Research Journal of Applied Sciences, Engineering and Technology 13(7): 533-543, 2016
DOI:10.19026/rjaset.13.3013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 2, 2016 Accepted: August 1, 2016 Published: October 05, 2016

Research Article

A Study of Ten Popular Android Mobile Cloud Storage Applications

[1]Asou Aminnezhad, [2]Pooya Khanmohamadi Hezaveh, [3]Mohsen Khodadadi and [4]Amelia Tan
[1]Faculty of Computer Science and Information Technologi, Universiti Putra Malaysia,
[2]Faculty of Computer Science and Information Technologi, Asia Pacific Universiti,
[3]Faculty of Computer Science and Information Technologi, Universiti Technologi Malaysia,
[4]Department of IT, Pacific Frase Corporation, Technologi Park Malaysia, Malaysia

Abstract: The mobile cloud storage application becomes more ubiquities recently for storing data such as image, audio, text files and etc. The most important issue in this regard is security of these tools and using the best method for encrypting the users' data for keeping them protected. In this study, we examine ten mobile cloud storage applications namely 4Shared, One Drive, Mega, Surdoc, Cubby, ADrive, Safe Sync, Team Drive, Wuala and Just Cloud. In these applications, we analyze the intercepted communications to determine encryption of the captured text and voice communication to bring out the results to find out the best cloud application that follows the encryption methods mostly. Thus, we use a histogram to analysis the text file and use a Wire shark to check whether a plaintext has been found in the cloud storage application or not, after that we analyze the plain text.

Keywords: Cloud storage applications, data communication, encryption, mobile interception

INTRODUCTION

Currently, cryptographic communication has become attractive topics since it affected the online storages' security like Mega, 4share, Sur Doc and etc. The cryptography in communication is increasingly used by individuals, business and government agency and has become a controversial topic as it helps secure our data by using encryption methods. Cryptography is the conversion of data into a secret code for transmission over a public network. The cryptography is based on changing the Plain text into cipher text by encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext. The encryption algorithm uses a key, which is a binary number from 40-256 bits length. The greater number if bits in the key (cipher strength), possible key combinations and the longer it would take to break the code. The data are encrypted, or "Locked", by combining the bits in the key mathematically with the data bit. As it is mentioned by Bellovin a novel combination of public and secret keys cryptography can be secure against active attack attempts of hackers, also, William clarified the secure cryptography method to protect against being hacked by giving information about data encryption standard and DES encryption algorithms.

There are a few security standard technologies such as an SSL (secure sockets layer) that are used to establish an encrypted link between a server and a client. Also, there is another technology that called an IPsec, which is a framework for a set of protocols for security at the network or packet-processing layer of network communication that was proposed by Taher as a computer product patent to secure private communication (Elgamal and Hickman, 1998).

In addition, an Advanced Encryption Standard (AES) that is a national institute of standard and technology specification for the encryption of electronic data. To find a trustable data, we looked for pre-implemented AES development online to be used as the encryption methodology that must be written in different languages and by different developers.

To provide the required variety in the programming methodology, which is coded in C# by McCaffrey (2003) and the in detail information about secure method in cloud to encrypt data was discussed by Aminnezhad *et al*. (2013).

The aim of the research paper is determining encryption in communication with audio and text for the cloud storage. We examined the ten online storage applications for android devices such as 4Shared, OneDrive, Meg, SurDoc, Cubby, ADrive, Safe Sync, TeamDrive, Wuala and JustDrive. Based on these applications, we analyze and capture all the audio and text communication with using "shark for root" application that the application will generate a pcap file. We used a Wireshark to open the pcap and examine the

Corresponding Author: Asou Aminnezhad, Faculty of Computer Science and Information Technologi, Universiti Putra Malaysia, Malaysia

communication whether is encrypted to create ahistogram that captures the communication method for examining all the encrypted application level. This study overviews the cryptography interception techniques and the ten popular cloud storage for the android mobile application. Also, we will present an experiment result and discuss our findings and conclude the remarks.

MATERIALS AND METHODS

In this section, we found out that each of the cryptography protocols have interception method and put the results in Table 1. Internet Protocol Security (IPsec) authenticates and encrypts the IP packets during IP network sessions. Boirun (2013) stated that IPsec can be used to establish Virtual Private Network (VPNs), which authenticate, encrypt and encapsulate data for transport. The AES encryption is a stronger file encryption method that can be used to protect classified data and hardest one to crack due to a large number of the key combination. The SSL and Transport Layer Security (TLS) is the most widely deployed security protocol nowadays to provide a secure channel between two operating machines over the Internet or an internal network that was proposed as a patent by Freed and Gannesan (2006).

Cryptography application: There is a wide range of cryptography applications available for different mobile operation systems like Android, iOS, Window mobile and etc. some of them only support sending a text and voice file, but others support text, voice and video file in the communication. In this section, we examine the ten popular encrypted Android applications that support voice, text and video file. These applications are 4Shared, One Drive, Meg, SurDoc, Cubby, ADrive, Safe Sync, Team Drive, Wuala and Just Drive. We installed the latest Android version of these ten applications in the mobile phone to examine them.

The reason for choosing these applications is simple: we are interested in use free applications in the market that only need to register for accessing the storage space up to 100GB. Another reason is that these applications are commonly used now a days for sharing the date/information and using to back up the information by users. These applications allow users to download and upload information by using the mobile phone. But the main reason is using cryptography method for encryption in these 10 applications.

Overview of the cryptography application: According to our research about these applications, 4Shared has its own security cryptography communication protocol and all the data of the communication are encrypted with using 128-SSL. 4Shared's security platform is designed around, administration control, data integration and application interoperability. It delivers this secure infrastructure through a wide range of processes and technologies that help to prevent unauthorized access to confidential information and facilitate privacy management. Specifically, SSL is the standard protocol for data transfer security that sets an encrypted link between 4shared server and your browser. Once the link is established all the communication will be confidential.

The Mega cloud storage uses the AES-128-bit encryption for bulk data transfers and shared files to use the RSA-2048 encryption method. The features for this application are in a most secure environment because the data is encrypted before upload and decrypted after download and as stated by James (2014) that if users lose the security key, they won't be able to access their data anymore. The Just Cloud uses the 256-bits AES encryption for all the data and stores them in the cloud server in the safe and secured space. The security and encryption method for Wuala uses the AES-256-bit encryption for data transfer along with RSA-2048 that it is a strong security method for a digital data. The Sur Doc uses the SSL with AES-128-bit encryption to ensure the data security; also a RAID-5 configures servers and offline backup to provide self-managed redundant replication for protection against disc failure. The ADrive uses the SSL-encrypted to transfer the files and the user account is password-protected to prevent the unauthorized access and had a security feature that is geographical redundancy. It means that the online storage service stores several copies of the data in different places and in the case of losing data by user they still can be accessible on server in a different location. The One Drive uses the SSL encryption to

Table 1: Cryptography interception techniques

Cryptography protocol	Interception methods	Comment
IPsec	Data mining	Is a communication interception technique that uses a computer system to investigate the data?
	Wiretapping	Installing a device to record or transmit the detail of a conversation.
	Internet interception	The ability to access and unscramble encrypted message
	Video surveillance	Install a video camera to spy on user action and conversation.
TLS/SSL	Man-in-the-middle	Impersonates other parties to the conversation to gain access of the information that the parties send to each other.
	Side jacking	Sniffing data packet to steal session cookies and hijack a user session.
	Sniffing	Using easy and available software to intercept data that being to send from or to user device.
AES	Brute-force	Is a crude algorithm which works through every possible answer until get the correct answer?

transfer the data that anyone cannot intercept it. The user can create, edit or delete the files with the confidence that these actions will be reflected in OneDrive account.

Is the communication encrypted? Based on our research, we figured out that upload and download the communication are encrypted for these 10 applications. Also, we used the histogram to check the encryption frequency and based on the frequency we found that a higher frequency has a higher encryption security. For uploading the audio file, the higher frequency was the Safe Sync that it shows 40000 and for downloading, the higher was the Team Drive that shows 14000. In addition, to upload and download text section the higher frequency was for the 4Shared application by 30000 frequencies. These are the results that we found after examining those 10 applications to find an encryption frequency.

Afterward, we found out that if the cloud storage doesn't have the encryption suffers from the security flaws on that application. According to this finding, 4Shared has this flaw among these ten applications. Also, we observed that the plain text from Wireshark clearly shows the login ID and the login password for 4Shared when the login was success.

In addition, Aminnezhad *et al*. (2015) and Azfar *et al*. (2014) did the same research about encryption method in medical and VoIP application. The researchers used two Google nexus phones to work on the experiment of their research, but we used one Samsung Galaxy SII Android phone with android version 4.2.2 and the ten cloud storage applications in Table 2 were examined in the experiments. Wi-Fi network was used as a communication channel that only connected to the phone in order to avoid other traffics when we start capturing the traffic. In our experiment, the Wi-Fi was only connected to the Samsung android phone and there are no other devices connected to the Wi-Fi. This is to ensure the consistency on the packet that we will capture in later on.

Setup: To capture the network traffic in the pcap format we used an android application is called Shark for root. The mobile cloud storage was run on one phone meanwhile upload and downloads the text and audio file that were captured separately. For each of the ten applications, we captured both upload and download traffic for text and audio files that the time to capture depends on the file size. We will stop the shark for root by finishing the upload or download. The same audio file was used to upload and download for the ten applications.

Table 2: Support platform and authentication method of cryptography application

Cryptography application	Support mobile platforms			Authentication method
	Android	IOS	Window	
4Shared	Yes	Yes	Yes	Valid email to access and password
OneDrive	Yes	Yes	Yes	Valid email to access and password
MEGA	Yes	Yes	No	Valid email to access and password
SurDoc	Yes	Yes	Yes	Valid email to access and password
Cubby	Yes	Yes	No	Valid email to access and password
ADrive	Yes	Yes	Yes	Valid email to access and password
Safe Sync	Yes	Yes	Yes	Valid email to access and password
TeamDrive	Yes	Yes	No	Valid email to access and password
Wuala	Yes	Yes	Yes	Valid email to access and password
JustCloud	Yes	Yes	Yes	Valid email to access and password

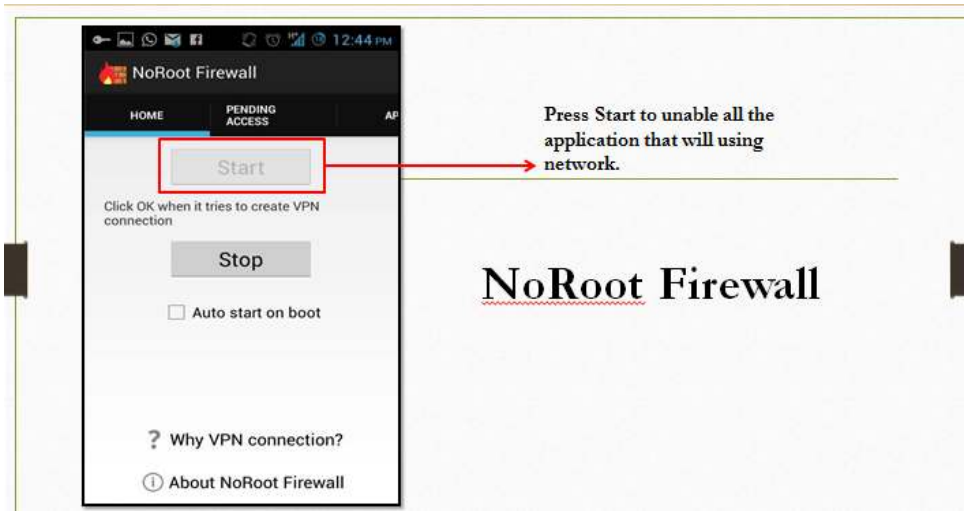

Fig. 1: Press start on no root firewall

To make sure there are no other captured traffics, all of the other applications that might generate Internet traffic was turn off by using the application is called a No Root Firewall. The procedures and details of capturing each ten applications are shown as following (Fig. 1 to 8). First step will be press start on the No Root Firewall. This application is to allow specified application enable on the network access. Before starting to upload or download the file, this step must be done at first. Select a file format to upload/download. We have chosen for audio file size about 2.27 to use for this purpose. The total time of upload/download depends on the completion time of the upload/download of the file and the Internet speed over the Internet. When the file was complete upload/download, the shark for root should be stop capturing the packet continuing. The file was automatically saved in the file manager with pcap file format. We found the plaintext of username and password on 4shared application, it can be clearly seen that the username is evilson513@hotmail.com and the password is jason123456. Thepacketfiles were captured

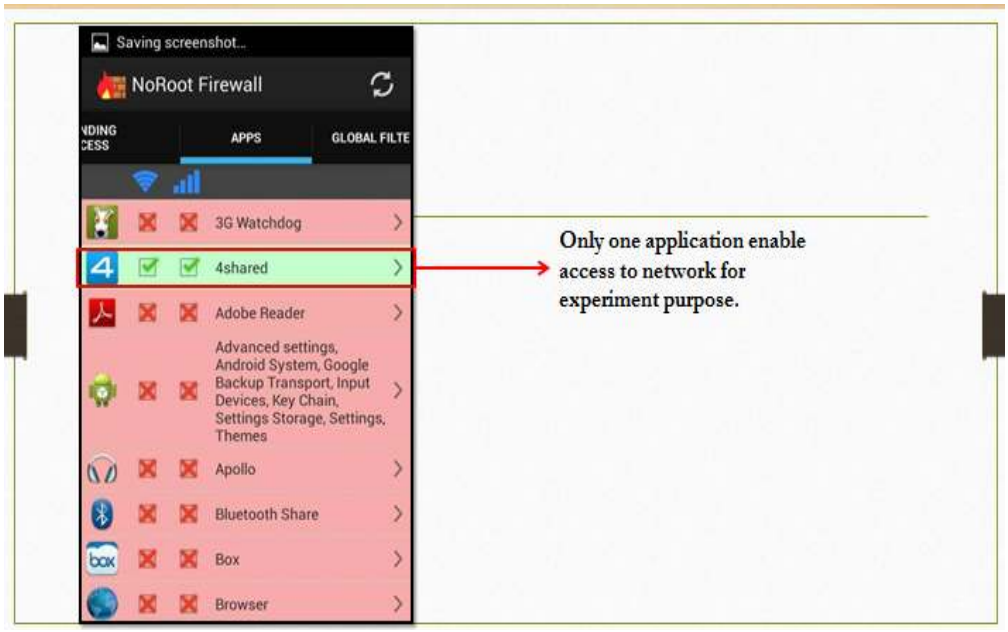

Fig. 2: Use Network access on specified application

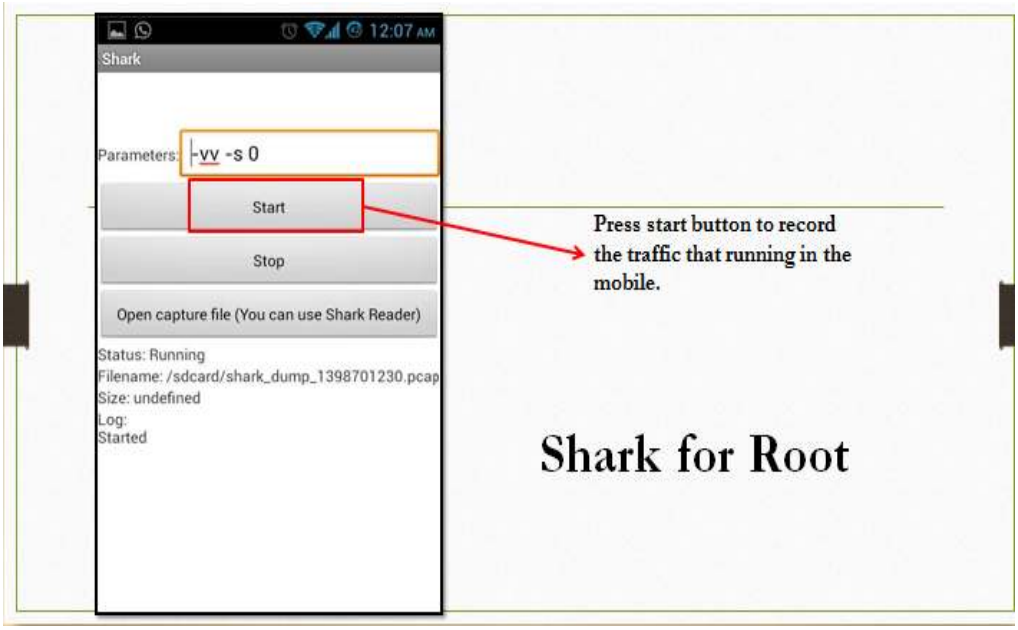

Fig. 3: Press start for shark for root

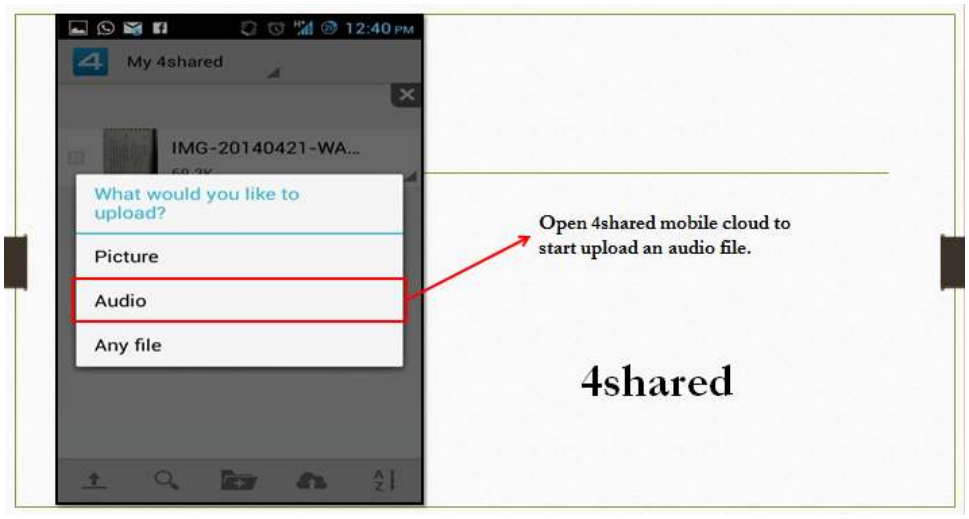

Fig. 4: File selected

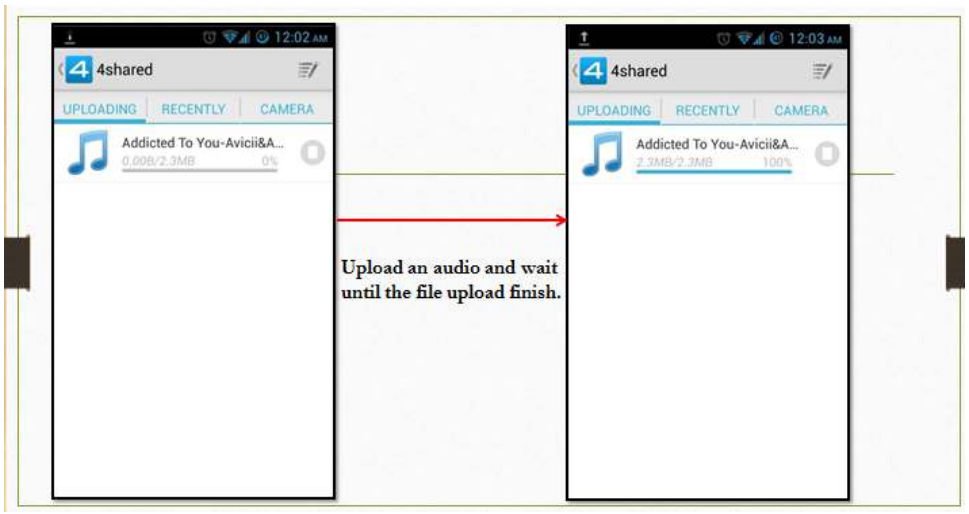

Fig. 5: The total time of uploading/downloading

Fig. 6: Stop button after finish uploading/downloading

Fig. 7: File location

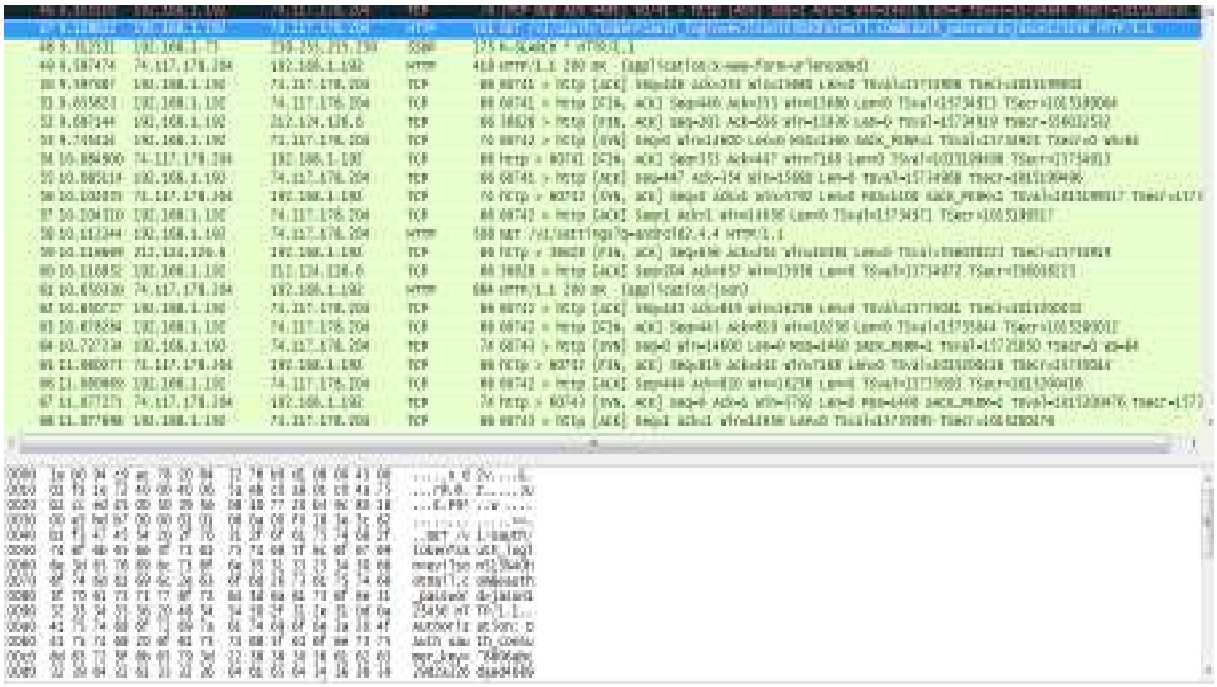

Fig. 8: Plain text in 4shared

Table 3: Authentication ID and password

Cloud storage	Login ID	Password
Adrive	mmy5500@gmail.com	Mymark70
Surdoc	mmy5500@gmail.com	Mymark70
Wuala	mmy5500@gmail.com	123456789
Safe Sync	mmy5500@gmail.com	12345678
4Share	evilson513@hotmail.com	jason123456
Mega	evilson513@hotmail.com	evilson513@hotmail.com
Box	evilson513@hotmail.com	jason123456
Chubby	genius_inging_90@hotmail.com	12345678
Teamdrive	inging906@gmail.com	inging906@gmail.com
JustCloud	genius_inging_90@hotmail.com	12345678

by upload and download the audio file with 2.27MB file size (Table 3).

Analysis of the captured packets: The method that applied to find out whether the capture packets are

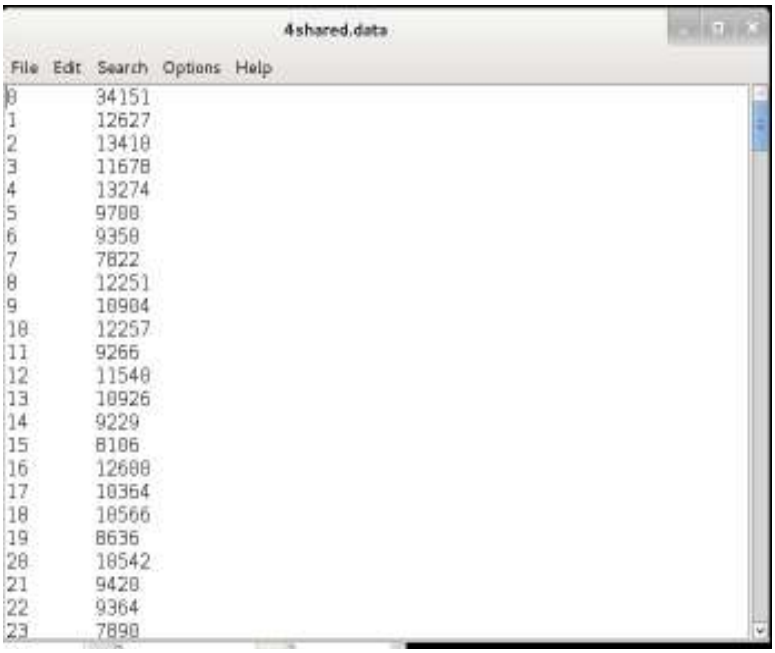

Fig. 9: The date of frequency and byte value of 4shared

encrypted or not is a Pcap Histogram tool to read the payload of captured packets and plot a histogram with the frequency on the Y axis. There are three ways to judge whether the histogram is encrypted or not from the histogram:

- If there is a readable plain text, alphabet in lowercase or uppercase are known as non-encrypted. As we know that the encrypted data is not readable.
- If the byte values are distribution equality on the graph, it means that the data is encrypted.
- If the graph is not clustered around arange, it means that it is dispersed and the data is not encrypted.

We have found the histogram method according to the based study (Azfar *et al*., 2014). The study of ten popular Android mobile VoIP applications contains a script to plot histogram that using perl language. Firstly, we saved the script file in pcaphistogram.pl and used the drag and drop method to certain a code and run the pcap file in order to generate the pcaphistogram. The code is shown as below:

perl<pcaphistogram.pl><4shared.pcap>|gnuplot: Furthermore, based on the histogram, value that uses to plot out the histogram is based on the frequency and byte value. The value in data can be seen as a Fig. 9.

The histograms are following the data on packet file (pcap) to plot the histogram in the correct sequence.

Based on the Fig. 10, contain highest frequency with the byte value was the Safe Sync application that shows the frequency number was 40000 as it can be seen from Fig. 11. It was the highest frequency compare with the others 9 application as they are shown in Fig. 11 to 13. For Safe Sync, the found histogram states that the frequency of bytes with no clusters, which suggests that Safe Sync might also be encrypted. For Just Drive, the results were remarkable because just a minor cluster can be seen that suggests is not encrypted. It is same for the 4shared that the minor cluster shows the probability of not to be encrypted.

RESULTS AND DISCUSSION

In this case, there were two tests performed after capturing the packet meanwhile the upload and download. The first experiment was after capturing the packet in upload and download using audio file that analyzed by using Voice over misconfigured Internet telephones (vomit) to retrieve back the original song. The second experiment was for the text file that analyzed on Wire shark to search the written text file in the plaintext.

Voice over misconfigured Internet telephones (vomit): This method has been used to converts the audio file into a wave file that can be played with ordinary sound players. Vomit is required tcpdump output file to conduct this experiment.

Text files upload/download analysis: The packet was then being tested in the Wireshark to check whether the text file was encrypted. If there was any plaintext found, it shows the text file was not encrypted, same goes to the plaintext not found, it means text file was encrypted.

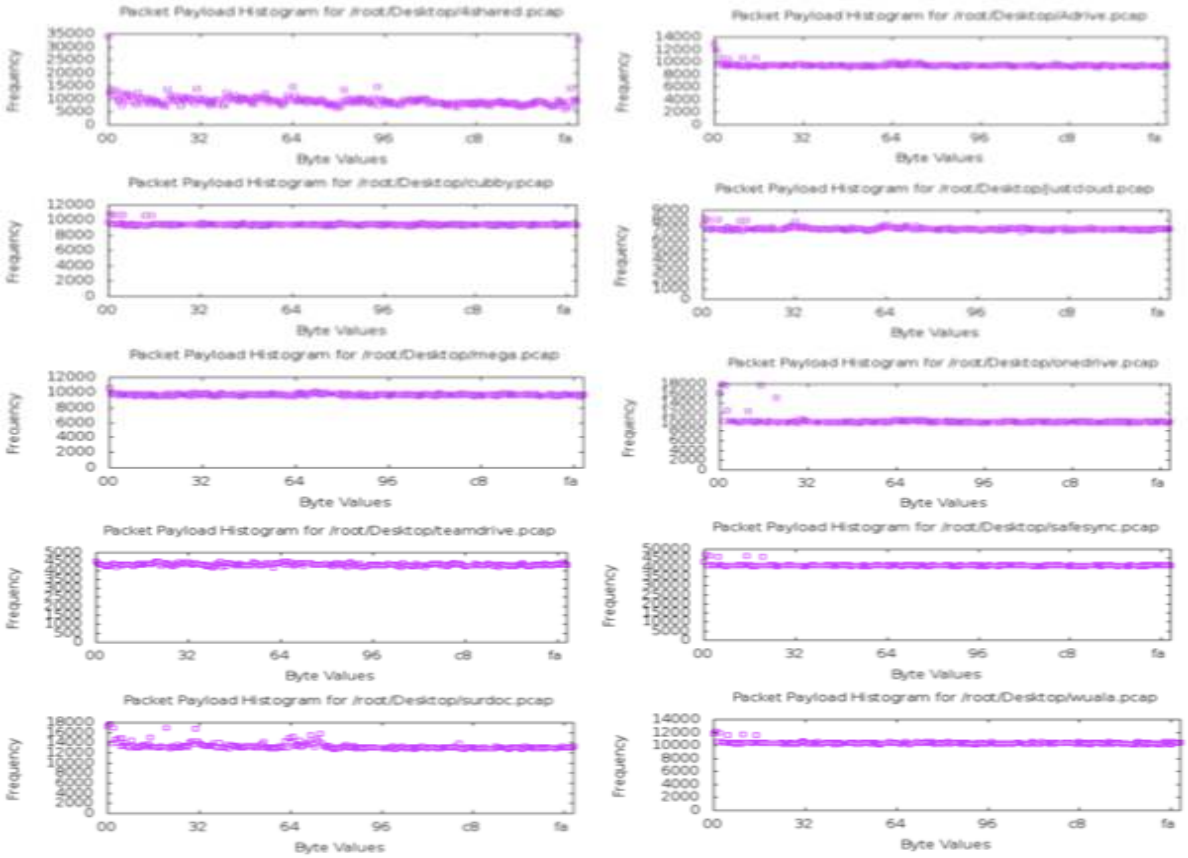

Fig. 10: Analysis of histogram on upload audio file packet

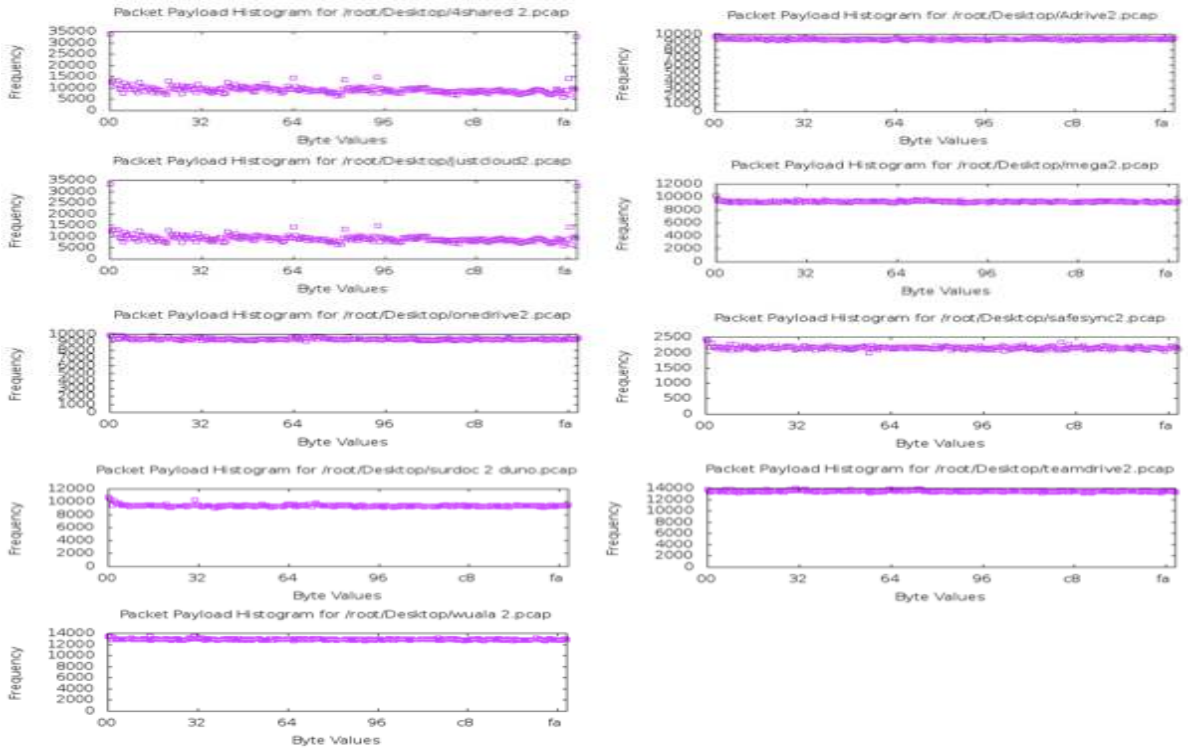

Fig. 11: Analysis of histogram on download audio file packet

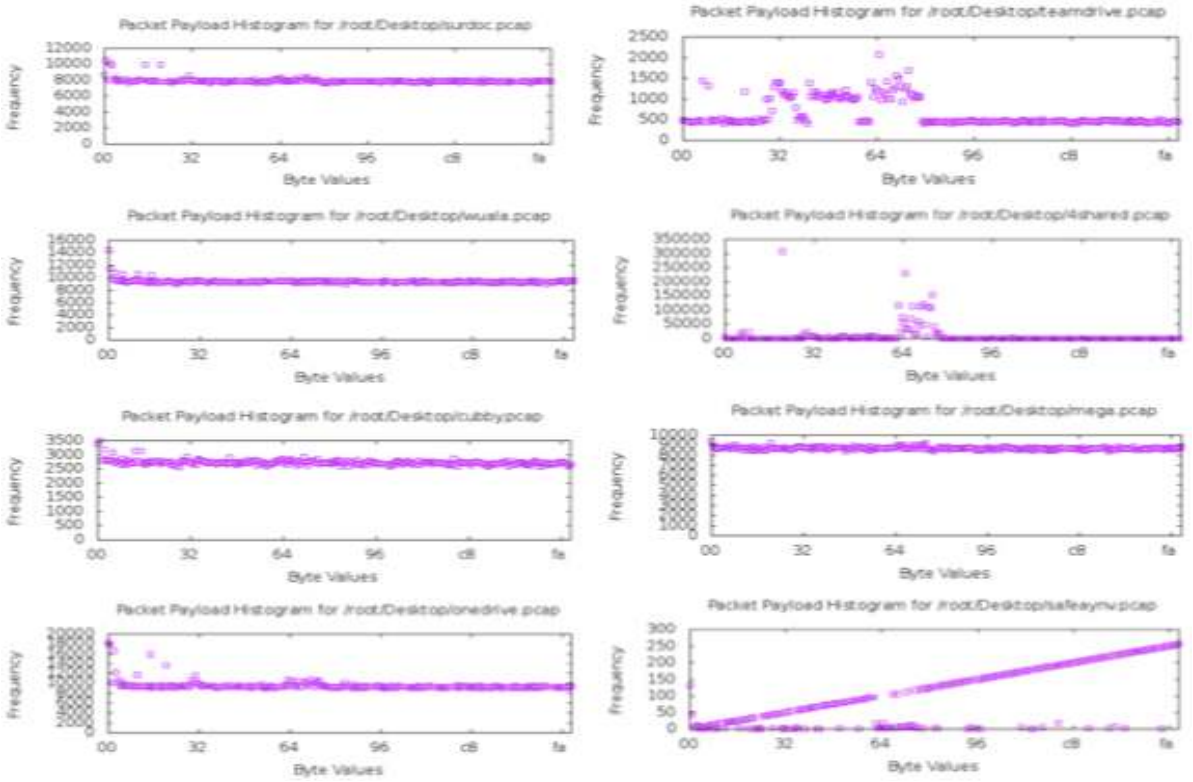

Fig. 12: Analysis of histogram on upload text file packet

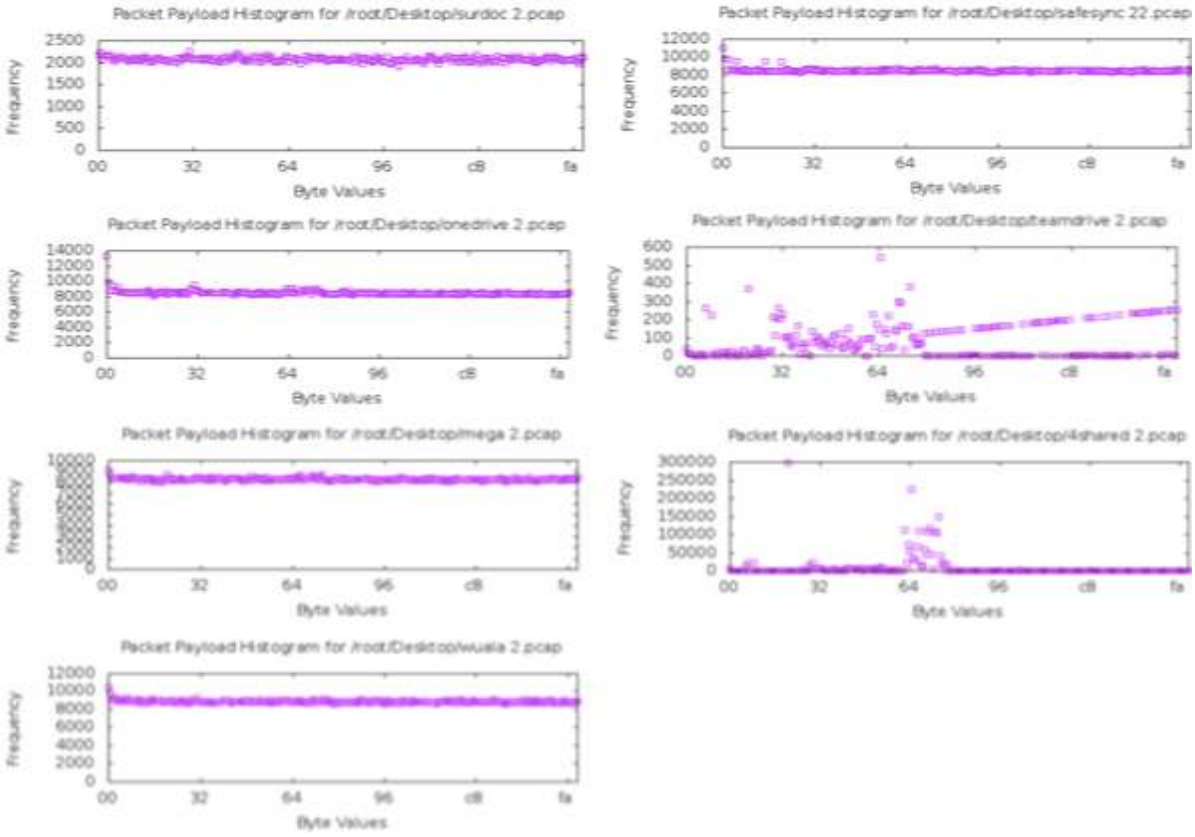

Fig. 13: Analysis of histogram on download text file packet

Fig.14: Plaintext found on mega

Fig. 15: Encrypted symbol on TeamDrive

Based on the Wireshark analysis, the only plain text that can found are shown in Fig. 14. Figure 14 shows that only the plaintext can be found among the ten applications. It shows the content type is text/plain, current length and access control.

In the figure showing that the Team Drive is encrypted and no any plaintext was found in Fig. 15.

Audio upload/download analysis: After capturing the packets, it was tested by using vomit to retrieve back the original format. If the audio is able to retrieve back the original format, it means it was not encrypted. Besides that, it was encrypted.

In addition, on the Audio file within upload and download frequency, the highest encrypted based on histogram among the ten mobile cloud storage applications which on the upload packet is Safe Sync. The mosthigher the frequency, the highest encryption will form; as the result that showed, Safe Sync is the highest encrypted cloud storage application, which is

Table 4: Frequency of each application

		Audio		Text	
No.	Package/Application	Upload package	Download package	Upload package	Download package
1.	4Shared	10000	10000	300000	300000
2.	OneDrive	10000	10000	10000	8000
3.	MEGA	10000	10000	8500	8500
4.	SurDoc	14000	10000	8000	2500
5.	Cubby	10000	-	3000	-
6.	ADrive	10000	10000	-	-
7.	Safe Sync	40000	2000	250	8000
8.	TeamDrive	4500	14000	500	200
9.	Wuala	10000	13000	9000	9000
10.	JustCloud	7000	10000	-	-

40000. The second highest based on the histogram of the ten mobile cloud storage application, which on the upload packet is SurDoc. The frequency of the Sur Doc is 14000. Team Drive will be the lowest encrypted based on histogram among the ten mobile cloud storage application on upload packet. The frequency of the Team Drive is only containing 4500. This mean, in upload packet, Team Drive is the lowest encrypt.

While for the highest encrypted based on histogram among the ten mobile clouds storage application on download packet is Team Drive. As the diagram above, the frequency of the TeamDrive is 14000, which are higher than other nine mobile cloud storage application. While for the second highest encrypted based on the histogram, the numberof ten mobile cloud storageapplications on download packet is Wuala. The frequency of the Wuala is 13000 that lower 1000 than Team Drive. SafeSync is the lowest encrypted based on histogram among the ten mobile cloud storage application on download packet that is 2000 only.

In the other hand, the Text file upload and download's frequency based on the histogram. The highest one on upload side is 4shared, the second one is One Drive and the third one is Wuala. The different of each frequency are obvious when to compare the histogram with the others.

Furthermore, the download side, the highest frequency is still 4shared. And the second highest is Wuala. Come to the third highest which is MEGA. The details of each application with the frequency are shown in Table 4.

CONCLUSION

In this research, we conduct an in-depth analysis of the ten mobile applications as summarized in the Table 1 to 4 by using the histogram and root for shark. According to our results, On the Audio file within upload and download frequency, the highest encrypted based on histogram among the ten mobile cloud storage applications, which on the upload packet is Safe Sync. For the frequency as the result shown belongs to the Safe Sync by owning the highest frequency in the cloud storage application. While for the highest encrypted based on histogram among the ten mobile clouds storage application on download packet is Team Drive. In the other hand, for the text file upload and download's frequency based on the histogram, the highest one on upload side belongs to the 4shared. This research helps to contribute towards a better understanding of legal interception of packet interception between the client and server. Also, we are working on providing more secure data transmitting for medical purpose. The re-encryption formula will help the multiuser to use and trust the cloud computing, encryption and decryption under a certain tag name that put together with the file.

REFERENCES

Aminnezhad, A., A. Dehghantanha, M.T. Abdullah and M. Damshenas, 2013. Cloud forensics issues and opportunities.Int. J. Inf. Process. Manag., 4(4): 76-85.

Aminnezhad, A., M.T. Abdullah and P.K. Hezave, 2015. An investigation of the secure data communication in medical mobile applications. J. Theor. Appl. Inform. Technol., 73(2): 239-245.

Azfar, A., K.K.R. Choo and L. Liu, 2014. A study of ten popular android mobile VoIP applications: Are the communications encrypted? Proceeding of the 47th Hawaii International Conference on System Sciences.Waikoloa, HI, pp: 4858-4867.

Boirun, R., 2013. The Importance of File Encryption During Uploading to Cloud Storage. Retrieved from: http://www.drivepop.com/importance-encryption-uploading-transferring-cloud-storage/.

Elgamal, T. and K.E.B. Hickman, 1998. Secure socket layer application program apparatus and method. Google Patents US 5825890 A.

Freed, M. and E. Gannesan, 2006. Secure sockets layer proxy architecture. Google Patents US 7149892 B2.

James, K., 2014. The Most Secured Cloud Storage Providers. Retrieved from: http://www.bestcloudstorage.net/secured-cloud-storage-providers/.

McCaffrey, J., 2003. Keep your data secure with the new advanced encryption standard. MSDN Magazine.