RESEARCHERID
THOMSON REUTERS

[Kumar* *et al.*, 6(5): May, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY ENHANCEMENT FOR CLOUD DATA THROUGH A TWO FACTOR APPROACH

T. Senthilkumar*, S. Prabakaran, Jaya Verma, Revathi Reddy
* Department of Computer Science and Engineering,
SRM University, Kattankulathur – 603203, Tamil Nadu, India

DOI: 10.5281/zenodo.573549

ABSTRACT

The rate of upgrading traditional mobile phones to smartphones is escalating due to the functionality they provide. A multitude of data is stored in phones and many applications require a great deal of memory to run. However, smartphones have limited memory. This limitation can be overcome by using cloud storage. It also provides services like easy data access and sharing. Since the cloud storage is generally hosted by third parties, there is a risk of unauthorized access to data and security is one of the primary concerns. In this paper, we propose a two-factor approach for enhancing the security of cloud data. The system allows the user to store encrypted data in the cloud. Data is encrypted using user's secret key and device id. The user needs to possess both the security key and device key for decrypting and accessing the data. Since the device key is directly extracted from the device, we need to use the same device for encryption and decryption. Even if the device is lost or stolen, it cannot be used to decrypt data due to lack of security key. If the CSP tries to steal data, it will be missing some keys and hence will be unable to decipher the information.

KEYWORDS: Two factor, cloud storage, mobile security.

INTRODUCTION

Traditional mobile phones are increasingly being replaced by smartphones. One of the reasons for this growth is the availability of various applications for entertainment and work apart from the mobile telephony functions. One of the distinct features of smartphones is the availability of a large number of applications which can be downloaded from the app markets. However, this feature also exposes users to security threats as it is easier for hackers to distribute malware. They can disguise malware as useful apps and distribute them in app markets.There are many other channels for malware to affect targets. They can use the inbuilt sensors like GPS, microphone or camera. The data collected by some legitimate apps can also be utilized by malware since most of the apps request unnecessary permissions and do not provide options to the user to choose only the required permissions. Some malware can also intercept SMS messages to get confidential information like bank account details. Phishing links can also be sent through e-mails and messages. The data collected by malware can be sent to external agents through networking functions like Wi-Fi or Bluetooth.

Smartphones are also being utilized for business use. The employee-liable BYOD (Bring Your Own Device) model is gaining popularity. However, most of the users are not aware of the fact that their smartphones are vulnerable to cyber attacks. A lot of personal data is often stored in smartphones. In-built sensors like GPS and camera can also be used for keeping the user under surveillance. The users are not aware of the various vulnerabilities which can make them susceptible to attacks. For example, most of the users do not know that the certificate information and browser security indicators should be checked for websites while performing security sensitive operations like online money transactions.

There are many services like e-commerce, net banking and instant messaging which are enriching user's experience. However, these services bring serious security concerns as the user details can be accessed and misused by third parties. Many banking applications require the user to use two passwords (two factors) where one is the login password and another is the one-time password sent to the user during money transaction. Our proposed system is analogous to a banking system where the user needs to use two security keys.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

The remaining part of the paper is constructed as follows: Section 2 provides a review of the works related to this field. Section 3 introduces the proposed model. The system architecture and algorithms used are elaborated in Section 4. Section 5 concludes the paper.

RELATED WORKS

In this section, we review the works related to mobile security. Daojing He et al. [1] provides a survey of the different types of attacks and vulnerabilities in smartphones. It describes various ways in which malware can collect sensitive information and send it to hackers. It also states the problems associated with mobile security like limited memory and CPU power of phones which restrict the sophistication of malware detectors. It also provides some measures which can be taken on the part of users and app market administrators to prevent malware. One of the problems with mobile security is that users are not aware of their phones being vulnerable to cyber attacks and the security measures which need to be taken. Bukelwa Ngoqo et al. [6] proposes a framework to forecast security behavior of student mobile phone users and find a relationship between awareness and behavioral intent. Questions are asked related to security areas like use of strong passwords, storage of sensitive information, use of antivirus software, downloading files and responding to suspicious email/SMS links. The level of awareness (LA) is calculated on the basis of user's scores for knowledge, attitude and behavior and a measuring tool is developed.

Dan Tao et al. [3] propose an automated testing system for performing security testing of mobile terminals. Virtualization technology is used for performing tests on the cloud platform. The proposed system checks for vulnerable apps and also their corresponding vulnerability levels.

Chaitrali Amrutkar et al [2] provide an analysis of different mobile browsers and conclude that most of them do not follow W3C guidelines. Due to a small screen, security indicators like lock icon or https prefix are not visible. The users do not have access to certificate information about the sites and hence can be tricked into visiting fraudulent sites.

Seyed Yahya Vaezpour et al [4] proposes a solution to the phone clone co-location problem when placed on cloud hosts. It states that the risk of information leakage is lesser when the user's phone clone is placed with his friend's clones instead of placing with stranger's clones. It implements the highest degree first algorithm to allocate hosts based on the user's communication graph and also calculates the potential risk of placing the clones together. Also, it provides a dynamic migration algorithm to shift the clones to another host when the risk becomes higher to prevent covert channel attacks. Zubair Md. Fadlullah et al. [5] provide a game theoretic algorithm to obtain a balanced set of QoS and security parameters for users by ensuring maximum possible security with least delay for the user and maximum bandwidth utilization for the network operator. The user sends his security and bandwidth requirements to the network operator. Greater security implies more delay and lesser delay implies compromising the security of the system.

Juan M. Perez et al. [7] addresses the problem of loss of control when data resides in the cloud. The cloud service provider may bypass the access control policies defined by the user and provide data to third parties. To overcome this problem, a novel cryptographic scheme is proposed. It also provides an authorization model for defining access control rules for the data.

In the study [9], Kevin Allix et al. conducts an analysis of different malware and proposes a naïve malware detection algorithm. This algorithm makes use of the localization features like packaging time digital certificates which are common among different malicious software. Vaibhav Rastogi et al. [10] discusses the transformation of one malware into another by using simple techniques like package renaming, data encoding and call indirections and how such malware can be detected.

PROPOSED WORK

Data from mobile phones can be stored in the cloud for efficient storage and easier access from different devices. However, there is a considerable risk in storing data in clouds as the data resides outside the organizational bounds. The Cloud Service Provider (CSP) can potentially access the stored data and provide it to third parties. If we provide access control rules then we have to rely on CSP for enforcing these rules.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Our model provides a data-centric solution for protecting data in clouds. It makes use of cryptography and authorization model for enforcing security. It uses a combination of proxy re-encryption (PRE) and identity-based encryption (IBE) for encrypting data. In PRE scheme, a proxy is used to re-encrypt an already encrypted data. In IBE scheme, the identity of users is used as a key for encrypting data. For our model, we use identity-based proxy re-encryption(IBPRE) in which a ciphertext encrypted using a user's identity is converted to another ciphertext using the user's device id or IMEI number.

An authorization model is used for defining access control rules for the data. It uses Role Based Access Control (RBAC) scheme in which a particular role is granted a set of privileges. A user can be assigned to one or more roles. The privileges define which user is allowed to decrypt data and get access to its contents.

ARCHITECTURE

The system comprises of a mobile device and databases for storing user details and user's files. The databases are hosted on private clouds. The users of the application are facilitated to store encrypted data in the cloud. The user details database stores the user's basic information name, email id, username, login password and user's response to verification question. Another database is used for storing the user's uploaded files. Once the user logs in, he can choose to either upload or download data. For both encryption and decryption, the user has to provide his secret key and the device id is extracted from the device. Hence there are three factors involved with security, the user login password, secret key and device id.

During registration, a role can also be assigned to the user. For example, if the user is assigned the role of sales manager, he can access files of sales department but cannot access files of purchase department. We can grant certain permissions to each role. These permissions and role's details are also stored in the database and matched during data access.

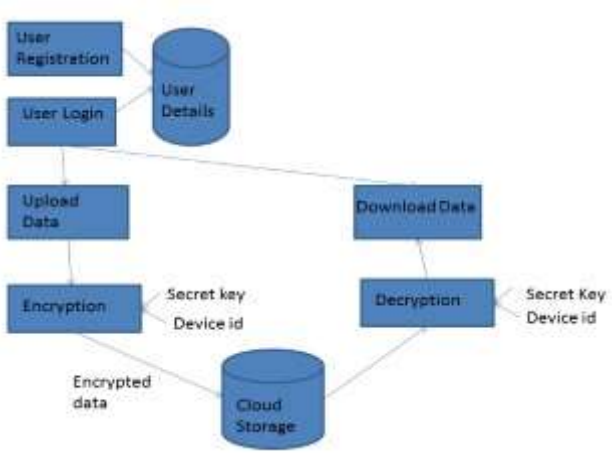

Figure 1: System Architecture

When data is moved to the cloud, its corresponding authorization rules are also stored in the database. These rules specify which users or which roles can access the data by decrypting it.

IMPLEMENTATION

User Authentication

User authentication involves two steps: registration and login. During registration, the user is asked to enter his details like email id, chosen user id and password. The user also needs to answer a verification question which is used when the user wants to reset his password. These details are stored in the database. During login, if the user id and password match a particular user then the user is successfully logged in.

Data Encryption

The proposed system uses a combination of proxy re-encryption (PRE) and identity-based encryption (IBE). PRE is a cryptographic scheme in which given a pair of keys a and b, the proxy can re-encrypt a ciphertext c_a encrypted using the key a to another ciphertext c_b using another key b. On the other hand, identity-based encryption (IBE)

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

is a scheme in which the key pairs for a given entity are extracted from the identity of that entity. Here we can use the device id as the identity value.

As a combination of PRE and IBE, we can use an Identity-based Proxy Re-Encryption (IBPRE) scheme. The user provided key is used as id_a and device id is used as id_b. The document file to uploaded is converted into ciphertext c_a using id_a and then re-encrypted to ciphertext c_b using id_b. This encrypted ciphertext is then uploaded to the cloud.
The encryption of data while uploading to the cloud follows the following series of steps:
(1) *encrypt(pub,* id_a*, txt)* → c_a
(2) *reencrypt(pub,* id_b*,* c_a*)* → c_b

User Authorization
For enforcing access control on data, we use the Role-Based Access Control (RBAC) scheme. This authorization model uses the concept of *Roles* for assigning privileges to users. Each role is associated with a set of privileges and each user can be assigned one or more roles. A privilege defines an action which can be performed on the object like access to data by decryption, modification, deletion etc. where an object can be any image or document residing in the cloud.
If *OB* is a set of objects residing in cloud and *A* is the set of actions which can be performed on those objects then a privilege *P* can be defined as
P :=(A,Ob,P) , P⊆A x Ob = {(a,ob) , a∈A, ob∈Ob}
A grant is used to assign a privilege to a subject or role. If *SUB* is a set of subjects and *R* is the set of roles then a privilege *G* can be defined as
G :=(SUB∪R, P, G) , G ⊆ SUB∪R x P = {(u,p) , u∈SUB∪R, p∈P}
Subject-role assignment *D* allows a subject *s* to inherit all the privileges granted to role *r*. It can be defined as
D :=(SUB, R, D) , D ⊆ SUB x R = {(s,r) , s∈SUB, r∈R}
We can also establish inheritance of privileges between roles. A child role can inherit all the privileges granted to its parent role. If r_1 is child role and r_2 is parent role then the parent role assignment *E* can be defined as
E :=(R, R, E) , E ⊆ R x R = {(r_1, r_2) , r_1∈R, r_2∈R}
The authorization rules are placed into the authorization model by including the elements in binary relations. Re-encryption keys are generated by using device id. Hence we do not need to store public and private keys for each element. Since all the cryptographic tokens are provided by the data owner, if a CSP tries to access data then it would miss some re-encryption keys and will not be able to decrypt data.

Data Decryption
When the user wishes to download data, he has to provide the security key which was given at the time of uploading. The system again extracts the user's device IMEI number and the data is decrypted using these two keys. It uses the following functions:
(3) *decrypt(*c_b*,* id_b*)* → c_a
(4) *redecrypt(* id_a*,* c_a*)* → txt
The ciphertext c_b is first decrypted using id_b which is the device id to generate ciphertext c_a. This is again decrypted using id_a which is the user-provided security key to generate the plaintext *txt.*

CONCLUSION
In this paper, we introduced a novel two-factor mechanism for cloud storage system in which allows the user to encrypt the data using his/her secret key and device key. It is impossible to decrypt data using these two pieces of information. Our solution enhances the confidentiality of the data and also prevents unauthorized access when the device is lost or stolen.
Further lines of research include extending the privileges of the authorization model to include actions like modification and deletion of data. We can analyze novel cryptographic techniques which can enable secure modification and deletion of data in the cloud.

REFERENCES
[1] Daojing He, Sammy Chan and Mohsen Guizani, *Mobile application security: Malware threats and defenses*
[2] Chaitrali Amrutkar, Patrick Traynor and Paul C. van Oorschot, *An empirical evaluation of security indicators in mobile web browsers*

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[3] Dan Tao, Zhaowen Lin and Cheng Lu, *Cloud platform based automated security testing system for mobile internet*
[4] Seyed Yahya Vaezpour, Rui Zhang, Kui Wu, Jianping Wang, Gholamali C. Shoja, *A new approach to mitigating security risks of phone clone co-location over mobile clouds*
[5] Zubair Md. Fadlullah, Chao Wei, Zhiguo Shi and Nei Kato, *Joint optimization of QoS and Security for differentiated applications in heterogeneous networks*
[6] Bukelwa Ngoqo and Stephen V. Flowerday, *Information security behavior profiling framework(ISBPF) for student mobile phone users*
[7] Juan M. Perez, Gregorio Martinez Perez and Antonio F. Skarmeta Gomez, *SecRBAC: Secure data in the Clouds*
[8] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, *Two-Factor Data Security Protection Mechanism for Cloud Storage System*
[9] Kevin Allix, Quentin Jerome, Tegawende F. Bissyande, Jacques Klein, Radu State and Yves Le Traon, *A forensic analysis of android malware: How is malware written and how it could be detected?*
[10] Vaibhav Rastogi, Yan Chen and Xuxian Jiang, *Catch me if you can: Evaluating android malware against transformation attacks*

CITE AN ARTICLE

Senthilkumar, T., Prabakaran, P., Verma, J., & Reddy, R. (2017). SECURITY ENHANCEMENT FOR CLOUD DATA THROUGH A TWO FACTOR APPROACH. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(5), 471-475. doi:10.5281/zenodo.573549