JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Develop a Secure and Trust-based Key Management Protocol for Cloud Environments

M. Venu Gopal, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana

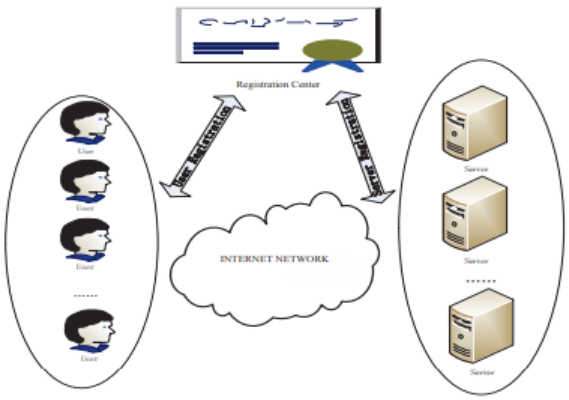
Dr.CH Sri Hari., Professor, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana
A. Manikanta, Assistant Professor, Dept of CSE, Siddhartha Institute of Technology and Sciences, Telangana

Abstract - With the maturity of cloud computing technology in terms of reliability and efficiency, a large number of services have migrated to the cloud platform. To convenient access to the services and protect the privacy of communication in the public network, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures gain wide attention. However, most of the existing three-factor MAKA protocols don't provide a formal security proof resulting in various attacks on the related protocols, or they have high computation and communication costs. And most of the three-factor MAKA protocols haven't a dynamic revocation mechanism, which leads to malicious users cannot be promptly revoked. To address these drawbacks, we propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management using Schnorr signatures and provides a formal security proof in the random oracle. Security analysis shows that our protocol can meet various demands in the multi-server environments. Performance analysis demonstrates that the proposed scheme is well suited for computing resource constrained smart devices. The full version of the simulation implementation proves the feasibility of the protocol.

1. INTRODUCTION

In the recent decade, cloud computing technology has been completely commercialized. It can not only improve service efficiency but also reduce costs. More and more companies are putting their services on the cloud platform for development, management and maintenance. This not only reduces the local maintenance burden for these enterprises, but also provides unified security and operation management for all services on the third-party cloud platform, as shown in Fig.1. Although third-party cloud platforms have more powerful technologies and more standard technical specifications to ensure that the servers run in a relatively secure environment, users and servers communicate in the public network. Therefore, authentication and key agreement are critical for the communication security. The use of mutual authentication and key agreement (MAKA) protocols not only prevent attackers from abusing server resources, but also prevent

malicious attackers posing as the server to obtain the user's information. Therefore, the MAKA protocols have been extensively studied since Lamport proposed a password-based authentication protocol. Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud servers rendering different services has also grown significantly. For the single-server architecture, it is difficult for users to maintain a variety of passwords for each server. To improve user experience, many scholars propose more flexible MAKA protocols for multi-server environments. Combined with the unified management features of the cloud platform, such protocols can be conveniently applied. The protocols for multi-server architectures model as shown in Fig.2, users and cloud servers only need to register in the registration center (RC) to mutual authentication and key agreement.



In the multi-server environments, the MAKA protocols can be further divided into two categories, two-factor MAKA protocols, namely identity, password, and three-factor MAKA protocols, namely identity, password, biometrics. The works in have shown that the password-based MAKA protocols suffer from several attacks such as guessing password attack. The cost of the password guessing attack on password-based protocol becomes lower and lower as the rapid development of computers. On the other hand, users usually utilize simple letters or numbers as their passwords, and even a large number of users directly use the default password if the smart devices don't require the user to modify the password mandatory. In order to solve this problem, several biometrics-based MAKA protocols have been proposed. Due to the uniqueness, availability and non transferability of biometrics keys (palm print, iris, finger print etc.), the three-factor MAKA protocols for multi-server environments provide more security than the two-factor protocols. In view of the openness of wireless networks, an adversary can intercept, modify, delete and replay any communication messages. Anonymity and un-traceability are also indispensable part of the MAKA protocols to resist the above-mentioned attacks. However, the current three-factor MAKA protocols still have the following defects

2. LITERATURE SURVEY

In 2001, Li et al. [5] introduced the concept of authentication protocol for multi-server environments and proposed the first password-based MAKA protocol using the neural network. Thanks to the complicated neural network, Li et al.'s protocol isn't suitable for smart devices with limited computing power. To improve efficiency, Juang [6] proposed a MAKA protocol for multi-server architectures by using hash functions and symmetric key cryptosystems. In the same year, Chang et al. [7] pointed out that Juang's protocol is flawed in terms of efficiency. They proposed a more efficient MAKA scheme for multi-server environments. However, in their protocol RC shares system private key with all servers. This will undoubtedly result in many security vulnerabilities. To improve security, some new MAKA protocols [8], [9] using hash functions and symmetric-key cryptosystems had also been proposed. In 2013, Liao et al. [10] proposed a multi-server remote user authentication protocol using self-certified public keys for mobile clients.

3. SYSTEM ANALYSIS:

3.1 Existing System

Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud servers rendering different services has also grown significantly. For the single-server architecture, it is difficult for users to maintain a variety of passwords for each server. To improve user experience, many scholars propose more flexible MAKA protocols for multi-server environments. Combined with the unified management features of the cloud platform, such protocols can be conveniently applied. users and cloud servers only need to register in the registration center (RC) to mutual authentication and key agreement

Disadvantages

In the multi-server environments, the MAKA protocols can be further divided into two categories, two-factor MAKA protocols, namely identity, password, and three-factor MAKA protocols, namely identity, password, biometrics. The works in [11], [12] have shown that the password- based MAKA protocols suffer from several attacks such as guessing password attack

3.2 Proposed System

We propose a dynamic revocable three-factor mutual authentication and key agreement (3DRMAKA) protocol which has more comprehensive functions, reliable security and relatively higher execution efficiency. Our contribution can be summarized as follows:

- We design a three-factor MAKA protocol which implements three-factor security. And we show that the proposed protocol can meet the demands of multi-server architectures such as anonymity, nontraceability, resistance password guessing attack and smart card extraction attack, and so on.
- Our scheme achieves the user's dynamic management. In our protocol, users can be dynamically revoked to promptly prevent attacks from malicious users. Without a dynamic revocation mechanism, RC can't punish malicious users in a timely manner. This may result in such malicious users still active in the network to communicate with other servers.
- In the random oracle, we provide a formal proof of the proposed protocol based on BDH, CDH and Schnorr signatures unforgeability assumptions. We show that the proposed protocol is mutual authentication secure and authenticated key agreement secure. 4) Our protocol has a good execution efficiency. Especially on the client side, the computation cost of our scheme is the lowest in the related existing protocols. This shows that our protocol is more suitable for device mobiles with limited computing resource. And, to prove that the protocol is technically sound, we programmatically simulate the proposed protocol.

Advantages

Proposed a biometrics based MAKA protocol for multi-server environments. Unfortunately, after our analysis in the security comparisons and cryptanalysis subsection of this paper, their protocol is vulnerable the server impersonation attack and the man-in the-middle attack. On the other hand, the MAKA protocol is also widely used in other environments, such as Passive Internet of Things.

MODULES:

DATA OWNER:

In this module, initially the data owner has to get register to the cloud server (CS1,CS2,CS3,CS4) . Data owner will login to the corresponding cloud server he got registered. Data owner encrypt will upload file to the cloud server (CS1, CS2, CS3,

CS4) Data owner verifies the file he uploaded either it is safe or not. Data owner can view, how many file has been uploaded to the corresponding cloud servers(CS1,CS2,CS3,CS4) Data owner will send file to trust manager to store the data owner file t5o the corresponding cloud servers (CS1,CS2,CS3,CS4)

CLOUD SERVER

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud consumer. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

TRUST MANAGER

Trust manager provides login authorization for both data owner and the end user.

Trust manager can view all the cloud status .Trust manager can view the feed backs given by end user and lists all positive and negative feed backs. Trust manager lists no of users in cloud services(IAAS,PAAS,SAAS).Trust manager can view the attackers in cloud servers(CS1,CS2,CS3,CS4) and the no of time attacked.

CLOUD CONSUMER

Cloud consumer first has to register to the cloud server (CS1, CS2, CS3, CS4) which particular cloud he has to use. Cloud consumer has to login to the cloud he got registered. Cloud consumer feedback about the data (positive or negative feedback)

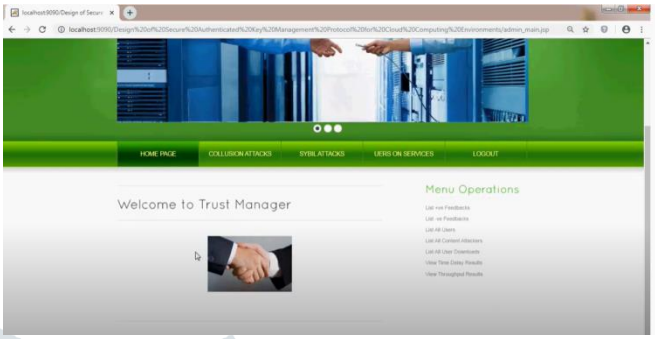
ATTACKER

Attacker will view registered users and cloud files

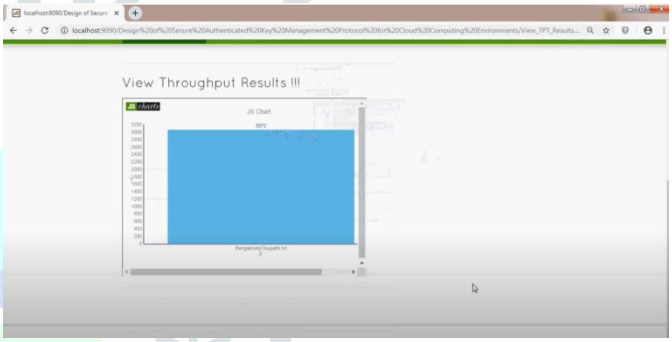
1 Collusion Attacks - to mislead feedbacks about the cloud

2 Sybil Attacks - When user uses more transaction per day (Exceeds the limit which is assigned by the Trust Manager)

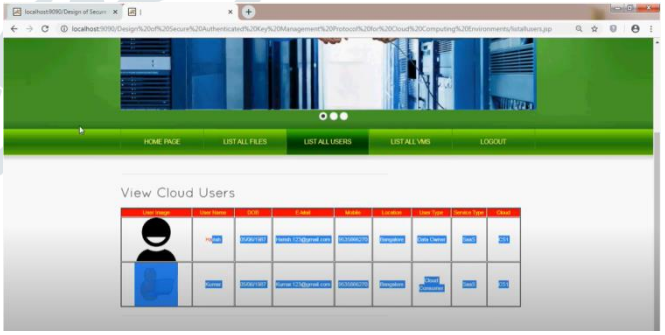
4. OUTPUT RESULTS:



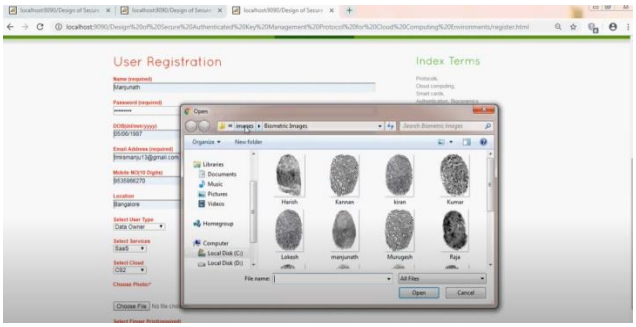
4.1 View Throughout results Page



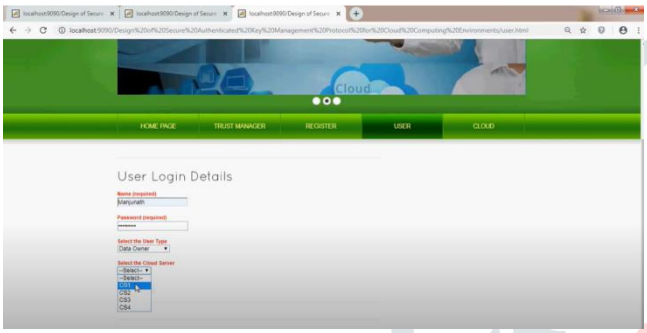
4.2 View Cloud Users Page



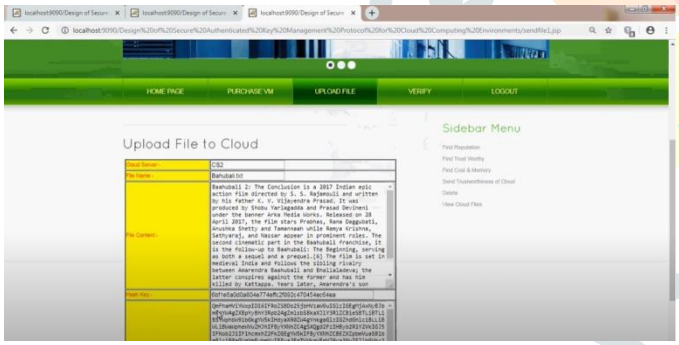
4.3 User Registration Page



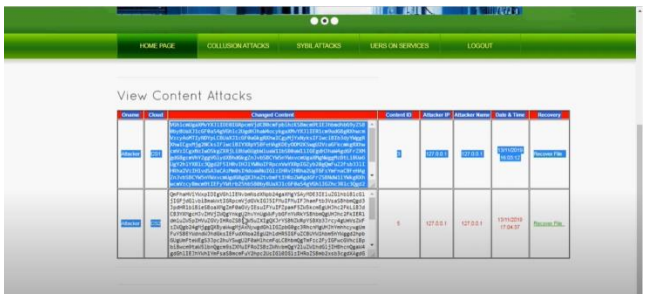
4.4 User Login Details Page



4.5 Upload File to Cloud Page



4.6 View Contents Attacks Page



4.7 Verify File in Cloud Page

5. CONCLUSION

To resist the exhaustion of password attack on the two-factor MAKA protocols, a large number of three-factor MAKA protocols have been proposed. However, almost all three factor MAKA protocols don't provide formal proofs and dynamic user management mechanism. In order to achieve more flexible user management and higher security, this paper proposes a new three-factor MAKA protocol that supports dynamic revocation and provides formal proof. The security shows that our protocol achieves the security properties of requirements from multi-server environments. On the other hand, through the comprehensive analysis of performance, our protocol doesn't sacrifice efficiency while improving the function. On the contrary, the proposed protocol has great advantages in terms of the total computation time.

REFERENCES

[1] J. Ronson, So You've Been Publicly Shamed. Picador, 2015.

[2] E. Spertus, "Smokey: Automatic recognition of hostile messages," in AAAI/IAAI, 1997, pp. 1058–1065.

[3] S. Sood, J. Antin, and E. Churchill, "Profanity use in online communities,"in Proceedings of the SIGCHI Conference on Human Factors inComputing Systems. ACM, 2012, pp. 1481–1490.

[4] S. Rojas-Galeano, "On obstructing obscenity obfuscation," ACM Transactionson the Web (TWEB), vol. 11, no. 2, p. 12, 2017.

[5] E. Wulczyn, N. Thain, and L. Dixon, "Ex machina: Personal attacksseen at scale," in Proceedings of the 26th International Conference onWorld Wide Web. International World Wide Web Conferences SteeringCommittee, 2017, pp. 1391–1399.

[6] A. Schmidt and M. Wiegand, "A survey on hate speech detection usingnatural language processing," in Proceedings of the Fifth International

Workshop on Natural Language Processing for Social Media. Association for Computational Linguistics, Valencia, Spain, 2017, pp. 1–10.

[7] Hate-Speech, "Oxford dictionaries," retrieved August 30, 2017 from https://en.oxforddictionaries.com/definition/hate speech.

[8] W. Warner and J. Hirschberg, "Detecting hate speech on the world wide web," in Proceedings of the Second Workshop on Language in Social Media. Association for Computational Linguistics, 2012, pp. 19–26.

[9] I. Kwok and Y. Wang, "Locate the hate: Detecting tweets against blacks." in AAAI, 2013.

[10] P. Burnap and M. L. Williams, "Cyber hate speech on twitter: An application of machine classification and statistical modeling for policy and decision making," Policy & Internet, vol. 7, no. 2, pp. 223–242, 2015.