JES
Journal of Engineering Sciences

Vol 11, Issue 1, Jan /2020
ISSN NO:0377-9254

TRUSTED DELEGATION CYBER PHYSICAL DATA SECURITY MOBILE HEALTHCARE

[1]NAGARAM NAGARJUNA, [2]RANGANA MAHESH,

[1,2]Assistant professor,

DEPT OF CSE

VIGNAN INSTITUTE OF TECHNOLOGY AND SCIENCE, HYDERABAD

Abstract—Attribute-based encryption (ABE) offers a promising solution for flexible access control over sensitive personal health records in a mobile healthcare system on top of a public cloud infrastructure. However, ABE cannot be simply applied to lightweight devices due to its substantial computation cost during decryption. This problem could be alleviated by delegating significant parts of the decryption operations to computationally powerful parties such as cloud servers, but the correctness of the delegated computation would be at stake. Thus, previous works enabled users to validate the partial decryption by employing a cryptographic commitment or message authentication code (MAC). This paper demonstrates that the previous commitment or MAC-based schemes cannot support verifiability in the presence of potentially malevolent cloud servers. We propose two concrete attacks on previous commitment or MAC-based schemes. We propose an effective countermeasure scheme for securing resource-limited mobile healthcare systems and provide a rigorous security proof in the standard model, demonstrating that the proposed scheme is secure against our attacks. The experimental analysis shows that the proposed scheme provides the similar performance compared with the previous commitment-based schemes and outperforms the MAC-based scheme.

Key words—Cyber-physical systems, mobile healthcare, cloud computing, attribute-based encryption

1. INTRODUCTION

In mobile healthcare systems, medical devices are equipped with cyber capabilities and located close to patients to collect clinical data and report diagnostic information. Such devices could be semiconductor-embedded smart intelligent sensors which are implanted inside the patient's body and work for real-time quantification of pathological symptoms. For diagnostic reports, personal health devices transfer private medical information to storage centers which manage these data in the form of electronic health record (EHR) . Currently, many cloud service providers offer medical information services such as IBM Cloud Solutions for Healthcare Google Cloud and Azure for health in practice. The cloud-based healthcare systems are beneficial since they can supply global connectivity to diverse healthcare devices and efficient resource maintenance in terms of storage saving.

However, delegating sensitive information to the potentially untrusted cloud servers raises concerns with respect to the patient's privacy. Thus, fine-grained access control to the patients' data is of utmost importance to preserve privacy of the clients' sensitive medical information. Attribute-based encryption (ABE) is a promising cryptographic tool to address this problem since it can provide pliable, fine-grained access control over data outsourced to the cloud.

Specifically, a data owner (a patient) generates an access policy, attaches to the encrypted message (a medical data), and transfers the ciphertext to the cloud server. As long as attributes assigned to a user (a medical practitioner) meet the policy enforced by the data owner, it is able to recover the message from the cipher- text1 . Despite its promising aspect, unfortunately, ABE asks for considerable decryption operations on users. Moreover, such a cost exhibits a steady increase in linear growth as the access policy

becomes bigger, i.e., more attributes and conditions are added to it. Green etal. gave a remedy to this issue by delegating to the cloud not only the ciphertext but also an ability to decrypt in partial on behalf of users. After the cloud partially decrypts and sends the result, a user decrypts the remaining part of the ciphertext of which computational cost is significantly smaller than to perform decryption from scratch. Thus, the great amount of computational burden on the user side can be offloaded to the cloud.

However, such a delegation of decryption raises a question about the correctness of the computation (even though it is partial) done by the cloud. In order to enable users to verify the partially decrypted ciphertext and attest to it, many studies adopted a commitment, a supplementary cryptographic tool that runs on top of ABE . In these schemes, a data owner generates a commitment value as well as a ciphertext which states that he commits to the encrypted message. Upon completing decryption, the user can use the commitment value to confirm that the partial decryption was done correctly. The commitment generation process, however, requires only public parameters, which implies that a malicious cloud is able to cheat users by forging a commitment for an arbitrary message and the original ciphertext. To achieve resilience to the malicious attempt, there was an endeavour to replace the commitment with unforgeable message authentication codes (MAC) to provide the verifiability of the computation result . Unfortunately, we ob served that it is still vulnerable to the tampering attacks: an adversary can bypass the verification even without forging MAC (The detailed attack scenario will be given in Section 3.).

Therefore, guaranteeing verifiable outsourced decryption of ciphertexts is an important step toward trustworthy delegation in a mobile healthcare system exploiting cloud computing. Motivated by the above rationale, we propose a generic tamper-resistant commitment scheme for mobile healthcare cyber-physical systems in cloud. In the proposed scheme, a trusted authority issues a public verification key and a secret commitment keys. Given a commitment key and a medical data to upload, a data owner generates a tamperresistant commitment value, encrypts the data, and uploads them to the cloud. After performing partial decryption, the cloud transfers the partially decrypted result to the user. He then performs final decryption, and uses the commitment value and the verification key to validate the correctness. Any malicious attempt to thwart the attestation results in the verification failure.

The contributions of this paper are: • We propose two attacks to reveal security breaches inherent in the existing verifiable outsourced decryption techniques. More precisely, we show that, in the commitment-based schemes the cloud can bypass the verification by tampering with both the ciphertext and the corresponding commitment value. In the recently proposed MAC-based scheme. We show that the cloud can bypass the verification by forging the ciphertext. • We propose a generic tamper-resistant commitment scheme for mobile healthcare cyber-physical systems in cloud, which can run on top of any ABE schemes with outsourced decryption capabilities. • We provide security and performance analyses to show that the proposed scheme provides tamperresistance for verifiable outsourced decryption, while rarely degrading efficiency compared with the existing schemes.

II. RELATED WORK AND SYSTEM DESCRIPTION

Since the introduction of outsourced decryption of ABE some follow-up works were proposed to enable users to check the correctness of the outsourced decryption Lai et al. solved this issue by employing a checksum mechanism.

However, their scheme is vulnerable to forgery attacks which enable an adversary to forge the checksum for any messages of his choice. Moreover, it requires encryption of both the messages and random values corresponding to checksums, which doubles the computational cost.

To overcome this problem, Lin et al. adopted a computationally lightweight commitment scheme to ABE. In the scheme, a sender commits to a message with a random coin and sends the result (i.e., commitment value) to a receiver. Provided the receiver recovers the message and the random coin correctly, he can verify whether the commitment value is valid. However, the sender generates a commitment value with only public parameters.

Thus, Lin et al.'s scheme still suffers from the same forging attacks as Lai et al.'s scheme. Xu et al. addressed this issue by adopting a MAC to each ciphertext. Since each MAC can be generated by only a sender who possesses a secret MAC key, an adversary can by no means forge the MAC without the key. However, we observed that an adversary can bypass the verification procedure regardless of the MAC mechanism (see Section 3). In addition to verifiability in outsourceable decryption, several variations were introduced, aiming at providing extra capabilities such as outsourcing key issuing key escrow exculpability out sourceable encryption enhanced security (CCA security) user revocation and keyword search In this paper, we focus on verifiable outsourced decryption schemes based on commitment and MAC, and their security vulnerabilities. Specifically, we review Lin et al.'s scheme and Xu et al.'s scheme as representative commitment and MAC-based schemes, respectively, to show that they are all vulnerable to our attacks. However, it is important to note that our attack scenarios are not limited to them.

III. SYSTEM AND THREAT MODEL

A cloud-based mobile healthcare system consists of data owner, cloud server, and user.

The role of each entity can be described as follows: 1) Data owner. This is an entity (e.g., patient) that generates medical data and has ownership of it. It encrypts the data and sends the ciphertext to the publicly accessible cloud server. It also generates a commitment value and uploads it with the ciphertext to the cloud server.

2) Cloud server. This is a cloud storage service provider globally connected to data owners and users. It manages ciphertext-commitment pairs sent by data owners. It partially decrypts ciphertexts in support of users. The cloud server is assumed to be curious about the outsourced medical data and may forge them or refuse to conform the dedicated operations of partial decryption because it requires less computational cost compared to honestly performing partial decryption. For example, if the cloud can bypass the verification of the MAC-based scheme the computational cost would be approximately half of the total operations needed for partial decryption.

3) User. This is an entity (e.g., medical practitioner or researchers) that wants to access data uploaded by data owners. Upon receiving the partial decryption result, it performs final decryption and checks if the cloud server honestly performed partial decryption.

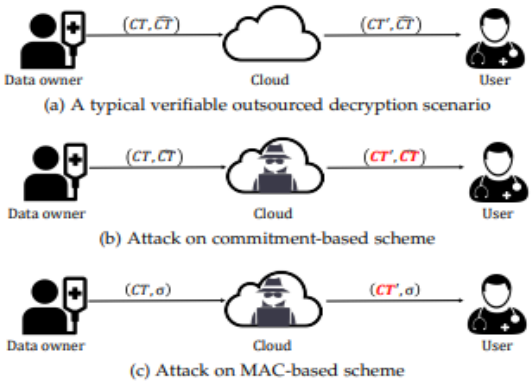

Fig. 1: Illustration of verifiable outsourced decryption and attacks

IV . PROPOSED ATTACKS

We envision an overview of the proposed attacks in Figure

. In the figures, forged components are marked in red. In Figure CT and CT0 represent a fully encrypted and partially decrypted ciphertext, respectively, and CTd is a commitment to the plaintext. Figure illustrates our attack on the commitment-based scheme, where the cloud sends the forged ciphertext-commitment pair to the user. Lastly, Figure illustrates our attack on the MAC-based scheme, in which the cloud sends the forged ciphertext and the original MAC to the user. In our attack scenarios, we assume there is neither any predefined message format nor predefined range of message values. The commitment-based schemes are vulnerable to our attack by tampering with the uploaded ciphertext and commitment together The MAC-based scheme tried to solve this problem by replacing the forgeable commitment with the unforgeable MAC but we found that the malicious cloud can bypass the verification without tampering with MAC. We describe each attack procedure in the following sections.

V. ALGORITHM DEFINITIONS

The proposed scheme consists of the following four algorithms:

1) $(VK, MK) \leftarrow Setup(\lambda)$ **by key server**. The setu algorithm takes as input security parameter λ ar outputs public verification key VK and master s cret key MK.
2) $CK \leftarrow KeyGen(VK, MK)$ **by key server**. Th commitment key generation algorithm takes as i put (VK, MK) and outputs secret commitment ke CK.
3) $\sigma \leftarrow Commit(VK, CK, M)$ **by data owne** The commitment generation algorithm takes VK, CK, and a message M, and outputs commi ment σ.
4) $y \leftarrow Vrfy(VK, M, \sigma)$ **by user**. The verificatic algorithm takes as input (VK, M, σ) and outpu $y \in \{0, 1\}$, where 0 and 1 indicate verificatic failure and success, respectively.

VI. CONCLUSION

In this paper, we proposed two tampering attack scenarios to reveal the security breaches inherent in the existing verifiable outsourced decryption schemes. According to our analysis, in the commitment-based schemes, the cloud can skip the partial decryption by tampering with both the ciphertext and the corresponding commitment value. Moreover, we showed that the cloud can bypass the verification in the MAC-based verifiable outsourced decryption scheme even though the MAC is unforgeable. We then proposed a generic tamper-resistant commitment scheme for mobile healthcare cyber-physical systems in cloud. The proposed scheme can run on top of any ABE schemes with outsourced decryption capabilities. We provided security and performance analyses to show that the proposed scheme provides tamperresistance while rarely degrading efficiency compared with the existing schemes.

REFERENCES

[1] Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., and Venkatasubramanian, K. K., "Challenges and research directions in medical cyber–physical systems," Proceedings of the IEEE, 100(1), pp. 75–90, 2012.

[2] Jovanov E., O'Donnell Lords A., Raskovic D., Cox P. G., Adhami R., and Andrasik F., "Stress monitoring using a distributed wireless intelligent sensor system," IEEE Engineering in Medicine and Biology Magazine, vol. 22, no. 3, pp. 49–55, 2003.

[3] https://www.ibm.com/cloud/healthcare.

[4]https://cloud.google.com/solutions/healthcare-life-sciences.

[5] https://azure.microsoft.com/en-us/industries/healthcare.

[6] Goyal, V., Pandey, O., Sahai, A., and Waters, B. "Attribute-based encryption for fine-grained access control of encrypted data", In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, 2006.

[7] Bethencourt, J., Sahai, A., and Waters, B. "Ciphertext-policy attribute-based encryption", In Security and Privacy, 2007. SP'07. IEEE Symposium on, pp. 321–334, IEEE.

[8] Ostrovsky, R., Sahai, A., and Waters, B. "Attribute-based encryption with non-monotonic access structures", In Proceedings of the 14th ACM conference on Computer and communications security, pp. 195– 203, ACM, 2007.

[9] Green, M., Hohenberger, S., and Waters, B. "Outsourcing the decryption of abe ciphertexts", In USENIX Security Symposium, Vol. 2011, No. 3, 2011.

[10] Lai, J., Deng, R. H., Guan, C., and Weng, J. "Attribute-based encryption with verifiable outsourced decryption", IEEE Transactions on Information Forensics and Security, 8(8), pp. 1343–1354, 2013.