Novel Method for Safeguarding Social Network Communication via Collaborative Antivirus Techniques and the Cloud

Omar Abdullah Batarfi

King Abdulaziz University, Jeddah, Saudi Arabia

Summary
Smartphones are strongly associated with everyday life, and users increasingly depend on their smartphones for frequent and essential tasks. This makes smartphones a prime target for attackers to distribute their malware in order to damage smartphones and steal sensitive user data. Unlike desktop computers, implementing efficient and high-performance security mechanisms on smartphones is a major challenge as smartphones have strict resource constraints in terms of memory size, computational ability, and energy. Implementing security mechanisms that consume a significant percentage of mobile resources will negatively affect the performance of mobile devices. One of the popular methods attackers use to access a victim's device is sending malicious URLs, images, and documents through social media. Attackers can then gain access to a user's sensitive data stored in their mobile device, such as their banking information, or remotely control and access the mobile device's camera, microphone, and other resources. The model presented here improves the SocialAV [1] solution proposed in the reviewed literature by using cloud computing and a different collaborative approach. The objective of this research is to implement a secure environment for social networks (secure chatting) that protects social network members from malicious content by running a lightweight and real-time antivirus program. The proposed model is dedicated to scanning malicious content within a social network and making its security services available to all users, regardless of their mobile device's capabilities.

Key words:
Social Network, Smartphone, malware, cloud computing, antivirus

1. Introduction

There are different categories of mobile device antivirus options. These can be classified by the location of the execution, services provided by the antivirus software, or the techniques used to detect the malware. In terms of location, there are two different types of antivirus software: host-based and cloud-based. In a host-based setting, the software is installed and fully executed in the main memory of the mobile device. However, in a cloud-based setting, the antivirus software is installed and executed inside the cloud to provide a lightweight antivirus solution that consumes less mobile memory and CPU space, while a smaller piece of software is installed on the mobile device itself to communicate with and receive the results of malware scanning from the cloud.

There are also different types of mobile antivirus software that differ in the way they detect malware, such as signature-based and behavior-based techniques. Signature-based techniques detect the malware by comparing the signature of the scanned file with familiar signatures of malware stored inside the antivirus database; if the signature of the file matches any signature inside the database, the file is considered a malicious file. However, behavior-based techniques analyze and monitor the behavior of objects, so if the software detects any unauthorized behavior or action, it will consider the object as malicious, or at least suspicious [5].

The proposed model in this research study is responsible for securing a social network environment. It is a hybrid solution that combines cloud- and host-based techniques. Cloud computing uses only the initial state as a central unit to manage the antivirus database. Otherwise, each member who contributes in virus scanning will host/store part of an off-the-shelf antivirus database. Antivirus software in the proposed model (ClamAV) [5] uses a signature-based scanning technique to detect viruses. The model also follows a collaborative approach where multiple mobile devices collaborate together to detect malicious content. The collaborative approach produces a lightweight solution for mobile devices that consumes fewer mobile resources (CPU, memory, and battery).

1.1 Contribution

Provide a secure social network environment by enhancing the SocialAV solution proposed in [1] by replacing the cellular network with cloud computing and improving the collaboration technique to increase the number of beneficiaries and make the services available to all members in a convenient manner, regardless of their mobile device's capabilities, in addition to combining multiple antivirus programs to increase the level of security across social media networks.

Manuscript received October 5, 2019
Manuscript revised October 20, 2019

2. Related Work

The Secloud model [2] provides an antivirus solution to scan a mobile device using multiple antivirus programs installed in the cloud, but it needs to make a full replication of the mobile device in the cloud. Unlike Secloud, the proposed model does not require a mobile replication in the cloud; it provides real-time antivirus services only for the data being transmitted within social media.

The SocialAV [1] model is a resource-aware antivirus model for a social network that distributes the malware signature database of the existing off-the-shelf antivirus software among different mobile devices to reduce the memory consumption for each individual device. The SocialAV model uses the cellular network infrastructure as a central unit to manage and distribute the database of the antivirus software between peers. In contrast to the SocialAV model, the proposed approach uses cloud computing as the central unit to manage and distribute the database. Using the cellular network restricts the amount of data being transmitted and requires an additional cost for each piece of data transmitted. Thus, the idea behind replacing the cellular network with the cloud is to reduce the overall cost of the model and benefit from the high performance of cloud computing in terms of response time and availability.

Also, if the proposed model is compared with SocialAV in terms of the technique used in virus scanning, SocialAV forwards a portion of the antivirus database sequentially between peers to scan the files transmitted in social media, whereas in the proposed model, all security guard members simultaneously scan files to detect viruses at the same moment using their own malware database portion. The result of comparison is shown in Table 1.

Table 1: comparison between all solutions

Solution	Security Scope	Cloud-based	Third-party antivirus	Description
SocialAV	Sharing the content within a social network	No	Yes, single antivirus	-Distribute AV database between multiple mobile devices -Partially dependent on the central unit (cellular network)
Secloud	Downloading applications	Yes	Yes, multiple antivirus	- Use multiple cloud-based antivirus programs - Need to have a full replication of the device in the cloud - Full dependency on the cloud
Proposed solution	Sharing the contents within a social network	Yes	Yes, multiple antiviruses	- Use multiple cloud-based antivirus programs - All security members simultaneously scan files to detect viruses Distribute AV database between multiple mobile devices Partially dependent on the cloud

3. Implementation and Overall Architecture

The proposed model (see Figure 1) is a social network antivirus software that detects malicious URLs and scans malicious files and documents transmitted within a chatting group. The solution benefits from off-the-shelf antivirus programs, such as ClamAV [5] and virusTotal [3]. The aim of the proposed solution is providing real-time and high-level protection to messenger functionalities on social media without consuming excessive mobile resources and without overhead costs. Therefore, all mobile devices, regardless of their type, capabilities, and operating systems, can benefit from this advancement.

The implementation of the proposed solution consists of four main parts: (1) cloud computing, (2) chat room environment, (3) multiple off-the-shelf antivirus tools, and (4) security guard members. Security guard members are trusted and well-known members. Their responsibility is scanning shared URLs and documents to detect malware and malicious behavior inside the chat groups.

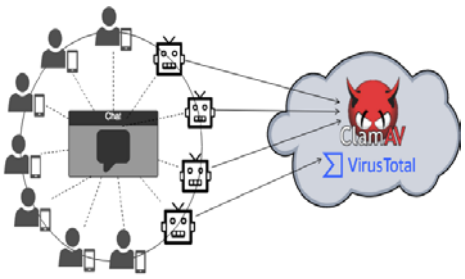

Fig. 1 Proposed solution

3.1 Cloud Computing Role

Cloud computing is a central node acting as a management unit. The cloud is used in the initial state to specify all security guard members in the chat group and distribute the database of antivirus between them. The proposed solution uses the Linux operating system (Ubuntu 14.04 LTS) with 10 GB disk size and a virtual processor (1 vCPU, 3.75 GB memory) located on Google Cloud. It also installs antivirus tools inside the cloud and then distributes its database between multiple members.

3.2 Chat Room Environment

The proposed model has implemented on Telegram Messenger, which is an open-source application and benefits from their Bot Platform [4] to represent security guard members.

3.3 Security Guard Members

Security guard members are responsible for applying a collaborative malware-detecting technique, a decentralized solution where specific members in the chat group will collaborate to detect malware by scanning the files and URLs using its antivirus database portion and then providing the virus scanning results to all other members. In the proposed approach, different chatbots have implemented [4] on Telegram API. Chatbots collaborate to filter all URLs and documents sent through the chat. The chatbots represent the security guard members in the proposed model that receive the antivirus database from the cloud and use it in virus scanning to provide a secure chat environment to all chat members.

3.4 Multiple Antiviruses

The proposed model uses ClamAV [5], which is an open-source antivirus software, and VirusTotal [3]. ClamAV databases consist of 59,140 malwares signatures, so these signatures have distributed between multiple security guard members in order to reduce the size of the antivirus database and make the tool suitable for running on mobile devices with limited capabilities.

4. Discussing Results

4.1 Increase Accuracy Using Multiple AV Tools

ClamAV is suitable for scanning different types of files, such as text, pdf, png, etc. However, it is not suitable for scanning URLs. Therefore, it is insufficient to use only ClamAV antivirus software to secure a social media environment as there are a huge number of malicious links transmitted within social media by fraudulent users to compromise other devices via these malicious links. The attackers can gain access to a person's mobile device; obtain their sensitive information, including bank account data; or remotely control and access the camera and other mobile resources. The proposed suggestion is deploying VirusTotal in addition to ClamAV and dedicating VirusTotal for scanning URLs. Consequently, using multiple antivirus tools will increase the level of security in a social network environment.

4.2 Scanning Files Concurrently to Speed up the Response Time

Security guard members can be either multiple admins of a social group who use a normal mobile device or they can be chatbots connected to the social network. The implementation of the proposed model is accomplished on the Telegram Bot API to prove the reliability of its virus scanning ability. There are three chatbots in the model representing ClamAV and one representing VirusTotal. Accordingly, each chatbot is associated with the Telegram chat group and connected to a Python antivirus application hosted in the cloud. All chatbots then collaborate together and run their Python antivirus applications concurrently to provide a secure chat environment that scans each message transmitted inside the chat, including URLs, images, documents, etc.

All chatbots work concurrently to scan files and messages, in contrast to SocialAV, which scans a file by forwarding this file sequentially between peers. In this situation, each peer scans the file by his own database portion, and after failing to detect viruses, the peer asks his next neighbor to scan the file and relay him a report. This process is repeated until a virus is detected or once the file has been forwarded to all peers. In my opinion, a concurrent scan is better than a sequential scan because as soon as a file or URL is sent, all virus scanning will be executed as rapidly as possible to check the safety of the file. Thus, the response time is reduced and increased the scanning speed rather than waiting for a sequential process to be completed.

4.3 Distributing the Database of Antivirus Software to Provide a Lightweight Solution

ClamAV is a desktop antivirus tool that uses a huge virus signature database. Therefore, deploying the whole package inside a mobile device would consume a lot of memory and processor space. Thus, in the proposed model, as in the previously discussed SocialAV mode, [1], the database of ClamAV antivirus software have distributed between multiple mobile devices.

In the proposed model, the database of ClamAV antivirus has distributed between three ClamAV chatbots to reduce

the size of the program and make it suitable to run on mobile devices with limited resources (e.g., CPU, memory). The sum of all three chatbots will provide the same virus scanning result as traditional ClamAV.

4.4 Replacing a Cellular Network with Cloud Computing to Reduce the Overall Cost for Individuals

Using a cellular network as a central management unit has a constraint on the amount of transmitted data and limits the additional cost for each communication between the cloud and peers. Consequently, using a collaborative malware-detecting technique by changing the central unit from the cellular network to the cloud will reduce the cost for individuals. In general, all members can benefit from scanning services without paying any extra costs. However, we still need to pay the cost for use of the cloud to host the antivirus software and applications that manage database distribution.

5. Evaluation and Data Sets

5.1 Data Sets

Data sets used to examine the model (1) are malicious and clean URLs that test the virusTotal bot application or (2) use malicious and clean files (pdf, images) to test collaborative ClamAV bots.
Accordingly, some of the malicious links collected that broadly spread across social networks, such as WhatsApp, that attract users to click on malicious links by offering gifts and discounts from familiar market stores. However, testing clean links is done by a group of clean web pages available on the Internet. To test ClamAV, the EICAR text file had scanned, which is a file considered to be malicious and designed specifically to test antivirus software. Also some clean files had scanned as a control.

5.2 Evaluation

In this section, the main enhancement will be evaluated in the proposed model: (1) response time and result of the antivirus software on the model, (2) proof of the cost-effectiveness of using the cloud in the model, and (3) the amount of memory and CPU consumed by the model. Finally, I demonstrate how the model improves the security level of the social network by using multiple antivirus techniques. How the approach works in practice

5.3 Response Time and Virus Scanning Result

The Chatbot platform (Telegram API) receives and scans messages from users in a specific group. Table 2 below shows the response time and result for each type of message (URL, file, document, text, image).

Table 2: Response time and result

Antivirus	Data type	Sample	Size	Response time	Result
ClamAV	Text file	Malicious Eicar	69 bytes	13.868 sec	True/ Negative
		Clean	4.0 kB	13.868 sec	True/ Positive
	pdf file	Clean	283kB	14.386 sec	True/ Positive
VirusTotal	URL link	Malicious	----	1 sec	True/ Negative
		Clean	----	1 sec	True/ Positive

Table 3 shows the cost of cloud use for the model and the amount of computational and memory resources used by the model.

Table 3: Cost and amount of mobile resources consumed

Cloud	OS	disk size	Memory Consumption	CPU	CPU Consumption
Google cloud platform	Linux/ Ubuntu 14.04 LTS	10 GB	Management DB	3.75 GB	Management DB
			VirusTotal		VirusTotal
			ClamAV		ClamAV

6. Conclusion

By implementing this technique, users will no longer have to worry about the security of a given chat room. The security responsibility will be on the shoulders of the chatbots. In this way, we can provide a secure chat environment for all chat members, regardless of their mobile device capabilities.

References

[1] L. Yang, V. Ganapathy and L. Iftode, “Enhancing Mobile Malware Detection with Social Collaboration”, 2011 IEEE Third Int’l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int’l Conference on Social Computing, 2011.
[2] S. Zonouz, A. Houmansadr, R. Berthier, N. Borisov and W. Sanders, “Secloud: A cloud-based comprehensive and lightweight security solution for smartphones”, Computers & Security, vol. 37, pp. 215-227, 2013.
[3] “VirusTotal", Virustotal.com, 2018. [Online]. Available: https://www.virustotal.com/. [Accessed: 11- Sep- 2018].
[4] “Telegram Bot API”, Core.telegram.org, 2018. [Online]. Available: https://core.telegram.org/bots/api. [Accessed: 11- Sep- 2018].
[5] “ClamavNet”, Clamav.net, 2018. [Online]. Available: http://www.clamav.net/. [Accessed: 11- Sep- 2018].
[6] “Malware Sample Sources for Researchers”, Zeltser.com, 2018. [Online]. Available: https://zeltser.com/malware-sample-sources/. [Accessed: 11- Sep- 2018].

[7] "theZoo aka Malware DB by ytisf", Thezoo.morirt.com, 2018. [Online]. Available: http://thezoo.morirt.com/. [Accessed: 11- Sep- 2018].

Omar Batarfi received his B.S. degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia in 1989 and his M.S. degree in Artificial Intelligence from George Washington University, Washington, D.C., USA in 1996. He received his Ph.D. from University of Newcastle Upon Tyne, UK in 2008. From 2008 to 2016, he was an Assistant Professor with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. He is currently an Associate Professor of Networking Security at Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include Big Data, Cloud Computing and Information Security.