Augmenting Android Sqlite Database by Encryption to Cloud with Reference to Binomial Distribution

Olaleye Solomon Babatunde
Department of Computer Science
Federal College of Education (Special), Oyo, Nigeria
olaleye3@yahoo.com

Abstract:
Smartphones now have become most important part of human lifestyle. Our dressing is not complete without at least one. Android out of the numerous types of smartphones are the most widely used. It gains this popularity due to its features and functionalities. The focus of this paper is to educate users on how to augment Android SQLite database user data by encryption to cloud storage. Android uses SQLite database for storing data. Due to connectivity to the Internet, there are numerous threats to mobile phones which have made the issue of security of data on smartphones very critical. However, the biggest challenge is data security. This work therefore addresses the issues of security of data on Android SQLite database by using cloud storage with the use of Advanced Encryption Standard (AES) for encryption of data. This enables user data to remain secure either at rest or in transit. Further, binomial distribution was used to compute the probability of selecting the best agent (cloud server) that is the probability of the success rate of the agent (cloud server). Amazon EC2 was used for cloud storage and a mobile application was developed for proper extraction of data and encryption to cloud storage. The application was evaluated using encryption time and decryption time as performance metrics. The study results werecompared with existing similar works and were found better.

Keywords:data encryption; Sqlite database; smartphone security; cloud storage; AES

1. Introduction

Smartphones have become integral part of our day to day life because they are used in keeping in touch with families, friends, businesses, Internet accessing and many other activities [19],[14],[24]. They are equipped with several technologies such as rapid processors, battery and storage. Android is the recent trend in this series which familiarity is spreading all over the world. It has numerous tools which supports developers of application to embed different characteristics in applications.

However, as the usage increases, storage space is not enough for all applications because of data being generated. Also, as more mobile applications increase, mobile applications' size also increases. There are plenty of mobile applications having attractive features that can be downloaded from Google Play Store for personal use. Hence, as the mobile applications performing on smartphone are getting more complex, the storage system tends to be the bottleneck of performance [16].

This shows that smartphones have limitations in certain areas such as their screen, battery life, storage space, security of data among others [2],[23]. Its screen can easily crack once it falls down. Battery life goes down quickly with usage especially when doing intensive computation, storage space is not always enough because the Operating System (OS) and other system software would have taken a lot of storage spaces and also user downloaded applications.

The growth of smartphones use has resulted in increased volume of sensitive data stored on them, which needs to be secured from undesired access. There exist methods of data protection on mobile devices to assist users secure their data. These include Personal Identification Number (PIN), pattern lock, passwords, biometrics and others. These existing methods have usability and security issues which made them not to fully secure user data. PINs and passwords may be difficult to remember for some users, pattern lock is vulnerable to smudge attacks and biometrics has high false rejection rates. Hence, there is the need for novel authentication system because there is no perfect user authentication system [18],[4],[5].

Further, with increased dependency on smartphones, comes increased need to improve performance and storage along with upgrading the security systems. Mobile companies today are continuously devising new models to meet customers' demands and maintain their market share. Smartphone appliances are highly being used as the major device of computing for more performance - intensive activities than imagined previously.

Storage has not been regarded as a critical component of tablets, smartphones and Personal Digital Assistants (PDA) at least in performance terms [7]. The performance of storage on mobile appliances is essential for experience of end user nowadays and its effect is expected to grow due to several reasons, the main among them being the development of wireless standard such as 802.11a and 802.11n which provide the importance for essentially greater throughput of network to mobile appliances [9]. As an outcome, the access to benefits of many cloud services from a split of functionality between the device and cloud places a huge burden on local resources involving storage [13]. Considering these problems, developers are increasingly focusing on the issues of storage, especially in regard to providing better security [15],[26].

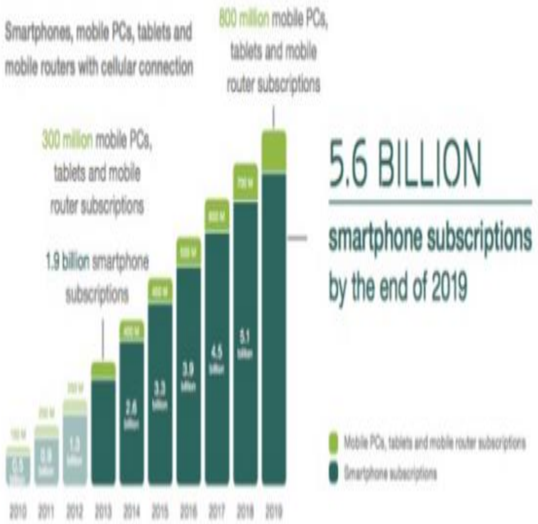

Fig. 1. Adoption of smartphone for global penetration [27]

The usage of smartphone has grown rapidly, owing to low costs of devices and internet services. Tablets and smartphones are now becoming a familiar replacement for laptops as they offer the same services at the same speed with increased ease. Figure 1 shows the adoption of smartphones at the rate of increase of usage. By the year 2013 there were about 1.9 billion smartphones subscriptions while it was also estimated that by year 2019 there would have been about 5.6 billion smartphone subscriptions. This shows that as the world population increases smartphone subscription increases [27].

Consequently, storage's energy overhead and background applications namely instant messaging, email, synchronization of file, updates for operating system, applications and some OS services like bookkeeping and logging can often be storage intensive [6]. Storage influences the performance of applications in unexpected ways that are traditionally thought of as network bound or Central Processing Unit (CPU) related [12]. Although smartphones have a less capacity of storage than personal computers, they make it feasible for users on the go to access online by different channels. As an outcome, there is a strong tendency to use data that are stored in the cloud. There is hence a developing trend towards accessing the cloud from smartphones using web applications [3].

This work covers security issues for protecting sensitive data on smartphones using Amazon cloud services. The use of binomial distribution was used for optimal locations of cloud servers. Relevant recent research papers were discussed to understand current trends on the research. The various security mechanisms adopted in the past were studied which gave better understanding of the work. From the security point of view, cloud [22] can also be used to store the confidential data of mobile sets so that smartphones will not be vulnerable to the mobile users and also, they can access data through their smartphones. In this work, smartphone data are enhanced on the user side by designing an improved compact security algorithm as well as using cloud infrastructure storage. The biggest challenge is data security either at rest or in transit and it is addressed with the help of cryptographic technique that is encryption and decryption. Encryption is the proven way to secure sensitive data. Secure data storage must be implemented to avoid stealing of sensitive data on mobile devices, using standard encryption algorithms with strong key to encrypt sensitive data residing on devices or in backend servers. Cloud based file system solves the storage issue of smartphones by offering continuous access anytime with unlimited cloud storage [10].

2. Statement of the problem

In recent times, smartphones have become an essential part of everyday lives of people. Securing sensitive data on smartphones have become more critical, because of increasing usage of mobile devices with Internet [8]. There is the need to ensure the three major security goals of data on smartphones that is confidentiality, integrity and availability. Because Android is not fully secured as it appears [28], security is one of the main concerns for smartphones users today with their vulnerability for attacks by malware, viruses, security threats, loss etc. [17].

3. SQLite

Based on [25] SQLite database (Figure 2) is a database used by Android for storing data. It consists of tables in rows and columns that are available to all applications for data storage. It is worthy of note that content provider is an intermediary between one application code and another application data. This aspect is very important when a developer wants to write a secure mobile application.

4. Justification for the study

It has been known from usage of smartphone that they are constrained in some areas such as their battery life, screen, security of data and storage space [2]. The user of Android smartphones today is found of using their devices to store sensitive data such as PIN, password, credit card numbers, debit card numbers, Bank Verification Number (BVN), email and so on. Hence, the need for research on improving and securing the sensitive data which on the long run also enhance the storage spaces of smartphones.

Similarly, there is no robust facility to save data in the cloud with appropriate extraction in android phones. Memory cards have reduced data security and reliability. Security is regarded as an essential concern for any smartphone which comprises sensitive information and accesses the internet. Due to inherent nature of these appliances such as portability and mobility they face additional security problems contrast to conventional devices of computing.

Nevertheless, today's business applications are going mobile and are using business information of an enterprise in mobile context to develop revenue by enhancing productivity. So, there is a need to secure mobile devices from different attacks. Thus, smartphone must meet a promising characteristic of providing integrated services of cloud power and at the same time should provide a well secured retrieval and storage through web client.

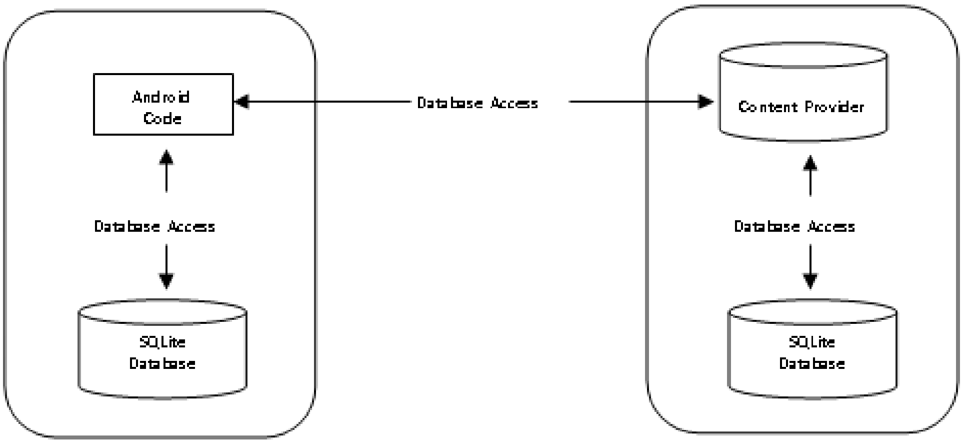

Fig. 2. Android SQLite database

5. Purpose of the study

The purpose behind this research is based on the realization that the growth of android smartphones use has resulted in increased volume of data being stored on them which leads to insufficient storage space. Based on confinement to the power, cost and size, smartphones will continue to deploy improved end flash memories as the main area of storage [11]. The smartphone storage was mentioned by [12],[16],[2] to be insufficient for users due to regular usage, increase in usable mobile applications, increase in the size of mobile applications and data generated by access to the Internet. Therefore, it is essential to carryout research on improving its storage by securing the data stored on it. Another motivating factor to choose this area of research is the vision of the cloud computing which is the opportunity of accessing data anywhere at any time. Mobile users can utilize the infrastructure, platform and software services with the aid of cloud providers on demand basis. There is unlimited storage for cloud users at minimal cost. This feature of cloud computing has really motivated this research to find out how android mobile users can utilize the cloud storage by putting appropriate security in place to protect users' data at rest and in transit.

6. Research methodology

This research surveys existing security works on android smartphones from 2008 to 2017. This approach enables the researcher to discover research gap where there is need for improvement. A security model which was already designed named SoloEncrypt [20] security architecture in order to enhance smartphone storage and provide security for user sensitive data was used.

Further, Advanced Encryption Standard (AES) which was publicly tested and approved by the National Institute of Standards and Technology (NIST) was adopted. To achieve the research objectives, a mobile application was developed and implemented on four Android smartphones of varied configurations. For cloud storage, Amazon Elastic Cloud (EC2) server was used due to cost savings and its many services.

Binomial distribution was used to find the optimal locations of cloud servers. The evaluation parameters to be used are *encryption time and decryption time* which are standard performance metrics approved by NIST for evaluating encryption algorithm. The study results were compared with existing ones using speed of encryption and decryption.

7. Experimental set up

7.1 Description of the mobile application

A mobile application was developed using Android studio 2.2.3 written in java and xml for the design of user interface. Amazon Elastic Compute Cloud (EC2) server was used for cloud storage and database. To guide against attack, the encryption key is randomly generated. The developed application is named ‘Solo App’ and can be downloaded from Google Play Store. The Google Play Store is an official store for all Android applications approved by Google where safe applications can be installed and use on all Android devices. The icon of Solo App has been registered with Google Play Store and is as shown in Figure 3. It can be located on the Play Store by typing ‘Solo App’.

Fig.3.Solo App

7.2 Evaluation parameters

The following devices (Table 1) were used for the experiment. The four devices were selected using convenience sampling.

Table 1(a): Configurations of devices

Smartphones	**Samsung Galaxy Note 8 (AD1)**	**HTC U11 (AD2)**
OS	Android 7.1.1 Nougat	Android 7.1 Nougat
CPU	Octa-core 2.35 GHz	Octa-core 2.45 GHz
RAM	6 GB	4GB
Storage	128 GB	64 GB

Table 1 (b): Configurations of devices

Smartphones	**Sony Xperia X2 Premium (AD3)**	**One Plus 5T (AD4)**
OS	Android 7.1 Nougat	Android 7.1.1 Nougat
CPU	Quad-core 2.45 GHz	Octa-core 2.45 GHz
RAM	4 GB	6 GB
Storage	64 GB	64 B

8. Results and discussion

8.1 Results

The experimental results are presented based on each of the four devices used for the experiment in Table 2 and Table 3. As a precautionary measure to reduce errors and ensures accuracy, each file size is repeated three times and the average time is recorded against the file size for each encryption and decryption.

Table 2: Encryption time

FILE (MB)	AD1 (s)	AD2 (s)	AD3 (s)	AD4 (s)
0.5	0.63	0.78	1.09	0.88
2.0	1.22	1.80	2.01	1.37
3.0	2.11	2.56	2.92	2.43
5.0	3.72	4.00	4.01	3.62
7.0	4.54	5.31	5.97	4.73

Table 3: Decryption time

FILE (MB)	AD1 (s)	AD2 (s)	AD3 (s)	AD4 (s)
0.5	0.60	0.71	1.01	0.57
2.0	1.18	1.65	1.89	1.30
3.0	2.07	2.55	2.57	2.34
5.0	3.51	3.87	3.76	3.33
7.0	4.29	5.13	5.34	4.52

8.2 Discussion

The concern of this work is to secure data on smartphones by using cloud infrastructure. The experimental results revealed that the algorithm encrypts with better speed and it takes less time to decrypt. For AD1 it took 0.63s to encrypt 0.5 MB of data while it took 0.60s to decrypt the same data. AD2 took 0.78s to encrypt 0.5 MB file size and took 0.71s to decrypt. Further, AD3 took 1.09s to encrypt 0.5 MB file size and 1.01s to decrypt. Likewise, AD4 took 0.88s to encrypt 0.5 MB file size and 0.57s to decrypt. Other results based on different file sizes and their corresponding encryption and decryption time are as presented in Table 4 and Table 5. The differences in encryption and decryption time 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 work using Crypto++ as presented by [1] speed benchmark. Crypto++ is one of the known cryptography libraries for cryptographic schemes. They had set speed benchmarks for commonly used encryption algorithms. For AES of 128-bit key size, their encryption speed benchmark is 4.196s. Therefore, comparing these results with the encryption speed benchmark showed better encryption time. Poonguzhali et al. (2016)[21] secure storage of data on Android based devices results showed that a 5MB file size took around 8.3s on first device and around 5.78s on second device to encrypt while this results for 5 MB shows 3.33s for minimum and 4.01s for maximum encryption time.

Table 4: Estimatingserver availability using binomial distribution

No. of agents (n)	**Formation of successful agents** (x)	**Probability that at least single server will exist on any particular iteration**(p)	**Standard deviation**	**Binomial z ratio**
100	20	0.5	5.000	-5.90
100	40	0.5	5.000	-1.90
100	60	0.5	5.000	+1.90
100	80	0.5	5.000	+5.90
100	100	0.5	5.000	+9.90

Where n= number of agents (servers); x= total number of successes to pick the best agents; p= probability of a success on an individual trial. Table 5 shows the assumption of available 100 servers and the probability of selecting the best cloud servers is computed using binomial z ratio. The formation of 20,40, 60, 80 and 100 servers with at least single server arecomputed. From the results, the **best case** with at least one server is computed to be +9.90 while the **worst case** with at least single server is -5.90. The implication of this is that cloud providers have unlimited servers available for cloud users all over the world and they are made available on request.

9. Conclusion

This research work had been able to develop a mobile application that can reside on android smartphones to provide security for user data at rest as well as in transit. The mobile application can be downloaded from Google Play Store. Advanced encryption standard was used to provide the encryption to Amazon cloud and can likewise be decrypted at any time in anyplace as long there is internet connectivity. Five smartphones were used for the experiments and the results were impressive when compared with existing works.

REFERENCES

[1] Abdel-Karim, A. T. Performance analysis of data encryption algorithms, Available at: http://www.cse.wusl.edu/-jain/cse567-06/encryption_perf.htm. 2017, Accessed: 15 June 2018.

[2] Altamimi, M., Abdrabou, A. Naik, K. & Nayak, A. ‘Energy cost models of smartphones for task offloading to the cloud, *IEEE Transactions on Emerging Topics in Computing,* 6(1), 2015, pp. 1-14.

[3] Asami, H., Uchida, Y., Ohbatake, H., Sato, K., Nakatani, J. et al. Study group on information security issues of smartphone and cloud computing final report, Available at:http://www.soumu.go.jp/main_sosiki/joho_ tsusin/eng /pdf/121022 _01.pdf, 2012, pp. 1 - 62. Accessed: 18 June 2018.

[4] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M. & Smith, J. M. ‘Smudge attacks on smartphone touch screens’, Proceedings *of the 4th USENIX Conference on Offensive Technologies,* Berkeley, CA, USA, 2010, pp. 1-10.

[5] Beust, C. Cedric’s weblog: Android’s locking pattern. Available at: http:// beust.com /weblog2/archives /000497.html. 2016, Accessed: 18June 2018.

[6] Carroll, A. &Heiser, G. ‘An analysis of power consumption in a smartphone’, *Proceedings of the USENIX Conference on USENIX Annual Technical Conference*, USENIX ATC’10, Berkeley, CA, USA, 2010, pp. 21–42.

[7] Castellucci, S. J. &MacKenzie, I. S. ‘Gathering text entry metrics on android devices’, *Proceedings of the 2011 Conference on Human Factors in Computing Systems (CHI), CHI EA ’11,* ACM, New York, NY, USA, 2011, pp. 1507-1512.

[8] Donald, A. C., Oli, S. A. &Arockiam, L. ‘Mobile cloud security issues and challenges: a perspective’, *International Journal of Engineering and Innovative Technology (IJEIT)*, 3(1), 2013, pp. 401-406.

[9] Halperin, D., Kandula, S., Padhye, J., Bahl, P. &Wetherall, D. ‘Augmenting data center networks with multi-gigabit wireless links’, *Proceedings of the ACM SIGCOMM 2011 conference, SIGCOMM ’11*, New York, USA, 2011, pp. 38-49.

[10] Kaur, S. Cloud based file system on mobile devices, Masters’ Thesis. San Diego State University, 2012, pp. 1-52.

[11] Kim, H. & Ramachandran, U. ‘Fjord: informed storage management for smartphones’, *IBM Research,* California, USA, 2013, pp. 1-5. Available at: https://www. computer. org /csdl/proceedings/msst /2013 /0217/00/ 06558 430.pdf.Accessed: 17 June 2018.

[12] Kim, H., Agrawal, N., &Ungureanu, C. ‘Revisiting storage for smartphones’, *ACM Transactions on Storage (TOS),* 8(4),2012, pp.1-14.

[13] Koukoumidis, E., Lymberopoulos, D., Strauss, K., Liu, J., & Burger, D. ‘Pocket cloudlets’, *Proceedings of the 16thInternational Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS ’11,* New York, NY, USA, 2011, pp. 171-184.

[14] Kuppusamy, K. S., Senthilraja, R. &Aghila, G. 'A model for remote access and protection of smartphones using short message service’, *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* 2(1), 2012, pp. 91-100.

[15] La Polla, M., Martinelli, F. &Sgandura, D. ‘A survey on security for mobile devices’, *IEEE Communications Surveys and Tutorials,* 15(1), 2013, pp. 446-471.

[16] Liu, W., Hu, Y., Rong, H. & Li, R. ‘Optimizing file system performance for android-based consumer electronics by an experimental method’, *Journal of Convergence Information Technology (JCIT),* 8(17), 2013, pp. 50-57.

[17] Mandeep, S. &Kanwalvir, S. D. ‘Securing RJSON data between middleware and smartphones through Java scripts based cryptographic algorithms’, *International Journal of Soft Computing and Engineering*, 3(2), 2013, pp. 189-194.

[18] Masqsood, S., Chiasson, S. & Girouard, A. ‘Bend password: using gestures to authenticate on flexible devices’, *Journal of Personal and Ubiquitous Computing, Springer*, 20(4), 2016, pp. 573-600.

[19] Muneer, A. D. &Javed, P. ‘Evaluating smartphone application security: a case study on android’, *Global Journal of Computer Science and Technology Network, Web & Security*, 13(12), 2013, pp. 8-15.

[20] Olaleye, S. B**.**, Ranjan, I. & Ojha, S. K. ‘SoloEncrypt: a smartphone storage enhancement

security model for securing users' sensitive data', *Indian Journal of Science and Technology,* 10(8), 2017, pp. 1-8.

[21] Poonguzhali, P., Dhanokar, P., Chaithanya, M. K. and Patil, M. U. 'Secure storage of data on android based devices', *International Journal of Engineering and Technology,* 8(3), 2016, pp. 177-182.

[22] Ramgovind, S., Eloff, M. M. & Smith, E. 'The management of security in cloud computing', *IEEE International Conference on Information Security for South Africa (ISSA)*, 2-4 August2010, pp. 1-7.

[23] Ruiz-Heras, A., Garcia-Teodoro, P. & Sanchez-Casado, L. 'ADroid: anomaly-based detection of malicious events in android platforms', *International Journal of Information Security-Springer*, 2016, pp 1-14. doi:10.1007/s10207-016-0333-1.

[24] Sarwar, M. & Soomro, T. R. 'Impact of smartphone's on society', European *Journal of Scientific Research,* 98(2), 2013, pp. 216-226.

[25] Singh, R. 'An overview of android operating system and its security features', *International Journal of Engineering and Applications*, 4(2), 2014, pp. 519-521.

[26] Suarez, G., Tapiador, J. E., Peris, P. &Ribagorda, A. 'Evolution, detection and analysis of malware for smart devices', *IEEE Communications Surveys and Tutorials,* 16(2), 2014, pp. 961-987.

[27] Thomas, K. C. & Moon, Y.'Why storage solutions are accelerating the mobile revolution', *Global Standards for Microelectronics Industry, Samsung Electronics Report*, 2014, pp. 1-24.

[28] Tiwari, M., Srivastava, A. K. & Gupta, N. 'Review on android and smartphone security', *Research Journal of Computer and Information Technology Sciences,* 1(6), 2013, pp. 12-19.