American Journal of Computer Science and Technology
2020; 3(1): 1-6
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20200301.11
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Blowfish Implementation on SoloEncrypt Security Model for User Data Protection Prior to Cloud Storage

Olaleye Solomon Babatunde

Department of Computer Science, Federal College of Education (Special), Oyo, Nigeria

Email address:
olaleye3@yahoo.com

To cite this article:
Olaleye Solomon Babatunde. Blowfish Implementation on SoloEncrypt Security Model for User Data Protection Prior to Cloud Storage. *American Journal of Computer Science and Technology*. Vol. 3, No. 1, 2020, pp. 1-6. doi: 10.11648/j.ajcst.20200301.11

Received: October 8, 2019; **Accepted**: October 29, 2019; **Published**: March 17, 2020

Abstract: Smartphones' data security has become increasingly important in the advancement of mobile technologies. Users today use smartphones as means of communication, sending and receiving messages, browsing the internet as well as storing sensitive information. Due to these functionalities smartphones today are preferred targets of attacks. Hence, the foremost goal of this work is to provide security for user data on smartphones by the implementation of Blowfish encryption algorithm prior to cloud storage. Blowfish encryption algorithm is a popular and well tested cryptographic algorithm to provide security for user data in mobile cloud computing. Further, there is the need for the development of a mobile application to provide the needed security on smartphones using this existing algorithm. This paper therefore proposed a Secure App using java + xml which was implemented on SoloEncrypt security model. Three Android devices were used to carry out the experiment; Samsung Galaxy On7 Prime, Samsung Galaxy J2 Pro and Samsung Galaxy J7 Nxt. Encryption time and decryption time were parameters used for evaluating the encryption algorithm which are among the standardized metrics approved by the National Institute of Standards and Technology (NIST). The experimental results revealed that the algorithm encrypts with better speed and it takes less time to decrypt when compared with related work.

Keywords: Blowfish, SoloEncrypt, Data Security, Cloud Storage, Smartphones

1. Introduction

Smartphone is a phone that is smart enough to provide all the facilities to consumer which laptop and personal computer provide [1]. It is a mobile phone with more advanced features and greater computing capacity such as touch technology, web browsing, fast and increased storage, many applications which can be downloaded from internet, camera, scanning, e-mail and so on. With all these facilities, smartphones also have risks of security for data and financial transaction done through internet. From the security point of view, cloud [2] can also be used to store the confidential data of mobile user so that mobile phone will not be vulnerable to the mobile user and also user can access that data through their smartphone. This approach needs the combination of mobile computing and cloud computing which is called mobile cloud computing [3]. There are risks associated with smartphones which are data leakage, phishing attacks, unintentional disclosure of data etc.

Securing data in mobile cloud have become more important in the recent days because of increasing usage of mobile devices with internet. In [4] it was reported that the smartphones are in the top of the invention list as they are built on a mobile Operating System (OS), which is capable for advanced computing and faster in connectivity than ordinary mobile phones. Smartphones are famous for malicious code. There are many chances to lose or steal the data because mobile devices are mostly unprotected. An unauthorized person can easily access the information stored on the mobile devices. As stated in [4] the following are top mobile threats that affect security of mobile devices:

1. Data loss from lost/ stolen devices.
2. Information stealing by mobile malware.
3. Data leakage through poorly written third party applications.
4. Vulnerabilities within devices, OS, design and third-party applications.
5. Insecure network access and unreliable access points.

Smartphones have emerged as a type of mobile device providing “all-in-one” convenience by integrating traditional

mobile phone functionality and the functionality of handheld computers [5]. Various models of smartphones have been released catering for the various demands of mobile users. Today smartphones offer PC-like functionality to end-users allowing them to check their e-mail, maintain calendars, browse the internet, watch videos, play music, etc. In addition to these functions, they are also used for private sensitive tasks such as on-line-banking that makes them an attractive platform for attackers [6]. The storing of personal data on the smartphone has become a common practice. Awareness of the risks associated with smartphone usage is relatively low when compared to the awareness of risks for desktop computers. Sensitive data such as email and bank passwords are frequently stored by users in an unsafe manner on their smartphones. These poor security practices attract attackers to concentrate on smartphone platforms in order to exploit the vulnerabilities of the smartphone OSs and application software, as well as user generated vulnerabilities. Therefore, there is a growing need to address the security risks associated with smartphones.

The main objective of this work is to provide security for user data on smartphone using blowfish encryption algorithm on SoloEncrypt security model [7]. Further, the user data will be stored in the cloud in encrypted form and can be accessed by user by supplying appropriate credentials (Personal Identification Number (PIN)) whenever needed. In addition, the research work is evaluated using time performance metrics.

2. Related Work

A lot of researches have been carried out on securing users' data on smartphones using different methodologies. Some are discussed here, [8] worked on secure storage of data on Android based devices. They reported that the key components required for data protection are; the data to be secured and the security key used for encrypting the data. The encrypted data can only be readable if the security key is known, so there is a need to store the security key on the device or generate the security key on the fly with the password provided. Storing the keys on the device pose a threat of data compromise if the key is stolen and it is always recommended to generate the security key from the password as per the standard Password Based Encryption Standard.

Federal IT Market Forecast [9] suggested that Offloading computation from resource constrained devices has been an area of focus for researchers. Security functions such as anti-virus scanning are resource intensive and additionally the computation and associated memory activity will deplete the battery power of the smartphone. Cloud computing seems to be a good fit by shifting the computation from the mobile devices to the cloud, hence exploiting the computational power of the cloud and the fact that the cloud computers are provided with mains power. Cloud computing has emerged as a new computing paradigm providing hosted services by exploiting the concept of dynamically scalable and shared resources accessible over the internet. A cloud service is rented on demand, i.e. based on the customer's current requirements. Because the cloud provider can dynamically allocate virtual processors to their customers, cloud computing is highly scalable, hence the user can have as much or as little service as he or she wants at any given time. Depending on the type of the cloud service rented, the responsibility of the user in managing the service varies. A well secured system should provide confidentiality, integrity, availability, and accountability.

In a research paper [10], it was explained that smartphones are used to download free Android applications, which bring much fun and convenience to their life. Convenience results in the fact that more people tend to store their privacy information in their phones. However, privacy information means a lot to the users, compared with how much the phone costs. If privacy information is used by malicious attackers, such as contact information, Short Message Service (SMS), and data on storage card, the consequence would be unpredictable.

Android provides the following security features to achieve security objectives;

i. Security at the operating system level through the Linux kernel,
ii. Compulsory application sandbox for all applications,
iii. Application defined permission and user have to grant permissions [11].

Android is not fully secured as it appears, even when such robust security measures are in place. According to [11], there are several security problems faced by android users, some of them are:

i. Android has no security scan over the applications being uploaded on its market.
ii. There are some applications which can exploit the services of another application without permission request.
iii. Android's permission security model provides power to user to make a decision whether an application should be trusted or not. This human power introduces a lot of risk in Android system.
iv. The Open Source is available to legitimate developers as well as hackers too. Thus the Android framework cannot be trusted when it comes to develop critical systems.
v. The Android operating system developers clearly state that they are not responsible for the security of external storage.

In every cloud environment [15], user authentication and security of data are major challenging issues. Consequently, an efficient and scalable access control scheme was proposed by the authors. It was reported that a blowfish hybridized weight attribute-based encryption mechanism could provide data security in cloud environment. In view of this discussion, security of user data is seen as one of the main concerns for smartphones users today. As the power and features of smartphones increase, so has their vulnerability for attacks by viruses, threats etc. especially when connected to the Internet.

3. Description of SoloEncrypy Security Model

The SoloEncrypt security model is presented in Figure 1. It is divided into three sections; the user side, the service provider and cloud environment. There are various levels of security in the model, security at the user side, security at the service provider's side and security in the cloud. The focus of this work is to provide security at the user side. Security at the service provider's side is done through the firewall while at the cloud providers side there are many policies and privacy being adopted based on the cloud provider as well as the country where it is located [7].

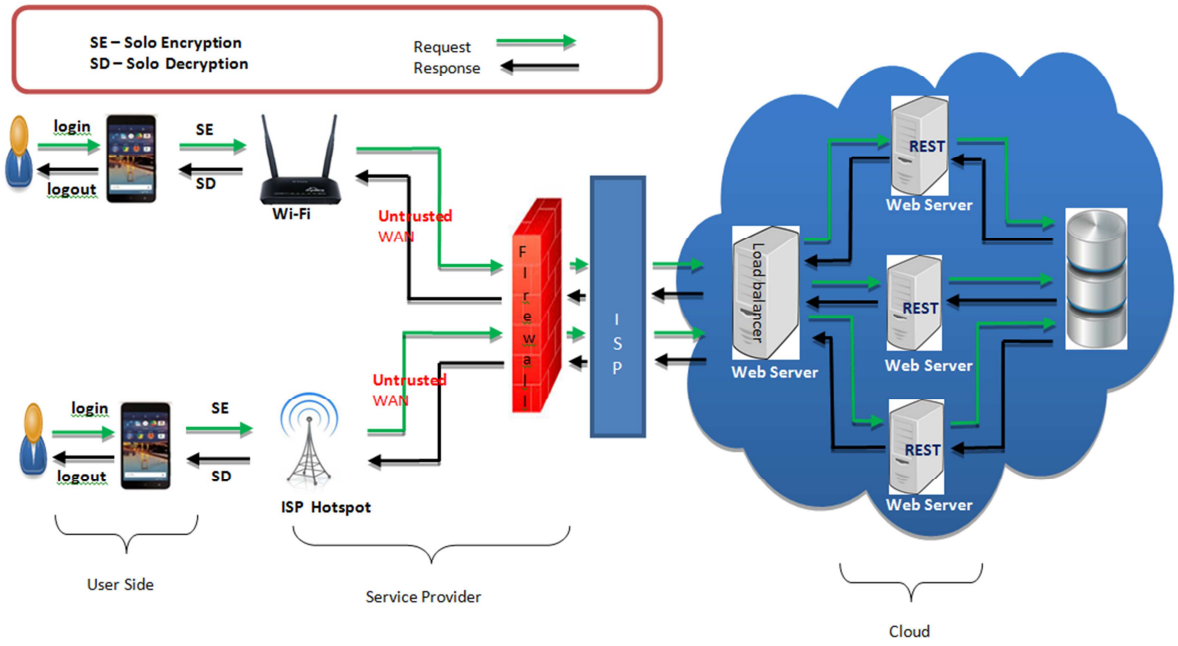

Figure 1. *SoloEncrypt security model [7].*

3.1. User

The user is the owner of any smartphone who uses his/her smartphone to carry out calls, SMS, email, internet browsing and many more. The smartphone can be connected to the internet either through wi-fi (wireless fidelity) or internet service provider like MTN, Airtel, Glo etc. The user when connected uses a medium that is not secure because connecting the internet makes the user prone to attacks. This research work focuses on providing security for user data at the point of generating the data and ensures its encryption at this point before sending to cloud.

3.2. Service Provider

The service provider ensures availability of constant connectivity to the internet. This is achieved either by wireless fidelity or internet service provider. However, the service provider makes use of firewall to provide security at its own level. The service provider can allow or deny the user access to some services by means of the firewall. But user data to and fro the service provider is not protected by them, they only allow user accessibility.

3.3. Cloud Environment

The cloud environment provides unlimited resources to its users based on demand. Smartphones users can avail themselves of the benefit of cloud storage. There are many cloud providers today, among are Amazon Web Service, VMware, Microsoft Azure, Red Hat, Google Cloud, IBM cloud etc.

According to [12] some security risks that should be considered before opting for cloud services are;

1. Client should spend some time to know about the cloud service providers from whom services can be taken and emphasis on their regulations before taking any trivial service from them.
2. Client should be accountable for the security of their data.
3. Cloud service providers made some contracts according to which client will not get any idea about where their data is being located or stored under which country and jurisdiction.
4. Cloud service providers should have the provision to recover client's data from disaster and store it in safe place.
5. If Client sense any fraud activity from the Cloud service provider side investigation process should be started immediately taking no longer time.

4. Blowfish

Blowfish is a 64 bit block cipher with variable length key [13]. It is commonly used in software applications. Blowfish can resist many attacks. It is an encryption algorithm used in known public domain provided by Bruce Schneier (a leading cryptologist). It is on record as one of the fastest block

ciphers although slow in use with some applications. Its variable length key ranges from 32 to 448 bits. It is not patent, license free and can be used by all for free [14].

5. Experimental Design

5.1. Evaluation Parameters

Secure App named MyStorage (Figure 2) was developed to evaluate the performance of the SoloEncrypt security model, 3 Android devices of different configurations were used. They are Samsung Galaxy On7 Prime, Samsung Galaxy J2 Pro and Samsung Galaxy J7 Nxt. Table 1 shows the detail configurations of the devices while the snapshots of some of the user interfaces are showed in Figure 2 and Figure 3. The encryption time and decryption time are used as evaluation parameters. They are among National Institute of Standards and Technology (NIST) standardized metrics for evaluating an encryption algorithm.

Table 1. *Configurations of Devices.*

	Mobile Devices		
	Samsung Galaxy On7 Prime	**Samsung Galaxy J2 Pro**	**Samsung Galaxy J7 Nxt**
OS	Android v 6.0.1 (Marshmallow)	Android v6.0.1 (Marshmallow)	Android v6.0.1 (Marshmallow)
CPU	Quad-core 1.2 GHz	Hexa-core - 2x1.8 GHz	Octa-core 2.0 GHz
RAM	4 GB	2 GB	3 GB
Internal Storage	64 GB	16 GB	16 GB

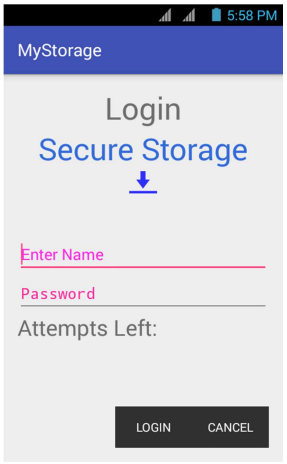

Figure 2. *User interface for secure app.*

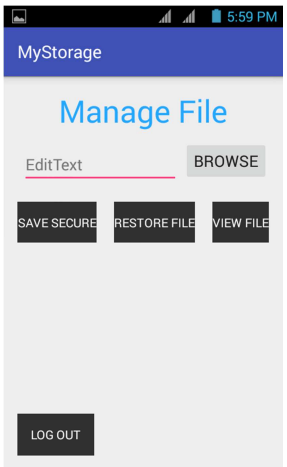

Figure 3. *User interface to manage files.*

5.2. Evaluation Criterion

The performance metrics are encryption time (milliseconds) and decryption time (milliseconds).

Encryption Time: It is the time that an encryption algorithm takes to produce a cipher text from a plain text.

Decryption Time: It is the time that an encryption algorithm takes to produce a plain text from a cipher text.

6. Experimental Results

The experimental results are presented based on each of the three devices used for the experiment in Figure 4, Figure 5 and Figure 6. As a precautionary measure to reduce errors and ensures accuracy, each file size was repeated 3 times and the average time was recorded against the file size for each encryption and decryption.

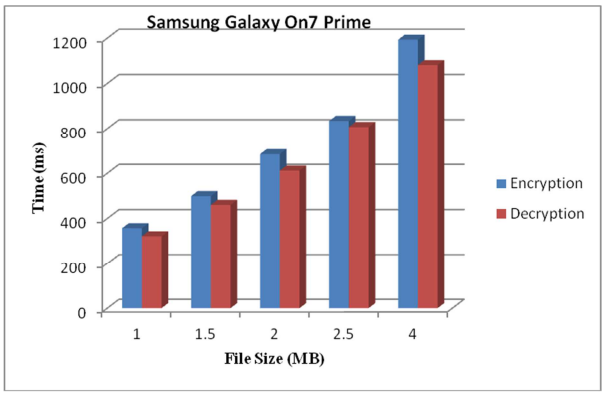

Figure 4. *Experimental results on Samsung Galaxy On7 Prime.*

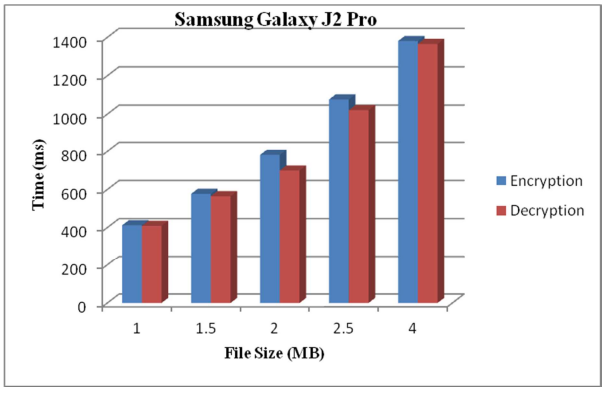

Figure 5. *Experimental results on Samsung Galaxy J2 Pro.*

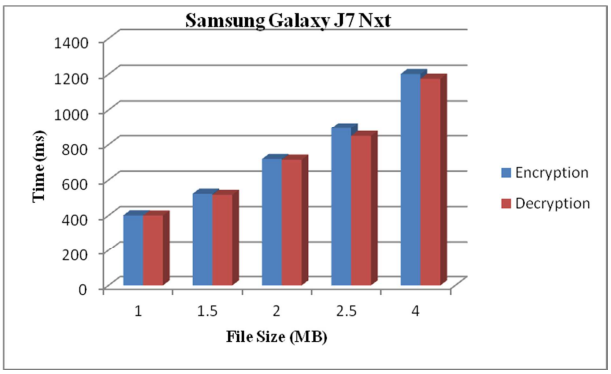

Figure 6. *Experimental results on Samsung Galaxy J7 Nxt.*

7. Discussion

Smartphones are commonly used computing and communication devices today. They are used for personal use as well as for business transactions. Mobile users are using their devices to store all types of data including sensitive data in an unsecure manner. But smartphones have limitations in terms of storage space and security. The concern of this work is to secure data on smartphones by using cloud infrastructure. The implementation was done using a mobile application named Secure App, which was developed using Android Studio 2.2.3. Secure App uses Blowfish as an encryption algorithm. The experimental results revealed that the algorithm encrypts with better speed and it takes less time to decrypt. For Samsung Galaxy On7 Prime, it takes 1193 milliseconds (ms) to encrypt 4 MB of data while it takes 1081 ms to decrypt the same data. While on Samsung Galaxy J2 Pro, it takes 1381 ms to encrypt 4 MB of data and takes 1366 ms to decrypt the same data. For Samsung Galaxy J7 Nxt, it takes 1202 ms to encrypt 4 MB of data and 1175 ms to decrypt. The differences in encryption and decryption times were based on the differences in each device's configuration. Therefore, the encryption time and decryption time for each file size were found reasonable when compared with earlier works of [8, 15] results, for 5MB file, encryption time taken was around 8.3sec. The same file on dual core mobile it took 5.78sec and on 1GB RAM and quad core device it took less than 2 sec.

8. Conclusion

8.1. Concluding Statements

This work has discussed security issues as related to smartphones and cloud storage. It has shown that smartphones are increasingly becoming a target of security threats. There are unlimited storage facilities in the cloud however the major challenge is security which this work addressed. In order to protect user data Blowfish encryption algorithm was proposed for encrypting user data prior to cloud storage. To achieve this, Secure App was developed which resides on user smartphone. It can be used to encrypt and decrypt user data. Three Android devices were used to carry out the experiment and time performance metrics were used for evaluation. The results were encouraging. However, for future work, the Secure App will be fully developed and placed on Google Play Store for wide usage by Android users and a well-known cloud will be used to store the user encrypted data.

8.2. Recommendations

It is recommended that:

1. Other cryptographic encryption algorithms be developed and tested on smartphones.
2. Internet connectivity is upgraded to 4G all over Nigeria to enable proper use of the developed Secure App.
3. Encryption and decryption were used for evaluation; there is the need to use more evaluation techniques.

Acknowledgements

This research work is fully sponsored by Tertiary Education Trust Fund (TETFund), Nigeria.

References

[1] Bhavya, S., Sugandha, S. & Mayank, A. (2014). Securing smartphone data by offloading computation on cloud. *International Journal of Emerging Technology and Advanced Engineering,* Vol. 4, No. 7, pp. 949-958.

[2] Ramgovind, S, Eloff, M. M. & Smith, E. (2014). The management of security in cloud computing, Unpublished MSc Thesis, School of Computing, University of South Africa, Pretoria, South Africa.

[3] Niroshinie, F., Seng, W. L. & Wenny, R. (2012). Mobile cloud computing: A survey. *Elsevier*. www.elsevier.com/locate/fgcs, pp. 85-106.

[4] Donald, A. C., Oli, S. A. & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Engineering and Innovative Technology*, Vol. 3, No. 1, pp. 401-406.

[5] Ria, D. & Indrajit, D. (2013). Smartphone security by cloud computing. *International Journal of Innovations in Engineering and Technology*, Vol. 2, Issue 3, pp. 122-130.

[6] Cisco (2010). Annual security report. http://www.cisco.com/en/us/prod/collateral/vpndevc/security_annual_report_2010.pdf. Accessed 27th August 2019.

[7] Olaleye, S. B., Ranjan, I. & Ojha, S. K. (2017). SoloEncrypt: A smartphone storage enhancement security model for securing users sensitive data. *Indian Journal of Science and Technology,* Vol. 10, Issue 8, pp. 1-8.

[8] Poonguzhali, P., Dhanokar, P., Chaithanya, M. K. & Patil, M. U. (2016). Secure storage of data on android based devices. *International Journal of Engineering and Technology,* Vol. 8, No. 3, pp. 177-182.

[9] Federal IT Market Forecast 2011 – 2015, U. S. (2010). Market research media, September 2010 update, Accessed 24th August 2019.

[10] Weizhe, Z., Hui, H., Qizhen, Z. & Tai-hoon, K. (2014). Phone protector: Protecting user privacy on the Android-based mobile platform. *International Journal of Institute of Distributed Sensor Networks*, 2014, pp. 1-10.

[11] Tiwari, M., Srivastava, A. K. & Gupta, N. (2013). Review on android and smartphone security. *Research Journal of Computer and Information Technology Sciences*, Vol. 1, No. 6, pp. 12- 19.

[12] Brodkin, J. (2009). Gartner: Seven cloud computing security risks. http://www. infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853. Accessed 13th August 2019.

[13] Gonsai, A. M. & Raval, L. M. (2014). Evaluation of common encryption algorithm and scope of advanced algorithm for simulated wireless network. *International Journal of computer Trends and Technology (IJCTT),* pp. 7-12.

[14] Elminaam, D. S. A., Kader, H. M. A. & Hadhoud, M. M. (2012). Performance evaluation of symmetric encryption algorithms. *A publication of International Business Information Management Association (IBIMA)*, Vol. 8, pp. 58-64.

[15] Ghosh, S. & Karar, V. (2018). Blowfish Hybridized Weighted Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing. *Applied Science,* 2018, 8, 1119, pp. 11-15.