption and decryption process and use only required a small portion in Memory Usage compared to Advanced Encryption Standard (AES) technique.

Index Terms— Secure Memo, Blowfish Encryption, smartphone, Android Studio.

I. Introduction

In the modern lifestyle, people around the world are using a mobile device or known as smartphone that mostly used in daily life which for work, socialize and entertainment. When the development of mobile technology grew up from year to year increase, it become targetable from anonymous to steal the personal information that stored in the mobile devices. Mobile device usually has a typical featured as a computer mechanism which is memory data stored, application and central processing unit (CPU). In the existing application, the data of user stored usually only secure in mobile platform which providing the numeric passcode, strong password and pattern before opening the application.

With the modern technology, commonly people use a digital device rather manual method for keeping the information with instant. Thus, the uses of cyberspace for stored the personal data information are being a normal way without hesitated. In this situation, the number of attacker will rise within on the lack of specific application that commonly used by majority people. Threat by attacker will be alter, stole or eavesdropping the personal data that been stored on the application of user devices without knew about it.

The number of IT professionals saying Android was the riskiest increased and was by far the most frequent platform indicated (64%). Moreover, Apple/iOS followed Android by (16%) and Windows Mobile (16%) and Blackberry (4%). Perception of Android security problems continued to grow theatrically as the platform perceived to have the greatest security risk (up from 49% in 2013 and 30% in 2012) [1].

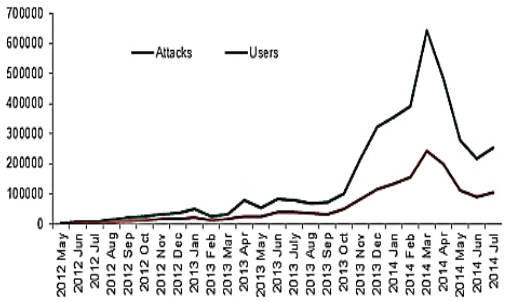

Fig. 1: The relationship between the number of mobile device users and the number of the attacks

Based on Figure 1 shows the survey has taken from May 2012 to July 2014 about the incident that occurs between the number user of mobile devices and attack by unauthorized hacktivists. There are many lack of application development on mobile devices that can be lead into cyber-attack. Normally the attack is concentrate on the data transmitted across the network that being one of vulnerable method for interception between the data that been send. The way to preventive this lack is by develop a security on the application platform being used especially the personal data been stored and transmit on the network.

II. Literature Review

There are three main areas that has been explored: Mobile Application, Encryption Algorithm Techniques and Database Management System. The review has been conducted by referring several resources such as journal, articles, proceeding, technical report and research papers.

The emerging of technology has changed the way of managing people's activities information by using smartphone instead of personal computer. Not only operated as a basic mobile phone, the integration between operating system such as IOS and Android with several features such as video camera, multimedia player, web browsing, multi-touch screen and advanced computing capability leads to the introduction of Mobile Application.

Commonly, the Mobile Application development approach can be classified into three categories namely Web, Native and Hybrid. For Web development approach, the web page must be residing on the server which include a set of HTML, CSS, JavaScript and other related files to fully accessing the web application. It designed according to format of smartphones or tablets. In contrast, the Native development approach has been

developed as an executable binary data that only suitable for one specific mobile operating system and its own devices. Meanwhile, the hybrid development approach combines both Web and Native development approach.

Table I summarizes several features on mobile application. For this study, the Native application has been chosen as the suitable mobile application development where allow programmer to fully access the smartphone features especially Storage and Fingerprint. Besides, it also offers faster processing speed in handling encrypt / decrypt process and offer high advanced graphic which useful for latest design.

TABLE I
Comparison among Mobile Application Development Method

	Web Application	Native Application	Hybrid Application
Features	-Limited	+unrestricted	+unrestricted
Development tools	-Regular support	+Advanced support	+Advanced support (N) -Regular support (W)
Portability	+Portable	-Not portable	-Not portable (N) +Portable (W)
Maintenance	+Unrestricted	-Possibly restricted	-Possibly restricted (N) +Unrestricted (W)
Access to consumers	-Uneducated consumers -limit discoverable	+Discoverable +Large consumer pool	+Discoverable +Large consumer pool
Monetization support	-no integrated billing	+billing through portal	+Billing through portal
Distribution constraints	+free (self-hosting) +freedom	-Revenue share in portal -Portal controls	-Revenue share in portal -Portal controls
Performance	-slow	+Fast	-Slow web component +Fast native component
Look Feel	-inconsistent	+Consistent	-/+ partly standardized
App store	-No	+Yes	+Yes
Example Application	m.facebook.com	Instagram	PayPal

The second important aspect is related to Encryption Algorithm Techniques. According to [2], encryption refers as a technology that guarantee the security of information and maintain the information's confidentiality value by transforming original message to ciphertext. All encryption algorithms can be grouped into two: Symmetric-key (secret-key) and Asymmetric-key (public-key). For Symmetric-key, both encryption and decryption process use similar key meanwhile Asymmetric-key use public key for encryption and a private key for decryption. Generally, the level of security for encryption algorithm is depending on length of key, the initialization vector secrecy of the key and also how they are work together. This overall process of cryptography has been illustrated in Figure 2.

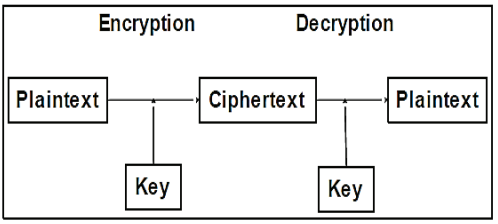

Fig. 2: Cryptography process

Table II depicts the analysis that being conducted to compare four common encryption techniques such as RSA, AES, Blowfish and Twofish.

TABLE II
Analysis on encryption techniques

Encryption Technique Algorithm	Specification parameter					
	Key length (bit)	Round	Block size (bit)	Attack Found	Stage of security	Encryption process speed
RSA	Depends on number of bit in module	1	Variable block size	Brute force attack, timing attack	high	medium
AES	128 192 256	10 12 14	128	Key recovery attack, side channel attack	high	medium
Blowfish	Range of 32-448	16	64	No attack found that successful against blowfish	Very high	Very fast
Twofish	128 192 256	16	128	Differential attack, related key attack	low	fast

Amongst these techniques, the Blowfish has been chosen because it offers the quickest in encryption process which involves small but effectively on key length required that is suitable for mobile application on mobile device. In addition, it does not have any cyber-attack succeed on it. The following Figure 3 represent the block diagram for Blowfish encryption technique.

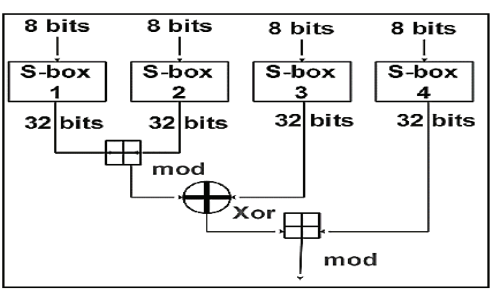

Fig. 3: Blowfish function F encryption technique

For storage purpose, the data management system which used to organize data and store into electronic devices. It can be either Traditional Data services or Cloud Data services [4]. The advantages of Cloud Database services can be explained in term of scalability, elasticity, easy to manage, location dependent and lower initial investment compared to Traditional Data services which becomes limited once number of user getting increased from time to time. In this study, Firebase cloud database has been used.

III. Methodology

For conducting this study, the Waterfall Methodology Model has been chosen. It involves five (5) stages which are Requirements, Design, Implementation, Verification and Maintenance. In the first stage, the objective is more on gathering all information related to the issue on the existing system, identifying the lack of the existing solutions, identifying the hardware and software requirement for developing mobile application and defining the target of users. After analyzing several information, the proposed design has been carried out to overcome the current design problem. The following Figure 4 represents the elements involves in this study.

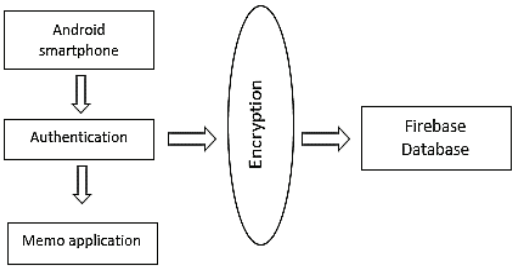

Fig. 4:Proposed Design

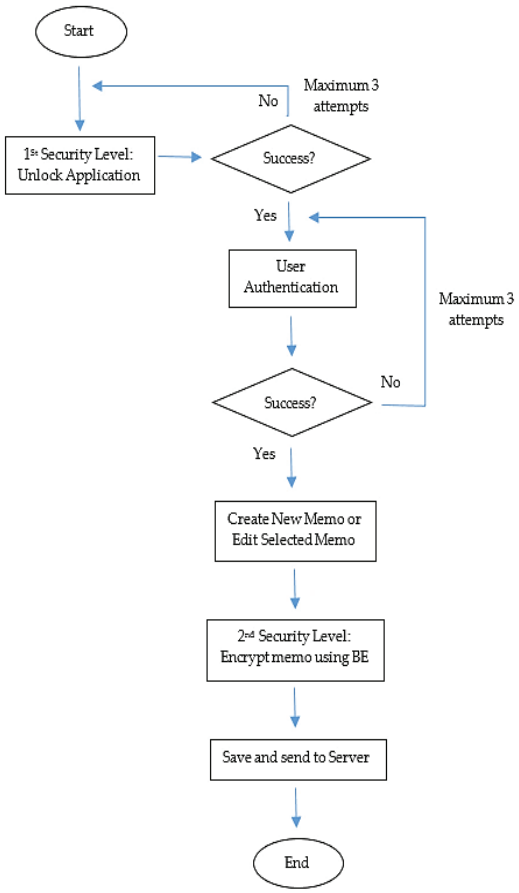

Fig. 5: Flowchart of the proposed system

The implementation has been carried out by installing and configuring the software and hardware which later being integrated with the running prototype. The development of mobile application is based on Java Language for Android application and Firebase as a database. The prototypes system will be tested in order to ensure its integrity, uses and possible lacking before being used by real user. In the last stages, it is responsible to verify and validate the system.

A. Analysis and Design

In this section, the detail information for developing a secure memo mobile application can be described. The following Figure 5 represents the flowchart of the proposed system which begin with application lock security and authentication process. Once user successfully unlock the system, user can create new memo or edit the existing memo. The encryption and decryption process using Blowfish will be applied once user manage memo and then send it to server for storage purpose.

For developing the system, basically it requires Android Studio, Firebase and Smartphone. Android 6.0 (Marshmallow) and personal computer also used at the initial stage for verifying the system implementation before applying on Smartphone. Figure 6 depicts the functionality of the proposed system which are Register User, Create and Display Memo.

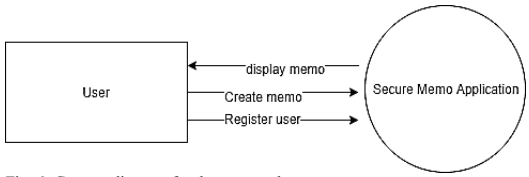

Fig. 6: Context diagram for the proposed system

B. Implementation

For implementation, the process is based on the proposed design that has been explained previously. There are several functions have been defined such as Registration Form, Login Form, Display Memo, Create New Memo, Update Memo, Delete Memo and the important part is Secure Memo. Both Figure 7 and Figure 8 represent all coding that has been developed for this system.

```
if(v==saveButtion){
    String tajuk = Edtitle.getText().toString().trim();
    String desc =Eddesc.getText().toString().trim();
    if(tajuk.isEmpty()){
        Toast.makeText(MemoActivity.this,"Don't leave Title
empty!",Toast.LENGTH_LONG).show();
    }else if(desc.isEmpty()){
        Toast.makeText(MemoActivity.this,"Don't leave description
empty!",Toast.LENGTH_LONG).show();
    }else if(!tajuk.isEmpty() && !desc.isEmpty()){
        Memo m = new Memo();
        m.setTitle(tajuk);
        m.setDescription(desc);
        m.setUserId(auth.getCurrentUser().getUid());
        m.setNoteId(newNoteRef.getId());

        newNoteRef.set(m).addOnCompleteListener(new
OnCompleteListener<Void>() {
            @Override
            public void onComplete(@NonNull Task<Void> task) {
                if(task.isSuccessful()){
                    Toast.makeText(MemoActivity.this,"Created new
Memo!",Toast.LENGTH_LONG).show();
                    Edtitle.setText("");
                    Eddesc.setText("");
                }else{

Toast.makeText(MemoActivity.this,"Failed!",Toast.LENGTH_LONG).show();
                }
            }
        });
    }
}
```

Fig. 7: Coding for Creating New Memo

```
public static String encrypt(String encryptData, String
keyEncrypt) throws NoSuchPaddingException,
NoSuchAlgorithmException, InvalidKeyException,
BadPaddingException, IllegalBlockSizeException {
    byte[] keyData = (keyEncrypt).getBytes();
    SecretKeySpec secretKeySpec = new SecretKeySpec(keyData,
"Blowfish");
    Cipher cipher = Cipher.getInstance("Blowfish");
    cipher.init(Cipher.ENCRYPT_MODE,secretKeySpec);
    byte [] hasil = cipher.doFinal(encryptData.getBytes());
    String strData = new BASE64Encoder().encode(hasil);


    return strData;


}
public static String decrypt(String encryptCode, String
keyDecrypt) throws NoSuchPaddingException,
NoSuchAlgorithmException, InvalidKeyException, IOException,
BadPaddingException, IllegalBlockSizeException {
    byte[] keyData = (keyDecrypt).getBytes();
    SecretKeySpec secretKeySpec = new SecretKeySpec(keyData,
"Blowfish");
    Cipher cipher = Cipher.getInstance("Blowfish");
    cipher.init(Cipher.DECRYPT_MODE,secretKeySpec);
    byte [] hasil = cipher.doFinal(new
BASE64Decoder().decodeBuffer(encryptCode));
    String strData = new String(hasil);
    return strData;
}
```

Fig. 8: Coding for Securing Memo using Blowfish Encryption Technique

III. Results and Discussion

The software testing has been conducted to determine the efficiency of security level between the prototype application and the existing systems. The requirement of test environment includes Smartphone, the prototype secure memo application and stopwatch to record the time response of encryption and decryption process involved. Several types of test have been performed such as Unit Testing, Integration Testing, System Testing and Acceptance Testing. Each test brings different aims and results.

Figure 9 shows the Login interface and its error handling when the process of logging is incomplete. Figure 10 shows the New Memo interface with and without error issue. Meanwhile, Figure 11 illustrates the example of encrypted memo and memo without encryption.

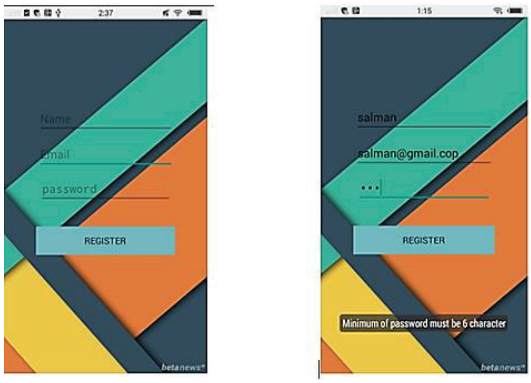

Fig. 9: Interface for Login and Error handling for incomplete Login activity

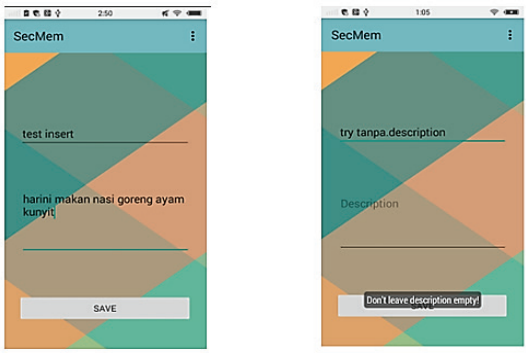

Fig. 10: Interface for Create New Memo and Error handling for incomplete Memo activity

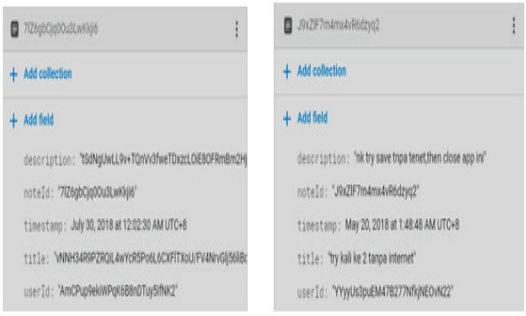

Fig. 11: Encrypted memo vs. Non-encrypted memo

Figure 12 until 15 illustrates the comparison amongst five (5) types of encryption techniques in several studies [5]. They focus on the duration time taken for processing data encryption on varies size of data in range of 25 KB up to 3 MB. Indeed, it clearly seen that Blowfish and Advance Encryption Standard (AES) are suitable to be studied where they require very lesser time when compares to others. In this study, the measurement for comparing between secure memo using Blowfish and AES has been determined based on Response Time for Encryption and Decryption process and Memory Usage involves during encryption.

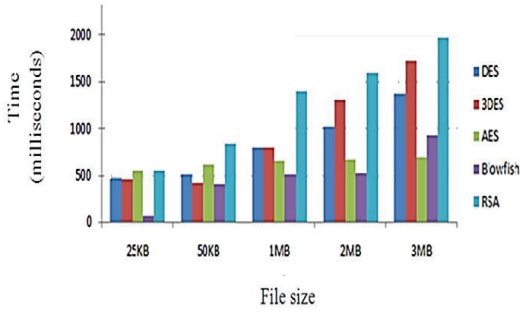

Fig. 12: Duration time taken amongst several Encryption Techniques

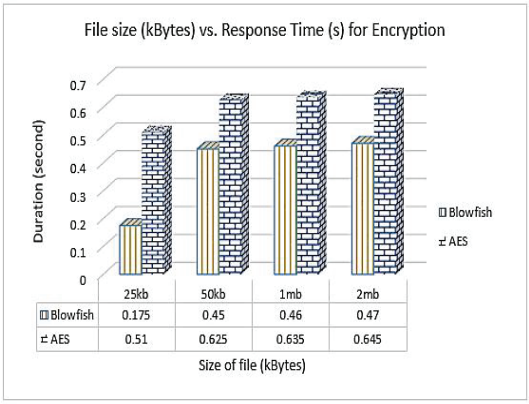

Fig. 13: Response Time for Encryption process

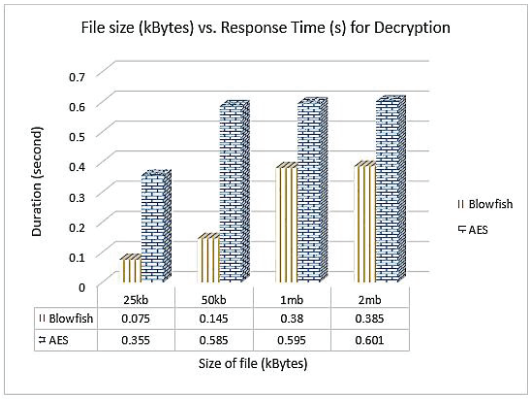

Fig. 14: Response time for Decryption process

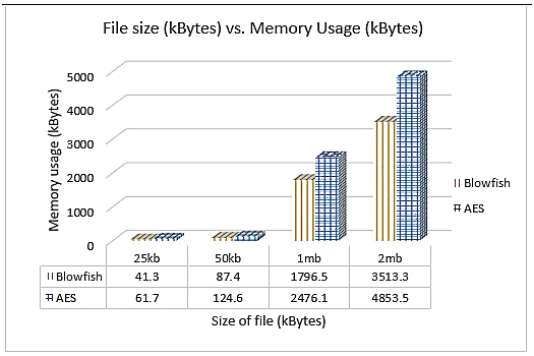

Fig. 15: Memory usage for Encryption and Decryption process

IV. Conclusion

The prototype of Secure Memo Mobile Application using Blowfish Encryption techniques has been successfully developed. This prototype help user to store their data into cloud database as a backup if any case happens to mobile phone. By applying Blowfish encryption over stored data, it provides more secure environment and enhanced data confidentiality if it is being stolen. The benchmarking process shows that the prototype offers faster Response Time during encryption and decryption process and more effective in term of system disk's Memory Usage compared to Advanced Encryption Standard (AES). This concept also can be expanded to solve any other issues which requires data confidentiality solutions.

Acknowledgment

The authors would like to thank INSFORNET, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka for giving opportunity and equipment to conduct this study.

References

[1] M. Sardasht, M. Bakhtiar and M. Rebwar M, "Mobile Application Security Platforms Survey". International Journal of Computer Applications, vol. 133, no. 2, pp. 40–46, 2016. Available at: https://doi.org/10.5120/ijca2016907736.

[2] G. Singh, A. Kumar, and K.S. Sandha, "A Study of New Trends in Blowfish Algorithm", International Journal of Engineering Research and Application (IJERA), vol. 1 Issue 2, pp. 321–326, 2013.

[3] J. Thakur, and N. Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering (IJETAE), vol. 1 Issue 2, pp. 6–12, 2013.

[4] S. Jain S, M.A. Alam, "Comparative Study of Traditional Database and Cloud Computing Database", International Journal of Advanced Research in Computer Science, vol. 8 Issue 2, pp. 80–87, 2017.

[5] Y. Mahamat, S.H. Othman, M.M. Siraj and H. Nkiama, "Comparative Study of AES, Blowfish, CAST-128 And DES Encryption Algorithm", International Organization of Scientific Research International of Engineering (IOSRJEN), vol. 6 Issue 6, pp. 1–7, 2016.

Ts.Haniza Nahar, a Senior Lecturer at University of Technical Malaysia Melaka (UTeM). She earned MSc. in ICT for Engineers (Distinction) from Coventry University, UK and BEng. in Telecommunication from University Malaya. She used to be an Engineer and has been qualified for CFOT and IPv6 Software Engineer. Her postgraduate dissertation has been awarded as the ***Best Project Prize***.

Ts. Dr. Zulkiflee Muslim, a Senior Lecturer at University of Technical Malaysia Melaka (UTeM). He earned MSc. in Data Communication and Software from University of Birmingham City, UK and BSc. in Computer Science from University of Technology Malaysia. He has professional certifications: CCNA, CCAI, CFOT and IPv6 Network Engineer Certified.

Muhammad Salman Suhaimi, a final year Computer Networking student at Faculty Information and Communication Technology, University of Technical Malaysia Melaka (UTeM).

Ts. Dr. Aslinda Hassan received her PhD degree in Electrical Engineering, from Memorial University of Newfoundland, St. John's, NL, Canada in 2014. She received M.Sc. degree in Computer Science, from Universiti Teknologi Malaysia (UTM) and B.Sc. degree in Business Administration with honors, from University of Pittsburgh, Pittsburgh, PA, USA in 2001 and 1999, respectively. In 2004, she joined Universiti Teknikal Malaysia Melaka, where she is currently a Senior Lecturer at Faculty of Information and Communication Technology. Her research interests include in vehicular ad hoc network, vehicular communication, wireless ad-hoc network, wireless sensor network, wireless communication, ad hoc routing protocols, cyber-physical systems (CPS), Internet of Things (IoT), network performance modelling and analysis as well as network programming interfaces. Currently, Dr. Aslinda serves as the head of Information Security, Digital Forensic and Computer Networking (INSFORNET) Research Group.