SECURITY AND PRIVACY RISK ON MOBILE CLOUDS OVER ADVANCED PERSISTENT THREAT

[1]Prof. Komal Jagdale, [2]Prof. Sheela Bankar, [3]Prof. Sonali Khairnar
[1]Assistant Professor, [2]Assistant Professor,[3]Assistant Professor
[1]Department of Computer Engineering,
[1]ISB&M School of Technology, Pune ,India

Abstract: Any person can gain access of his workplace personal data anytime at anywhere because of 5G network and cloud technology. The most appropriate way for us to access to cloud data is to use personal smart phone. On the other hand, Because of low security protection and limited computation resource, smart phone is somewhat vulnerable while facing with malicious attacks in open network. Attacker can penetrate to different levels of cloud as well as to infrastructure of mobile to steal and temper data, which may prone to new type of attack - advanced persistent threat (APT). This survey paper insights security and privacy risk of mobile cloud in the perspective of applied cryptography and also provides solutions for the risks.

Index Terms **- Mobile cloud, Applied cryptography, Advanced persistent threat, Security, Privacy.**

I. INTRODUCTION

Mobile devices connected to Internet which allows Internet users to take a benefit from many network services and applications much similar to desktop, to a large extent, cannot fully provide excellent user experiences for their users because of their constraints, including limited memory, processing power and battery life. To help mobile devices to move beyond the restrictions, mobile research and industrial communities invent a new framework. Mobile cloud, which is the junction of mobile devices and cloud, such that device users are allowed to offload heavy storage and computational cost to cloud to reduce the local resource and energy consumption. This is especially important in the era of big data.

II. OPPORTUNITIES OF MOBILE CLOUD

Mobile cloud is able to provide ‘‘real-time’’ personal and public data access for all Internet users at anytime, anywhere, on any mobile device. Mobile service providers can promote traditional new and more convenient offers to their clients in addition to traditional phone services like phone call, by leveraging the significant computing and storage ability of mobile cloud. Online learners can search anything that they are interested in from mobile cloud, and download unlimited. They can easily access resources from the course database, on-line universities’, and even public libraries. Mobile cloud services also provide benefit to clinics, hospitals and health care centers. It is a trend that Internet users prefer to launch finance-related activities on their smart phones. A blooming period for mobile finance is approaching. Due to being equipped with powerful computational resources, mobile cloud is strong enough to support various financial behaviors, such as money transfer, and bank payment. Mobile cloud game service is also another potential market. There are many new and popular game apps for different platforms like iOS, Android, Windows rising every year. Last of all, mobile cloud provides large-scale stream media store, large volume of social network data share, and location-based service for smart phone users. Considerable storage space, unlimited computational power, and convenient interface, these extremely appealing advantages of mobile cloud, that light up a bright prospective for diverse mobile services.

III. CHALLENGES IN MOBILE CLOUD

Taking advantage of advanced mobile and network technology, mobile users may enjoy various on-line activities, for example, Accessing social network information, watching on-line video (e.g. YouTube), checking email (e.g. Gmail), managing on-line banking (e.g. HSBC on-line bank), and on-line shopping (e.g. Amazon, eBay)[1]. This paper investigate security and privacy risk which are based on following user operations by standing at the viewpoint of applied cryptography: (1) (login) authentication between client and mobile cloud; (2) outsource data from local mobile device to remote cloud, and data integrity check; (3) search and share client’s remote data, and remote data computation.

When user authentication is considered, we usually think about the single way ‘‘client to cloud authentication mode’’, in which server will only allows valid clients to access to cloud system if the clients pass the corresponding ‘‘identity check’’. This type of ‘‘proof of identity’’ is extremely helpful in protecting cloud clients’ data privacy. They can mainly be categorized into three branches, namely knowledge-based, possession based and biometric-based authentications. Leveraging one of the approaches individually that may yield some potential security concern.

Knowledge-based authentication using user name and password is one of most user-convenience authentication Mechanisms. a single password authentication in which a mobile device/hardware must be fully trusted. Specifically, the hash value Hash(pwd) of a user’s password pw is regarded as a key to encrypt a randomly string K generated by the mobile user (i.e. CT = Encrypt(Hash(pwd), S)), and the encryption is further stored in the mobile device; meanwhile, the user’s identity ID and the string S are delivered to a cloud server. When trying to login the server, the user needs to send his ID to the server who returns a challenge ch. The user further taps password pw into the mobile, such that the mobile can recover K = Decrypt(Hash(pwd), CT) and next to compute a MAC(S, ch) for the server. With knowledge of S and ch, the server can check the validity of the MAC value.

Possession-based authentication enables mobile clients to make use of something they hold to fulfill identity authentication. Accordingly, we may choose to use secure USB token, one-time password [4], or embed a public key infrastructure (e.g. [4]) into mobile devices, to strengthen the security of authentication. But this approach requires more computational cost and energy Consumption,

The biometric-based authentication [6–8] can be used to provide a unique and portable way for client identification via making use of client’s bio-characteristics, such as voice, face, iris and fingerprint [9]. How to secretly store and process personal bio-information in authentication is a major privacy concern. Since one’s biometric information is unique, if adversary obtains the information by hacking into the client’s mobile device, it will bring severe harm to personal privacy.

To achieve stronger authentication security, multi-factor authentication systems (e.g. [10–13]) have been proposed in the mobile cloud setting. In a multi-factor authentication mechanism, more than one factor/technique-base are implemented into identity verification. A device and a cloud server will need to share some secret information as a preparation for future authentication, such as Hash(pwd) or random string S. The authentication phase will take 2–3 factors’ information (for example, password and secure token, fingerprint and password) into the ‘‘challenge- and- respond’’ interaction (Fig. 1). The multi-factor mechanism strengthens the difficulty of cracking the verification in the sense that malicious attackers have to compromise all factors to lead to a successful attack. Because of its high security guarantee, many companies have employed multiple factors for client’s authentication,

Table 1 Comparison among different types of authentication.

Category	Security	Client to cloud	Cloud to client	Factor Update	Authentication deligation
Password	Weak	Yes	No	No	No
Possesion	Weak	Yes	No	No	No
Biomentric	Weak	Yes	No	No	No
Multi-factor	Strong	Yes	No	No	No

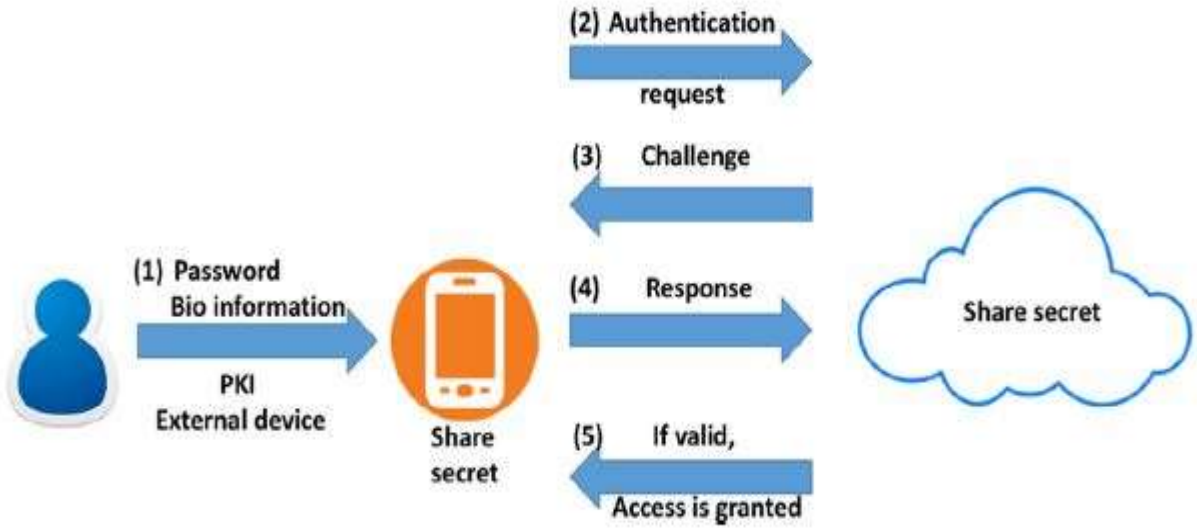

Figure 1. Unidirectional mobile to cloud authentication structure

IV. DATA SECRECY PROTECTION

The conventional cryptographic encryption is classify into two branches — symmetric encryption and asymmetric encryption. Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are the standard examples of the former, while public key based encryption, identity-based encryption , attribute-based encryption and functional encryption] are considered as the latter. The asymmetric encryption sometimes is generally referred to as public key encryption. To reduce local key storage cost, a mobile user may combine symmetric encryption with asymmetric one. Mobile encryption apps bring hope for lessening key management problem Nonetheless, both hybrid and apps modes leave computation, communication and trust problems to us.

The integrity check of outsourced and encrypted data is enviable while data owner loses the physical control of the data. However, this technique requires data owner to possess a ‘‘copy’’ of the data (or its digest) which is stored locally. This brings storage hindrance for mobile device users. Remote data auditing offers data integrity check with help of a trusted (third party) auditor even the data is outsourced to cloud. A remote data auditing system with data protection works as shown in Fig. 2. The data owner can upload encrypted block data to the cloud server, while valid data readers are allowed to download and decrypt the data for further use. A trusted third party, called auditor, takes charge of the data integrity check. The auditor is shared with some secret information by the data owner in advance. In the checking phase, the cloud server first sends the specified data to the auditor and next gives a proof to the auditor’s challenge. If the auditor accepts the proof, the data maintains its integrity.

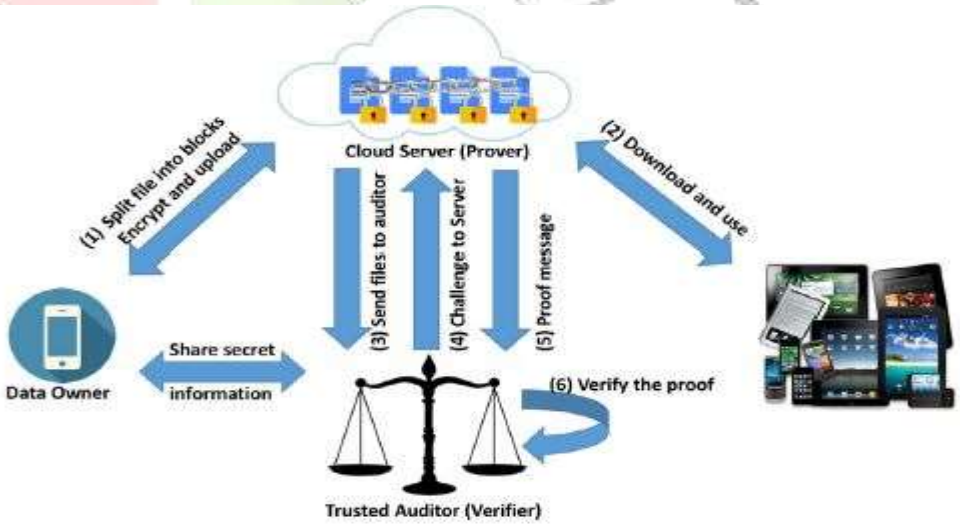

Figure2. Remote data auditing system with data protection

Mobile device users may need some secure means to search and retrieve their data stored in mobile cloud. Searchable encryption Mechanisms have been designed to guarantee data confidentiality and search privacy. Specifically, in a searchable encryption

scheme, a data owner is allowed to upload an encrypted database and an encrypted search index structure to a cloud server (in the 1st step), such that the server can locate the encrypted data by using so-called search token generated by the data owner (in the 2nd step), see Fig. 3. Searchable encryption mechanism is generally based on client–server mode. A data writer is allowed to encrypt and upload the data to cloud server, while a data reader is able to generate search trapdoor for the server, so that the server can search the related encrypted file(s). There are total four searchable encryption architectures, namely single writer/single reader, multi-writer/single reader, single writer/multi-reader, multi-writer/multi-reader. Symmetric searchable encryption (SSE) and public key based searchable encryption are two classic types of searchable encryption. SSE is usually everaged in practice as its efficiency is much better than that of public key based systems.

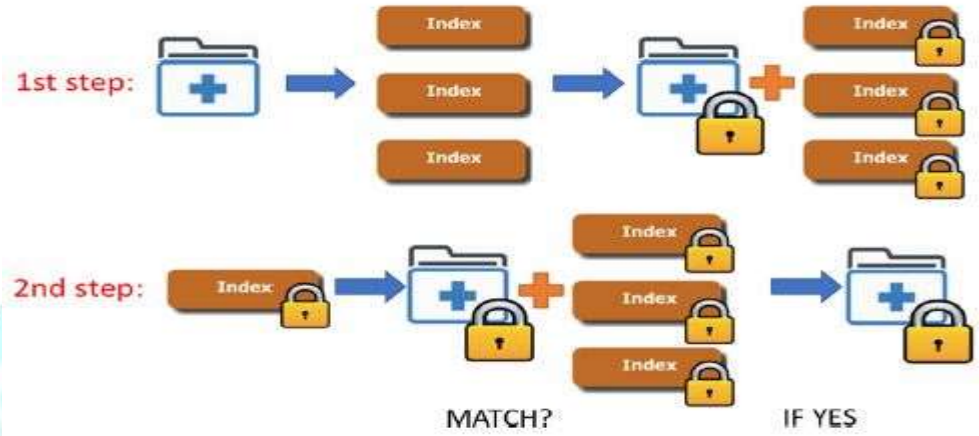

Figure3. Secure searchable encryption framework.

To securely share a file with others, a mobile device user may use traditional encryption like attribute-based encryption. But the traditional encryption requires the user to be always on-line, and to consume considerable computation resource to perform an encryption of sharing data, communication cost and battery to fulfill a simple data sharing. Proxy re-encryption (PRE) has been invented to tackle the above problem in an effective and efficient way in the sense that a user only generates a special key other than a cipher text, as the golden coin in figure 4 for cloud server, such that the server can convert the cipher texts of the user into those intended for others. In the figure, Alice is known as a delegator, while Bob is called a delegatee; the golden coin is referred to as a re-encryption key for the cipher text conversion. Mobile devices were limited to very restricted computational ability and storage space around a decade ago. It is undeniable that the recent advanced mobile software and hardware technologies give birth to a new generation of mobile devices with stronger computational power, larger storage room and longer battery life.

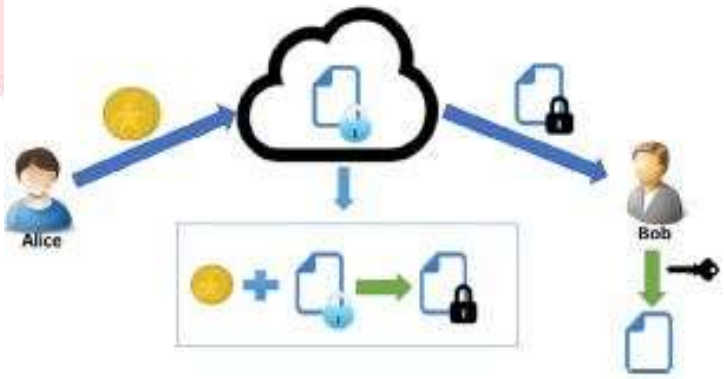

Figure 4. Secure encrypted cloud-based data share — proxy re-encryption

However, local data processing/computing and maintenance, in particular those related to large scale database, will definitely bring headache to mobile users. Thanks to the prevalence of cloud, mobile users are offered an option to outsourced their data to cloud, so that cloud can fulfill heavy computing tasks on behalf of the users. Without loss of data secrecy, many cloud users may choose to leverage encryption technique to ‘‘mask’’ their data before outsourcing. There is a few encryption technologies that can be used to

guarantee secure encrypted data computation. Below we focus on homomorphic encryption. We note that some other mechanisms, like secure two/multi-party computation, are also applicable to outsourced data computation applications. The reason we only mention homomorphic encryption is that the homomorphic technique is seen as the underpinning for ‘‘high-level’’ secure (computation) constructions.

V. CONCLUSION

Smartphone is vulnerable because of its natural disadvantage like low security protection and limited computation resource. As attackers may penetrate into different levels of cloud and mobile infrastructures to steal and temper data. This survey paper compared and analyzed some security and privacy risks on mobile cloud in the point of view of applied cryptography also investigated some challenges of mobile cloud.

REFERENCES

[1] Man Ho Au, Kaitai Liang, Joseph K. Liu, Rongxing Lu, Jianting Ning 2018. Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat. Future Generation Computer Systems 79 (2018) 337–349.

[2] I. Jeun, M. Kim, D. Won, Enhanced password-based user authentication using smart phone, in: GPC ’12, in: LNCS, Vol. 7296, Springer, 2012, pp. 350–360.

[3] T. Acar, M. Belenkiy, A. Küpçü, Single password authentication, Comput.Netw. 57 (13) (2013) 2597–2614.

[4] X. Yi, F. Hao, L. Chen, J.K. Liu, Practical threshold password-authenticated secret sharing protocol, in: ESORICS ’15, Part I, in: LNCS, Vol. 9326, Springer, 2015, pp. 347–365.

[5] A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, Cloud Authentication Based on Anonymous One-Time Password, in: Ubiquitous Information Technologies and Applications, in: LNCS, Vol. 214, 2013.

[6] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gen. Comp. Syst. 28 (3) (2012) 583–592.

[7] M. Karnan, M. Akila, N. Krishnaraj, Biometric personal authentication using keystroke dynamics: A review, Appl. Soft Comput. 11 (2) (2011) 1565–1573.

[8] T. Bhattasali, K. Saeed, N. Chaki, R. Chaki, A survey of security and privacy issues for biometrics based remote authentication in cloud, in: CISIM ’14, in: LNCS, Vol. 8838, Springer, 2014, pp. 112–121.

[9] Y. Yang, H. Lu, J.K. Liu, J. Weng, Y. Zhang, J. Zhou, Credential wrapping: From anonymous password authentication to anonymous biometric authentication, in: AsiaCCS ’16, ACM, 2016, pp. 141–151.

[10] K. Xi, T. Ahmad, F. Han, J. Hu, A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment, Secur. Commun. Netw. 4 (5) (2011) 487–499.

[11] D. Pointcheval, S. Zimmer, Multi-factor authenticated key exchange, in: ACNS ’08, in: LNCS, Vol. 5037, 2008, pp. 277–295.

[12] Y. Shah, V. Choyi, L. Subramanian, Multi-factor authentication as a service, in: IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015, pp. 144–150.

[13] J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, Two-factor data security protection mechanism for cloud storage system, IEEE Trans. Comput. 65 (6) (2016) 1992–2004.

[14] J.K. Liu, M.H. Au, X. Huang, R. Lu, J. Li, Fine-grained two-factor access control for web-based cloud computing services, IEEE Trans. Inf. Forensics Secur. 11 (3) (2016) 484–497.

[15] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, Z. Song, Authentication in the clouds: a framework and its application to mobile users, in: CCSW ’10, ACM, 2010, pp. 1–6.