A Cloud-aided RSA Signature Scheme for Sealing and Storing the Digital Evidences in Computer Forensics

Chu-Hsing Lin[1], Chen-Yu Lee[2] and Tang-Wei Wu[1]

[1]*Department of Computer Science, Tunghai University, 407 Taichung, Taiwan*
[2]*Department of Computer Science, National Chiao-Tung University*
1001 Ta-Hsueh Road, HsinChu, 30050, Taiwan
{chlin, g99350031}@thu.edu.tw, chenyu@cs.nctu.edu.tw

Abstract

The privacy of data or plain is an important issue in cloud computing. Therefore, to solve the problem, we establish the environment of cloud computing to process data with privacy and apply our scheme in the area of digital forensics for RSA signature algorithm. We experiment with efficiency of RSA signature in cloud computing. As a result, our scheme can reduce the loading of computing; besides, the clients don't need to waste storage spaces to save the results. The most important of all, we can take full advantage of the cloud computing for computing of large data and storage spaces.

Keywords: *Cloud computing, Digital forensics, RSA signature, Privacy*

1. Introduction

Recently, cloud computing have been a new fashion noun in Information Technology, and the data security have become a new issue in the cloud computing [1, 2, 3]. Most mobile devices, such as cell phone, can't process large size data; they depend on the cloud services with rich resources.

The storage of sealed digital evidences of crime forensics [4, 5, 6] would change from traditional photo, video types stored in a specific building to cloud services via Internet. The powerful computation and high speed communication cloud services will speed up the sealing process, logistical forensics engineering. However, it would be unsecure at the first part of the scenario, the digital evidences sent from the mobile devices at the first line to the cloud service. The evidence would be sent in plain text, without encryption to the cloud service through the Internet, but it would suffer from eavesdropping by any malicious people. If the evidences need to be sent under encryption, nevertheless the mobile devices would have insufficient computation power to perform the necessary actions.

In the paper, we improved a secure protocol model [7] to propose a novel scheme that achieves the requirements needed in the mentioned scenario to make sure the security of sealing and storing the digital evidences from first line people to the cloud services. The rest of the paper is summarized as follows. Section 2 enhances the protocol to be better in burden of computing and storage. Section 3, we will analyze the results of experiment between tradition and cloud structure. Finally, conclusions are given in Section 4.

2. The Proposed Structure in Forensics

In this section, we described the steps of uploading the digital evidences to the data center of forensics with privacy and downloading for verification. The cloud data center of forensics are divided into two services, cloud computing center and cloud storage center and shown in Figure 1. Suppose that the forensics officers want to store the digital evidences *DE* on the forensics data center in the cloud. The stored digital evidence should be encrypted by the aid of the cloud server as $C = DE^d \bmod n$, where $n = p * q$, and (p, q) are two distinct prime numbers [8][9][10].

In the cloud computing center, the cloud data center couldn't know what the forensics officers upload, and still finish the work forensics officers want to do. On the other hand, forensics officers permute the *DE* by using the low computing functions and send it to the computing center. After the encryption at the computation center, it is than sent to storage center to seal up for keeping. The detailed steps are described as follows.

Forensics officers' part:

Step1: Generate t random numbers $a_1, a_2, \ldots, a_t$ such that p and q are not divisors of a_i and compute $a_0 = (DE\prod_{i=1}^{r} a_i) \bmod n$, for some $r < t$.

Step2: Compute $b_i = a_i^2 \bmod n$, for $i = 0,1,2,\ldots,t$ and compose the results to a vector $B = G(DE, (a_0, a_1, ..., a_t)) = (b_0, b_1, \ldots, b_t)$. Last, forensics officers send the result B to the cloud computing center.

Cloud computing center:

Step3: On receiving *B*, the cloud computing center permute on *B* by using random permutation ψ. Let $B' = \psi(B) = (b_0', b_1', \ldots, b_t')$.

Step4: Compute a vector $V = F(B') = (v_0, v_1, \ldots, v_t)$, where $v_i = (b_i')^{(d-1)/2} \bmod n$. Finally, send the signature *V* to cloud storage center.

Cloud storage center:

Step5: On receiving *V*, the cloud storage center compute $U = \psi^{-1}(V) = (u_0, u_1, \ldots, u_t)$ where ψ^{-1} is the inverse permutation of ψ. Note that $U = F(B)$.

Step6: Compute $C = (u_0 a_0)\left((\prod_{i=1}^{r} u_i)(\prod_{i=1}^{r} a_i)\right)^{-1} \bmod n = DE^d \bmod n$. Finally, store the result *C* in this center.

Verifier:

Step7: Download the result *C* from cloud storage center, and verify the *C* by *e* associated public key to obtain the result is $DE = C^e \bmod n$.

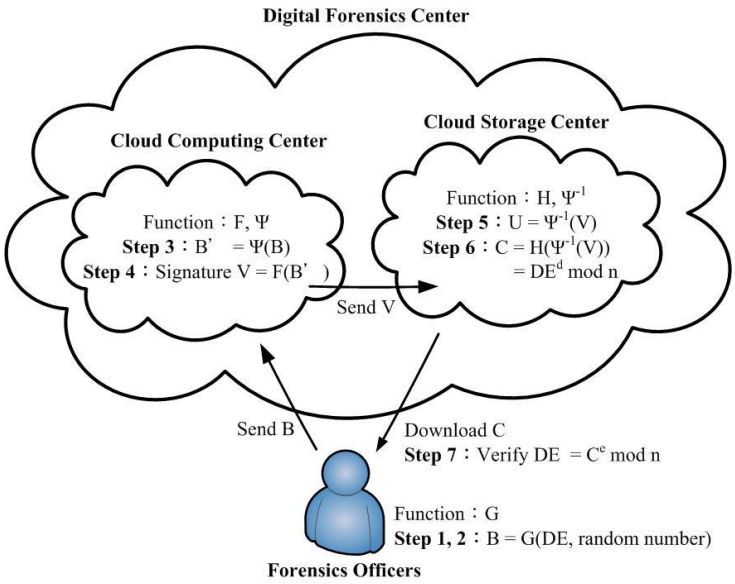

Figure 1. Steps of Cloud Structure

3. Experimental Results and Analysis

We would like to compare the efficiency of computation with the cloud structure and the traditional structure on the same experimental experiment. Among them, we set the argument of RSA key length 1024, 2048 and 4096, the number of random number is 40, and run 100 times to obtain the average time.

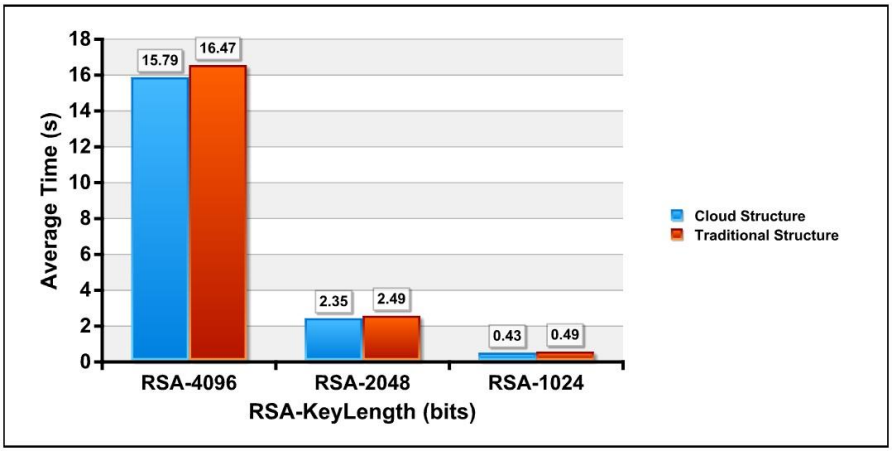

Fig. 2. Average Time with Different Key Length by Running 100 Times

As we can see in Figure 2, the results of the cloud structure represent a better efficiency than the traditional structure. The RSA-4096 in cloud structure is faster than the traditional structure about 0.68s, the RSA-2048 is about 0.14s, and RSA-1024 is about 0.06s. We find that if the key length is longer, and the execution time is lower. We can apply the cloud structure to some areas, such as digital forensics that we proposed in Section 2.

4. Conclusion

In this research, we propose a new digital forensics structure for RSA signature in cloud computing. This cloud structure can archive privacy, save computing power on mobile devices token by forensics officers. By RSA signature protocol, the verifier can verify the evidences in the court. Moreover, this protocol could be applied to many areas, such as digital forensics, online voting, or E-commercial, etc. We hope that we can accomplish online voting system in the future, and let it be used widely by people.

Acknowledgments

This work was supported in part by Taiwan National Science Council under grant: NSC 99-2221-E-029-039 -MY3.

References

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, pp. 1-11 **(2011)**.

[2] S. Ramgovind, M. M. Eloff and E. Smith, "The Management of Security in Cloud Computing", Information Security for South Africa (ISSA), pp. 1-7 **(2010)**.

[3] A. F. Mohammad and H. Mcheick, "Cloud Services Testing: An Understanding", Procedia Computer Science, Vol. 5, pp. 513-520 **(2011)**.

[4] S. J. Wang and D. Y. Kao, "Internet forensics on the basis of evidence gathering with Peep attacks", Computer Standards & Interfaces, Vol. 29, pp. 423-429 **(2007)**.

[5] Y. S. Yen, I. L. Lin and B. L. Wu, "A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence", Digital Investigation, Vol. 8, pp. 56-67 **(2011)**.

[6] F. Buchholz and E. Spafford, "On the role of file system metadata in digital forensics", Digital Investigation, Vol. 1, pp. 298-309 **(2004)**.

[7] C. H. Lin and C. C. Chang, "A Server-Aided Computation Protocol for RSA Enciphering Algorithm", Intern. J. Computer Math., Vol. 53, pp. 149-155 **(1993)**.

[8] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120-126 **(1978)**.

[9] S. Kawamura and A. Shimbo, "Performance Analysis of Server-Aided Secret Computation Protocols for the RSA Cryptosystem", The Transactions of The Institute of Electronics, Information and Communication Engineers IEICE, Vol. E73, No. 7, pp. 1073-1080 **(1990)**.

[10] F. Bao, C. C. Lee and M. S. Hwang, "Cryptanalysis and improvement on batch verifying multiple RSA digital signatures", Applied Mathematics and Computation, Vol. 172, pp. 1195-1200 **(2006)**.