International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Fast Secure and Anonymous Key Agreement Against Bad Randomness for CloudComputing

Sai Mounica M[1], Mohd Tajammul[2]

[1]*MCA, School of CS and IT, Jain University, Bangalore, INDIA*
[2]*Professor, School of CS and IT, Jain University, Bangalore, INDIA*

Abstract: On a cloud computer, services are usually available on the network service provider's network and are usually accessible remotely by cloud users through social media channels. An important agreement allows for the establishment of a secure channel in a public channel so that there is a secure connection between the cloud user and the cloud service provider. Important existing cloud computing agreements are plagued by other challenges, e.g., finding low connection delays, eliminating certificate management issues, improving user privacy and avoiding malicious computer programs. To address these challenges, we propose an anonymous 0-RTT protocol (verification and compact agreement) against malicious malicious software to establish a secure computer network. As a 0-RTT protocol, it greatly accelerates the efficiency of the secure channel establishment process. Additionally, our protocol does not require certificates in order to bind the public key to the business ID and solve the certificate management problem. Finally, a portable security protocol analysis is also proposed. The protocol satisfies not only common security features (e.g., known security key, anonymous key sharing), but also strong security guarantees, i.e., user privacy and resistance to malicious criminals. With cloud computing, users can remotely store their data in the cloud as well use the most sought after high quality applications.

Keywords: Cloud computing, secure channel, anonymous authentication, bad random resistance, zero return and return time.

Introduction:

Cloud computing has become one of the fastest growing technologies in the IT industry in recent years. It covers a large number of visual resources (e.g., computing power, storage, platforms, and services) and aims to maximize the efficiency of resources. Remote cloud users can access those services online using terminals, and access the required resources with a payment model as you need. Successful examples include Amazons S3 and EC2, Microsoft Azure, Google App Engine and Rackspace etc. This new computer model reduces startups and operating costs and increases user speed. Its benefits are enjoyed by many companies and individuals by switching to cloud computing IT solutions.

While enjoying the benefits of cloud computing, its unique architectural features also raise some insurmountable security challenges.

Cloud Computing has been seen as building the next generation of IT business, thanks to its long list of unprecedented benefits in IT history: self-help, an ubiquitous network.

Data extraction:

Users are relieved of the burden of storing and storing data when users place their (large-sized) data in the cloud, data integrity protection is a challenge to enable public testing of cloud data protection is essential Users can request external testing. a team to check the integrity of its submitted data. The goal is to improve data security on unreliable cloud storage servers that are often limited to services in the cloud server and client. Considering that large data sizes are stored on remote servers, access to the entire file can be the cost of sending input to the storage server. And transferring a file to a client network can consume heavy bandwidth. As the final capacity increases significantly beyond the growth of data access and network bandwidth, access and transfer of the entire archive even occasionally severely limit the robustness of network resources. In addition, the data verification output input disrupts the required server bandwidth used for normal storage and recovery purposes. The Third Party Auditor is the person responsible for handling remote data in a global manner. the goal is to improve data security by managing data on unreliable cloud storage servers with limited resources on the cloud server and client.

On a cloud computer, resources are usually available on a third-party network, that is, a cloud service provider (CSP) network, and are generally accessible remotely to cloud users through social channels. The processing is done remotely and the output is restored when the required processing is completed. Due to the nature of cloud computing and the openness of social media, an attacker can attack different types, such as impersonation, listening, cracking and abuse. Therefore, authentication and secrecy are confidential to be provided for communication between the cloud user and CSP, so that only authorized users can access resources and any attacker can violate the authenticity and confidentiality of altered messages. Besides, user privacy is also a major concern for cloud computing, which prevents the attacker from seeing that the two messages are coming from the same cloud user. Data in the cloud may contain sensitive information, for example, medical records, financial data. If user privacy is not considered, the attacker can listen to the connection in the cloud. Based on that, the attacker may obtain sensitive information, including who uses the cloud, how often, and the amount of data that changes and even the connection is encrypted. More importantly, if the attacker finds public individuals (e.g., business executives, celebrities) or other people who are sensitive to cloud culture, it may increase the likelihood that the attacker will damage the cloud. In fact, an attacker may launch a powerful attack (e.g., a phishing attack to steal sensitive information) in order to steal the personal information of cloud users (e.g., Cloud Hack Celebrity). Or the attacker may begin to reject the attack on the service to block the connection between the cloud used for diagnosis and the patient. Causing elimination in a crisis can have serious consequences and even lead to death. Therefore, user privacy is very important in cloud computing and should be protected.

Authentication Key agreement (AKA) is a widely used tool for achieving additional goals, allowing CSP and user to create a secure channel according to a shared session key. Besides, user privacy is also a major concern for cloud computing, which prevents the attacker from seeing that the two messages are coming from the same cloud user. Data in the cloud may contain sensitive information, for example, medical records, financial data. If user privacy is not considered, the attacker can listen to the connection in the cloud. Based on that, the attacker may obtain sensitive information, including who uses the cloud, how often, and the amount of data that changes and even the connection is encrypted. More importantly, if an attacker finds public individuals (e.g., business executives, celebrities) or other people who are sensitive to cloud culture, it may increase the likelihood that the attacker will damage the cloud. In fact, an attacker may launch a powerful attack (e.g., a phishing attack to steal sensitive information) in order to steal the personal information of cloud users (e.g., Cloud Hack Celebrity). Or the attacker may begin to reject the attack on the service to block the connection between the cloud used for diagnosis and the patient. Causing elimination in a crisis can have serious consequences and even lead to death. Therefore, user privacy is very important in cloud computing and should be protected.

Empty travel time (0-RTT) chat mode allows one business (e.g., cloud user) to send encrypted data using a time key and a session key message chat to a previously visited business. (e.g., CSP). The AKA protocol that supports 0-RTT will speed up the connection to the servers that users often visit. In particular, it is expected to bring low delays in situations that include high packet loss or high delays (e.g., cloud users with mobile devices). Most existing AKA agreements (including those that support 0-RTT) are built on a traditional PKI-based cryptosystem that has a certificate management problem. Unconfirmed public key cryptography (CL-PKC)) was introduced to eliminate the certificate management problem in the PKI cryptosystem system. However, a few certified AKAs that support 0-RTT are recommended for official safety analysis.

AKA agreements rely on random passwords that are used to prevent attackers from predicting session keys that result in and / or violate user privacy. In a cloud computing, cloud services typically use virtual technology, while guests (e.g., cloud users) use hypervisor-controlled resources [16]. If the hypervisor is malicious, it may predict random numbers [16] and endanger the safety of the AKA protocol. Moreover, as leaked by Snowden in SXSW 2014 [17], compared to a complete violation of the cryptographic system, it is easy to weaken the system by attacking the pseudorandom generator (PRG). In fact, a well-designed or poorly designed PRG can be used to produce such a random event. The most popular features of the Dual EC PRG were NIST, ANSI and ISO [18] and were used in other products, eg OpenSSL-FIPS v2, Microsoft's SChannel and the BSAFE RSA library [19]]. Therefore, secure contracts, e.g., TLS / SSL, made using Dual EC have a risk of violations [17]. For example, if the RSA BSAFE library (which uses Dual EC automatically) is selected, then all TLS connections made using this tool may be compromised.

Related Works:

The key agreement first introduced by Diffie and Hellman is widely used in cloudcomputing to secure transportation. In recent years, a number of important AKA agreements have been proposed.

However, most of them only support one or more RTT, where one or more connections (between organizations, e.g., cloud user and CSP) are required rather than 0-RTT. As shown, 0-RTT has much better performance than one or more RTT, e.g., to improve connection speed by 34% on average. In fact, some of the AKA agreements in support of the 0-RTT have already been signed among the most popular of the upcoming TLS.

1.3 and Google QUIC. Both can guarantee user privacy and may have a profound effect on the user experience of the cloud. The AKA agreements mentioned above are based on a standard PKI-based cryptosystem system, in which each entity must obtain a certified certificate in order to bind its ownership with its public key. Generally, the problem of certificate management is a burden.

Certified public key cryptography (CL-PKC) was introduced to alleviate the problem of certificate management. For CL-PKC, the public key to a business is its ownership associated with the public value it produces. As there is no certificate in use, overall certificate management is reduced. Similar to AKA agreements in a traditional PKI-based cryptosystem, most AKA agreements in CL-PKC do not support 0- RTT. The first unconfirmed 0-RTT AKA protocol was proposed. However, no official security analysis is provided on this protocol. The first flawlessly protected without the 0-RTT AKA protocol certificate was proposed. Later, a few 0-RTT certified agreements were also proposed. Unfortunately, user privacy is not considered in the above protocols. In the two protocols of the AKA computer cloud are proposed. However, neither of them supports 0-RTT and officially donates it security analysis. With the best authors' knowledge, no AKA secure protocol supports both 0-RTT and user privacy.

The security of AKA protocols is very much in line with the unpredictability of random numbers. In particular, there are three ways to deal with malicious planning, namely, a fixed, fenced or unsupported cryptosystem. The first avoids random use. However, it requires that the message sent be a little entropy. In fact, the entropy of the message in the real world is usually low. The second can be considered as the first extension. In this setting, random usage and system security are only guaranteed if the message and random together are enough minutes. entropy. However, the attacker may break the system, when selecting a PRG with a back door / badly built and the message will be sent without min-entropy high. The latter assumes that each user has a high quality seed and must make a nonce using PRG. Compared to the first two methods, it provides better guarantees as the attacker must completely break the PRG and interfere with the user's system to extract the seeds at once, then it can compromise the security of the system. So, in this paper, we do it with this line to avoid a bad the previous ones.

By using a homomorphism token with distributed data verification code, our system achieves the integration of storage integrity insurance and processing local data error, i.e., identifying invalid servers.

We also show how our main program is to support TPA cluster testing in submissions from multiple users.

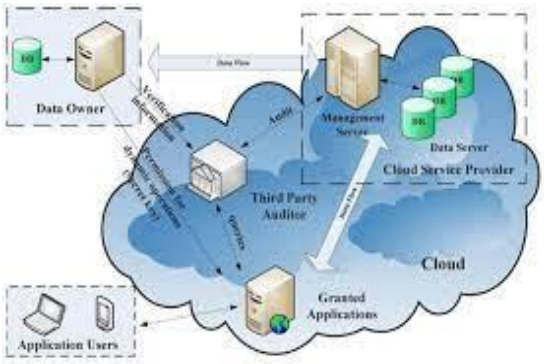
Homomorphic credentials are an unforgettable metadata generated by individual data blocks, which can be securely integrated in a way that assures the auditor that the line block of data blocks is computerized correctly by verifying only the integrated certificate. To look at it all in order to achieve confidentiality in public research, we propose a special integration of homomorphic confirmation with random mask methods. In our protocol, the linear combination of sample blocks in server response is randomly generated by a random artificial activity (PRF).

The proposed plan is as follows:

- Setup phase
- Audit phase

Analysis and Interpretation

We focus on cloud data storage security, which has been an important quality feature of service.



As users are no longer physically present have their data stored, traditional cryptographic primitives for the purpose of data protection cannot be direct accepted. Therefore, the way to successfully verify is the accuracy of the exported cloud data without the local copy of the data files becomes greater

in Cloud data storage challenge.

In terms of security, our protocol recognizes user privacy and random evil resistance. Even an attacker might listening to the communication in the cloud, can not distinguish whether the two messages are from the same cloud user. Therefore, most attacks can be avoided, especially attacks based on user personal information. In addition, even backdoored or poorly built PRG is used in the cloud the user to generate his random numbers, the attackers are still difficult weakening protocol security. Except for these two Security attributes, our protocol also achieves standard 0-RTT AKA security features that you must satisfy, which include known key protection, anonymous key sharing, non-compromised importer key lock and forwarder protection.

We recognize that our protocol may be used for others communication channels. However, compared to others communication, communication between the user of the cloud and CSP can be attacked by many types of attacks. Traditional communication channels in particular look for common security insufficient connections cloud computing.

In cloud computing, users may be more concerned about privacy disclosures and strict confidentiality, that is, resistance to bad random. In order to disclose privacy, such as mentioned above, most attacks can be avoided if AKA protocol satisfies the user's privacy. If random evil resistance is not considered, so the security of the AKA protocol is possible be weak. The last device for the cloud user is most likely attacks. Especially, today, is cloud compilation using a computer with IoT is a new trend. If random negative resistance is not considered, then communication is in-between IoT device and CSP can be easily attacked.

Take the cloud-based platform of age-old wearable health devices for example. it is possible that the attacker is easy to get close to the wearer health care device. An attacker may launch powerful ones attacks, e.g., side channel attacks or even physical attacks to corrupts the secret key stored on the device. We realize that corruption of the secret key may allow the attacker to make yourself a device. However, the attacker does not know listen to the connection between the device and CSP. Such imitation attacks are easy to spot, as the invader is unable to accurately read the patient's condition. However, when using a background or poorly designed on the device, the attacker may predict random the amount used. In this case, the attacker may read the session key and listen to the connection. Then there is the invader it may launch an advanced man on a moderate attack. the attacker may listen to the communication in general case. However, if there is an urgent message, e.g., cardiac arrest detected, the attacker may attack this message and send a general message to CSP. This can lead to death of the patient. Another example is webcams. If the attacker he can only find the secret web camera key, however you cannot see the web-monitored event. However, if a backdoored or poorly developed , the attacker may have full web camera control.

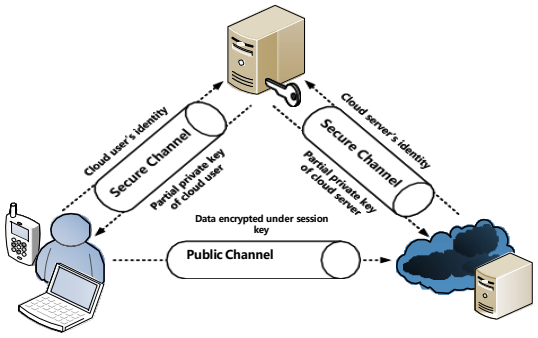


Fig. 1: System model

The trusted foreign company and is used to produce a long-term business secret key (cloud user or a CSP) by taking it as a business enterprise. Confidential a business key is generated using private component the key and the private key selected by itself. The public key of the business is simply its own ownership and the public value it produces itself. We recognize that, in order to obtain the private key of the component in business securely, a secure channel should be set up in advance between business and Server. To find a way to establish such secure channel.

This paper is focused on the establishment of a secure channel between the cloud user and CSP.

CSP offers a variety of services. It will provide the appropriate sponding service according to the application of the cloud user. Protecting cloud service security, secure channel (i.e., a secure time key) should be established between clouds user and CSP. We consider the issue of being a cloud user you have already visited CSP before. The cloud user then may send encrypted data using session key and session key message to CSP.

Batch Auditing

With the establishment of a privacy database that protects public research in Cloud Computing, TPA at the same time may handle multiple audits delegates to different user requests. an individual evaluation of these TPA functions can

it is boring and ineffective. Collection test it does not allow TPA alone to do much simultaneous audit activities, but also more reduces calculation costs on the TPA side.

Data Dynamics

Thus, to support data dynamics for maintaining the privacy of public risk audit is also very important. Now let's show our way The main scheme can be changed to build over existing data backup function, includes block level activities modification, removal and installation. We can apply this process to our construction for our benefit the secrecy of public risk assessment by data dynamics support.

Simply Archives

This problem is trying to find and verify a proof that the data held by the user in Remote cloud storage (called cloud archives or just archives) are not edited by archive and thus data integrity is verified. Cloud archive not cheating the owner, if cheating, in this case context, means that the archive can be delete some data or you can edit one of them data. While we are developing data evidence availability on unreliable cloud storage servers it is often limited by resources in the cloud server and client.

Verification Phase

Authentication before saving the file to archives, processes the file and adds more Meta data in file and archived. By time confirmation confirmation uses this Meta data to ensure data integrity. Icon it is important to note that our evidence of data integrity. The protocol simply checks the integrity of the data i.e. if data has been changed or illegally deleted. It does not prevent the archive from being modified data.

Conclusion

Given the popularity of cloud archive storage, it is desirable to enable clients to ensure the integrity of their data in the cloud. We design and implement an effective data integrity protection (DIP) system for small active memory recovery codes (FMSR) under multiple server settings. Our DIP system maintains errortolerance and repairs FMSR savingsstructures.
To understand the effectiveness of the FMSR and DIP integration, we evaluate its security capabilities, evaluate its effective time using testbed tests, and perform cost- effectiveness analysis.

References

- L. Zhang, X. Meng, K. Choo, Y. Zhang, and F. Dai, "Privacy preserving cloud establishment and data dissemination scheme for vehicular cloud," IEEE Transactions on Dependable and Secure Computing, 2018, doi:10.1109/TDSC.2018.2797190.
- M. Jouini and L. Rabai, "A security framework for secure cloud computing environments," in Cloud Security: Concepts, Methodologies, Tools, and Applications, 2019, pp. 249–263.
- J. Li, L. Zhang, J. Liu, H. Qian, and Z. Dong, "Privacy-preserving publicauditing protocol for low-performance end devices in cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572– 2583, 2016.
- M. ARMBRUST, A. FOX, R. GRIFFITH, A. D. JOSEPH, R. KATZ,
  A. KONWINSKI, G. LEE, D. PATTERSON, A. RABKIN, I. STOICA, AND M. ZAHARIA. A VIEW OF CLOUD COMPUTING. COMMUNICATIONS OF THE ACM, 53(4):50–58, 2010
- H. Krawczyk and H. Wee, "The OPTLS protocol and TLS 1.3," in 2016 IEEE European Symposium on Security and Privacy, 2016, pp. 81–96.
- B. Hale, T. Jager, S. Lauer, and J. Schwenk, "Simple security definitions for and constructions of 0-rtt key exchange," in 15th International Conference on Applied Cryptography and Network Security, 2017, pp. 20– 38.
- L. Zhang, "Key management scheme for secure channel establishment in fog computing," IEEE Transactions .