Machine Learning based Authentication Scheme to secure the Phishing Attack

[1]Vidyashree, [2]Dr.Mohammed Abdul Waheed

[1]Student, [2]Associate Professor
Department of Computer Science and Engineering
VTU Regional Center for PG studies Kalaburagi, India

Abstract*: One of the grave threats to smart phone users is a phishing attack. According to the latest lookout study, mobile phishing attack is rising annually by 85 per cent and will become a major threat to users of smart phones. Social engineering aims to get the password from the user by disguising himself as a trusted service provider. Many users of smart phones use the Internet infrastructure outside of the conventional firewall. Cloud-based documents are among the primary targets of mobile cloud computing for this phishing attack. Often, most Mobile users use their device's cloud storage. In order to prevent this password attack in a mobile cloud environment, we are proposing a new authentication scheme to provide novel security to the mobile cloud services. This scheme will verify the user and service provider using the Zero-knowledge proof-based authentication protocol, without password transmission. The scheme proposed will also include mutual authentication between the communications entities. The feasibility of the proposed scheme will be checked using Scyther, a protocol verification method. This project further proposes with machine learning technology for detection of phishing URLs by extracting and analyzing various features of legitimate and phishing URLs. Decision Tree algorithm, random forest algorithm and Support vector machine algorithms are used to detect phishing websites. The main theam of this paper is to detect phishing URLs as narrow down to best machine learning algorithm by comparing false positive and false negative rate and accuracy rate of each algorithm.

***Index Terms*: Scyther, Smart phone, Cloud, Novel Security**

I. INTRODUCTION

Mobile cloud is a hybrid computing platform that combines the advantages of cloud computing with cellular technology to build a modern mobile cloud computing (mcc) model. Figure 1 shows the general view of mobile cloud computing, mcc is the technology would help to overcome the hardware limitations such as processing, storing and networking on mobile devices for end-users. Authentication is one of the key obstacles to protection in the mobile cloud world. Authentication is an method for testing user identity originality. Using mobile devices and/or one or more other authentication methods, user identity can be checked in mobile cloud computing in the recent scenario, maximum protocols are to exchange or send the password to the verifier or the authentication server in the form of a hash value or the encrypted type. The attacker will catch the password that is being transmitted. This will also allow the phishers to create fake website or service capturing the user password. The purpose of this paper is not to submit the user password at any point of the communication process to the authentication server or cloud service providers. Therefore, this paper not allow delivering the user password out of end-user device, even to the trusted third party.

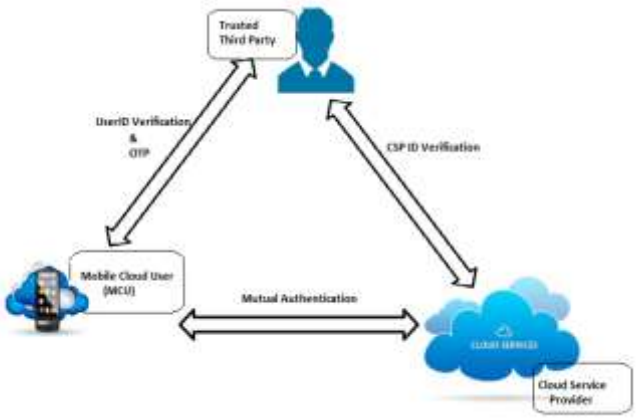

Fig. Proposed System

I. REALTED WORK

In 2013, Mohil et al. [16] this proposed a scheme based on PIN number and preconfigured voice prints to verify the identity of authentication user this method is proved to use more computation. Hence, it is not useful due to more computation and the power usage in a mobile device.

In 2015, Lin et al. [12]they introduced a secure method in the smart learning application in the cloud environment. This scheme registers user with original user ID in the authentication server (AS). This scheme sends the hash value of password to the authentication server in the encrypted form. The AS decrypts and can get the hash value of the password. This scheme was secure against the man-in-the-middle attack, but not safe against the phishing *attack due to password sharing between the communication entities.*

In 2016, Kalra et al. [17] and Huang et al. [18] proposed strong authentication based one-time password (OTP) and Message Digest value. This [17] scheme uses USIM with a secure channel to share the user identity. Hence, this scheme is not defined when the mobile device is missed or stolen. This [18] scheme uses the traditional password to verify the authentication phase, but the chance of cracking password in the server side. Hence, this is prone to phishing attack by the server side.

Researchers in several efforts (Yang et al., 2014; Li and Li, 2014; Si et al., 2014; Xia et al., 2014; Sookhak et al., 2014; Kaewpuang et al., 2013; Rahimi et al., 2013; Yang et al., 2013; Ma and Wang, 2012; Satyanarayanan et al., 2009; Ra et al., 2011) have studied varied aspects of MCC, including task outsourcing, heterogeneity, virtualization, energy saving, and remote auditing, aiming to enhance the MCCs performance and efficiency.particularly authentication is overlooked. The security challenges in MCC are twofold, namely cloud security and mobile network security because of the coexistence of cloud computing and mobile computing in MCC

(*Peng et al., 2014; Morrow, 2011; Zissis and Lekkas, 2012; Dijiang et al., 2011).* One of the most important security issues for MCC users is authentication and authorization (Esposito and Ciampi, 2015; Yu and Wen, 2012; Riley et al., 2011). As an example, a lost or stolen mobile device could be abused to access a host and download sensitive data from the cloud, if a mobile user is registered with a particular cloud service provider, both mobile device and cloud server should authenticate each other in order to secure the communication when the mobile user accesses the cloud from different locations using heterogeneous networks and various mobile device**.**

II. PROPOSED SYSTEM

The proposed authentication scheme has three phases.

- The first phase creates a group called G and its members. The TTP shares elements of group to the communication entities.
- The second phase handles registration of cloud user and CSP with the authentication server or a trusted third party.
- The third phase verifies cloud user and the service provider to achieve the mutual authentication process.

Initial Registration. Group G is having their set of values as G0, G1 are the carrier set of the random elements of group G [21, 23, 24, 29] public key may be G, G0. G is a Group carrier set cordiality of the order of Group |**?**|. Hence the

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified. Digital payment is like Bitcoin which uses sec256k1 group, based on elliptic curve. The Element size of this group is 256-bit strings, which is very hard in type of group [21].

Registration Phase. This phase accepts registration of cloud user and cloud service provider by the authentication server process. new user generates request with authentication server with its mobile number being of original identity. AS is always verifies list of available registered mobile numbers. If the number is new, AS sends OTP or else it terminates communication. The entered OTP will get Mobile Cloud User (AS) – TTP New Registration Request If Req. is new, Generate & Sends OTP Verification Success Verifying OTP Registering Public Key, Mobile No. & URL. User registration with authentication server. Once OTP is verified, then user enters the new user ID and password, mobile browser generates hash value of the user ID as H1 and generates a hash value of password as H2. Thease all communications are happening over a secure channel between AS and User. Cloud service provider, service and domain registration with authentication server and CSP generate a new request to AS and verifies existence of new domain in the existing list. If they free, AS accepts the request and generates domain tag with new unique one-time key.

Authentication Phase. This phase, authentication server, mobile cloud user and cloud service provider are participating in verifying user and CSP through the AS to they achieve mutual authentication without revealing real password between communication entities. Finally proposed authentication is using mobile number as an original identity to register the user. Once the user is registered successfully, the AS will generate the unique link to the client as follows. User mobile number is 9xxx7; when this user registers with authentication server they will get unique web URI called client URI as 9xxx7.myauth.in. Te AS will maintain the mobile number, client URI, hash value of user ID, public key of user as client profile like Table 2. User U sends the service request to CSP with participant mobile identity to the Cloud service provider.

III. ALGORITHMS AND METHODOLOGY

A.URL based

Using the IP Address

IP address is used as an alternative of domain name in the URL, such as "http://125.98.3.123/fake.html", users can be sure that someone is trying to hack their personal sensitive information. Sometimes, IP address is even after transformed into Hexadecimal code as shown in
"http://0x58.0xCC.0xCA.0x62/2/paypal.ca/index.html".

Rule: IF The Domain Part has an IP
Address → Phishing
Otherwise→ Legitimate

The **Long URL to Hide Suspicious Part :**
Phishers can use long URL to hide the doubtful part in the address bar.
For example:
http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&dispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8@phishing.website.html
To ensure accuracy of our study, we must calculate the length of the URLs in the dataset which is produced an average URL length. Results showed that if the length of URL is greater than or else equal to 54 characters then the URL classified as phishing. By reviewing always our dataset we were able to find 1220 URLs lengths equals to 54 or more which is constitute 48.8% of total dataset size.
Rule: IF URL length is ≤ 75→legitimate
otherwise→Phishing
We have been always able to update this feature by using a method based on frequency thus improving upon its accuracy.

Adding Prefix or Suffix which is Separated by (-) to Domain:
The dash symbol is rarely used in legitimated URLs. The Phishers which tends to add prefixes or suffixes which is always separated by (-) to the domain name so that their users feel that they are dealing with the legitimate webpage.
For example http://www.Confirme-paypal.com/.
Rule: IF Domain Name Part Includes
(-)Symbol → Phishing
Otherwise → Legitimate

Submitting the Information to Email :
The Web form allows a user to submit their personal sensitive information that is directed to the some initiative server for processing. The Phisher might provides and always redirect user's information to personal email. At the end, a server-side script language might be used such as "mail()" function in PHP. One more client-side function that might be used for this purpose is the "mailto:" function.
Rule: IF Using ""mail()\" or \"mailto:\" Function to Submit User Information" → Phishing
Otherwise → Legitimate

Using Pop-up Window :
It is unusual to find a legitimate website asking users to submit their personal information through a pop-up window. On the other hand, this feature has been used in some legitimate websites and its main goal is to warn users about fraudulent activities or broadcast a welcome announcement, though no personal information was asked to be filled in through these pop-up windows.
Rule: IF Popup Window Contains Text
Fields→ Phishing
Otherwise → Legitimate

B. Blacklist based
A Blacklist is created in the proposed model in which the website detected as phishing is saved for the future use a to keep a track record and data of the phishing website can be useful in analyzing the phishing website to increase the efficiency of the system.

C. WHOIS Database
The life of phishing site is very short, this DNS information may not be available after some time. If the DNS record is not available anywhere then the website is phishing. If the domain name of suspicious webpage is not match with the WHOIS database record, then webpage considers as phishing.

Cloud User (U). He/she is a mobile cloud user. He/she is registering as a new user with the TTP using one-time password to confirm the original identity. Then the user uses its user ID and password to generate public key with using mobile application and then sends the mobile number, user ID, and public key with client URL to the TTP.

Trusted Third Party (TTP). TTP is working as authentication server, responsible for verifying requested user and the cloud service provider. After initial verification, it is receiving the public key from the cloud user.

Cloud Service Provider (CSP). The CSP provides services like storage, computation, and communication service to the mobile cloud user. It verifies the user request with its URI. If URI is on the approved list, it will ask TTP for verification. Then TTP verifies the mobile number and the user ID. Finally user ID, TTP nonce, public key will send to CSP to confirm cloud user.

IV. EXPERIMENTAL RESULTS

Fig : Main Screen

This is main screen of the project which consists of three modules. They are Mobile user, TTP amd CSP. Through this we can interact with these above said modules.

Fig : User Register

This is used to register the users. The user can register themselves by entering all his details in the formsuch as fullname, contact, email….

Fig User Login

This is used to login the user by entering their username and password.

Fig : Generate Key and Send URL

In this module, the user uses its user ID and password to generate the public key with using mobile application and then sends the mobile number, user ID, and public key with client URL to the TTP.

Fig TTP Login

This module is used login for the TTP for user verification purpose

Fig : CSP Registration

Fig : View Request

Fig : Verify and send key to the user

[1]Vidyashree, [2]Dr.Mohammed Abdul Waheed
[1]Student, [2]Associate Professor
[1] Dept of Computer Science and Engineering
[1]VTU Regional Center for PG studies Kalaburagi, India
[1]vidyashrees15@gmail.com, [2]drmwaheed@gmail.com

V. CONCLUSION

To secure against this password attack in a mobile cloud environment, we propose a new authentication scheme to provide novel security to the mobile cloud services. This scheme will verify the user and service provider without transmitting the password using the Zero-knowledge proof based authentication protocol. Moreover, the proposed scheme will provide mutual authentication between the communication entities.

REFERENCES

[1] A. Mantovani, F. Marchesi, A. Malesci, L. Laghi, and P. Allavena, "Tumour-associated macrophages as treatment targets in oncology," Nature reviews Clinical oncology, 2017.
[2] J. C. Kagan and G. M. Barton, "Emerging principles governing signal transduction by pattern-recognition receptors," Cold Spring Harbor perspectives in biology, vol. 7, no. 3, p. a016253, 2015.
[3] X. Xiao, X. Cheng, S. Su, Q. Mao, and K.-C. Chou, "pLoc-mGpos: incorporate key gene ontology information into general PseAAC for predicting subcellular localization of Gram-positive bacterial proteins," Natural Science, vol. 9, no. 09, p. 330, 2017.
[4] A. Fatica and I. Bozzoni, "Long non-coding RNAs: new players in cell differentiation and development," Nature Reviews Genetics, vol. 15, no. 1, pp. 7–21, 2014.
[5] A. Bojarczuk, K. A. Miller, R. Hotham, A. Lewis, N. V. Ogryzko, A. A. Kamuyango, H. Frost, R. H. Gibson, E. Stillman, R. C. May, S. A. Renshaw, and S. A. Johnston, "Cryptococcus neoformans Intracellular Proliferation and Capsule Size Determines Early Macrophage Control of Infection," Scientific Reports, vol. 6, p. srep21489, Feb. 2016.
[6] J. F. Gibson and S. A. Johnston, "Immunity to Cryptococcus neoformans and C. gattii during cryptococcosis," Fungal Genetics and Biology, vol. 78, pp. 76–86, May 2015.
[7] H. Irshad, A. Veillard, L. Roux, and D. Racoceanu, "Methods for Nuclei Detection, Segmentation, and Classification in Digital Histopathology: A Review-Current Status and Future Potential," Biomedical Engineering, IEEE Reviews in, vol. 7, pp. 97–114, 2014.
[8] M. N. Gurcan, L. E. Boucheron, A. Can, A. Madabhushi, N. M. Rajpoot, and B. Yener, "Histopathological Image Analysis: A Review," IEEE Reviews in Biomedical Engineering, vol. 2, pp. 147–171, 2009.
[9] W. H. De Vos, L. Van Neste, B. Dieriks, G. H. Joss, and P. Van Oostveldt, "High content image cytometry in the context of subnuclear organization," Cytometry Part A, vol. 77A, pp. 64–75, Jan. 2010.
[10] M. B. Resnick, T. Konkin, J. Routhier, E. Sabo, and V. E. Pricolo, "Claudin-1 is a strong prognostic indicator in stage II colonic cancer: a tissue microarray study," Modern Pathology, vol. 18, p. 511, Apr. 2005.