Study on implementing tor communication in connection to storage service provider

Erika Ramadhani\textsuperscript{1,*} and Fietyata Yudha\textsuperscript{2}

\textsuperscript{1,2}Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

*erika@uii.ac.id

Abstract. The problem of the Storage Service Provider (SSP) is there is no standardisation for the privacy and security. The user can not ensure the availability and reliability of the system. Currently many types of SSPs include Google Drive and Dropbox. To determine the toughness of the system against suspicious activities, a test is carried out by accessing the SSP page and performing a login process using Tor communication to determine the response of the SSP system. The results show that the Google Drive and Dropbox systems consider Tor communication to be a suspicious activity to their system. This shows that the Google Drive and Dropbox systems have actions against suspicious activities that can interrupt the security of system.

1. Introduction

In current situation there are several type of Storage Service Provider (SSP) such as Google Drive, Dropbox, SkyDrive, etc. The use of SSP give a lot of benefit to the user, i.e., provide data storage, data retrieval, data backup and other function. the implementation of SSP in the system makes the system easy to synchronize with other hardware in anyplace and anytime. Another benefit from the SSP also give a cheap infrastructure, the developer of system do not need to scalable the system based on the adding of hardware, only by connecting to the SSP then the storage will add in the cloud based infrastructure.

The problem with the SSP cloud storage that there is no standardisation, which is the user do not know the boundaries of the cloud system. The user do not know the system are shared to another device or not, also the user can not ensure the availability and realiability of the system \cite{1}. Another concern in cloud storage is privacy and security in the cloud storage \cite{2}. Security is the most priority aspect, identity management and authentication are two of the most crucial things in a cloud system \cite{3}, \cite{4}.

According to these two concern, we are experimenting Google Drive and Dropbox to see the response of both systems when connected to the Tor network. The use of Tor network because it is a network form that works anonymously. We want to study what the effect of SSP to this such a communication, whether it is a threat or not when communicating to the SSP. If the Tor network is considered a threat, then how does SSP management respond to this. The experiment is done by building a Tor client, then accessing the Google Drive and Dropbox pages and then logging in.

The result of this paper indicate that Tor communication detected as threat for the SSP. There are several action response from the SSP that reject the connection of Tor such as the verification of user that come repeatedly. The result of this paper is a response of the SSP from Google Drive and Dropbox, that can be use as a reference of security when to develop the cloud drive system.
2. Tor Communication

The onion router (Tor) is a type of anonymity communication that uses routing process to reach the destination. In Tor network, routing process traverses to some hops and encryption process, which is the encryption done three times. The process hoping and encryption make the communication of Tor become anonymous. This type of communication is designed to secure cyberspace and empower cybercitizens [5][6][7][8].

3. Storage Service Provider

Cloud storage is a service for storing data, managing and backing up remotely and making that data available when accessed by users via the internet. There are many types of cloud storage providers, including Dropbox, Google Drive, Box, Amazon, Apple Cloud, and Microsoft SkyDrive. Several types of SSPs are a form of cloud computing services that include the Storage as a Service (StaaS) service that facilitates cloud applications for limited scale server systems [9][10][11].

4. Material and Method

The purpose of this paper is to see the response of the public storage Dropbox and Google Drive when connected to the Tor communication channel. The scenarios from this study are done by opening the Dropbox and Google Drive home page, then entering the login process, and recording what happened. To implement the scenario, we build the system that consists of WiFi onion router where the wifi have a Tor communication service, then a general WiFi where the system is not suit with the Tor communication. The use of general WiFi is to compare what the response of both Google Drive and Dropbox. WiFi onion router is build using Raspberry Pi, we use this hardware because it is easy to implement and portable. The use of this Raspberry also can be as a reference to make a dual WiFi to make a flexible connection, which is we don’t need to install a Tor application when we want to connect with anonymity.

![Figure 1. Architecture of wifi onion router](image)

5. Result and Discussion

In this section we discuss about the result of accessing the cloud storage, i.e., Dropbox and Google Drive with and without Tor based communication. We capture every result according to the scenario that discussed in the section 4.

5.1. Checking the Tor connection

To check the connection of Tor is by seeing the IP address using www.whatsmyip.org. From the Figure 2, the hostname refers to the Tor exit mrkrabs.exit.tor4us.net. While in the Figure 3, the route of Tor communication is show, there are 12 hops in the route to reach the exit Tor system supposed the communication pass the onion node in the Tor network.
In Tor communication, the IP address will change every 9-10 minute that is make the communication anonym. According to the experiment, the first time we test our IP address is 104.244.76.13. Then refresh it after 10 minute, the IP address become 192.254.134.242.

5.2. Accessing public cloud drive
In this section we experiment with Tor communication to connect with public cloud drive such as Google Drive and Dropbox. There are several requirement occurs when we use Tor connection, this requirement may be a reference to secure the system when we want to build the cloud drive.

5.2.1. Dropbox. The first time we connect to dropbox, it lead to the login page, then we submit our email and password. After that, the system give a confirmation captcha image as a feedback. The different when we use a normal connection, dropbox will lead to the dashboard, but not in the Tor connection. Confirmation captcha image repeatedly show up and not end with the dashboard of Dropbox. This happen because the Dropbox detect the wrong connection in their system so that the system give a feedback such as a repeatedly captcha image confirmation as depict in Figure 4. Captcha
image showed up because the system want to verify user are human not a robot. When using Tor communication, the system makes user look suspicious to reCaptcha algorithm.

5.2.2. Google Drive. We connect to the drive.google.com url then automatically the google system read the location of the user. While we use Tor communication, our IP address located in hungaria, then the google lead us to the hungaria based language in their system. Then lead to the login page to submit username and password. After login in, the system lead to the page to verify the user. Google drive using an sms to verify the user as depict in Figure 5. Because of Tor communication, our sms that send from google is not reaching to the phone number that has submit in the form. After a while, google system notify the user to the email that there is a suspicious activity on the login session.

Figure 4. Captcha image

Figure 5. Google drive verified

From the result in the section 4, any action from the Google Drive and Dropbox can be summarized in the Table 1. The result in the Table 1. can be the security requirement in the public cloud storage as a reference when to develop the cloud storage system. We conclude the three action, i.e., opening page, login session, and suspicious activity handling. Dropbox not set their language according to the location of user, while Google Drive change their language according to the location of user. In the login session,
both Dropbox and Google Drive give a normal login activity session submitting the username and password. Then after submitting the username and password, both cloud storage detect the suspicious activity in their system. Dropbox doing a verification of user by using the captcha image, while Google Drive giving a verification of user by sending the code via sms to user. Another action in Google Drive while their system detect the suspicious activity is their system notify the user by sending the email and inform the user about the suspicious activity.

| Cloud Storage | Action            | Requirement                    |
|---------------|-------------------|--------------------------------|
| Dropbox       | Login session     | Username and password          |
|               | Suspicious activity handling | Re-captcha image               |
| Google Drive  | Login session     | Username and password          |
|               | Suspicious activity handling | Notify the user via sms, and report to email |

Table 1. Summary of security action

5.3. Accessing Dropbox and Google Drive using normal communication
During normal communication, Dropbox and Google Drive generate normal responses when accessing web pages and logins. There are no notifications regarding suspicious activities from the system. In the dropbox system, the login process will still display the captcha page to maintain the security of the system, but there is no re-captcha action repeatedly.

5.4. Recommendation
A recommendation for making cloud storage is discussed in this section. based on the results of the experiment, a cloud storage model was created that was able to detect Tor's communication. To detect Tor communication on the system, referring to research [12], the Tor communication detection process is carried out based on the list of Tor servers. Determination of the Tor server is taken from the process of analyzing network traffic that matches the source and destination IP addresses for each connection with the Tor server list.

6. Conclusion
The conclusion of this paper shows that the Tor communication detected as a threat in the SSP both Google Drive and Dropbox. There are several action response that give from the SSP, we summarized in three action, i.e., opening page, login session, and suspicious activity handling. From those kind of point activity response, we can use it as a reference in the future when to build our own policy cloud drive system.

7. References
[1] D. Zhe, W. Qinghong, S. U. Naizheng, and Z. Yuhan, “Study on Data Security Policy Based On Cloud Storage,” pp. 145–149, 2017.
[2] S. Baker, W. Xiang, S. Member, and I. Atkinson, “Internet of Things for Smart Healthcare : Technologies , Challenges , and Opportunities,” vol. 3536, no. c, pp. 1–25, 2017.
[3] M. Computing, E. Sasi, and R. Saranyapriyadharshini, “RESEARCH ARTICLE SECURED BIOMETRIC AUTHENTICATION IN CLOUD SHARING SYSTEM,” vol. 4, no. 3, pp. 572–577, 2015.
[4] P. A. Crocker and R. Azevedo, “E-Ild Authentication and Uniform Access to Cloud Storage Service Providers,” 2013.
[5] E. Ramadhani, “Anonymity communication VPN and Tor: a comparative study,” in *Journal of Physics: Conference Series*, 2018.

[6] P. Syverson, “Practical Vulnerabilities of the Tor Anonymity Network,” 2015.

[7] A.-M. O. Emin Çalışkan, Tomáš Minárik, “Technical and Legal Overview of the Tor Anonymity Network,” 2015.

[8] G. Danezis, S. J. Murdoch, and G. Danezis, “Low-cost traffic analysis of Tor Low-Cost Traffic Analysis of Tor,” no. November, 2015.

[9] A. N. Beagrie, A. Charlesworth, and P. Miller, “Guidance on Cloud Storage and Digital Preservation How Cloud Storage can address the needs of public archives in the UK,” no. March, pp. 1–39, 2015.

[10] M. Computing, M. L. Neelima, and M. Padma, “A STUDY ON CLOUD STORAGE,” vol. 3, no. 5, pp. 966–971, 2014.

[11] V. Spoorthy, M. Mamatha, and B. S. Kumar, “A Survey on Data Storage and Security in Cloud Computing,” vol. 3, no. 6, pp. 306–313, 2014.

[12] V. Prenosil, “TOR-BASED MALWARE AND TOR CONNECTION DETECTION,” no. May, 2016.