**Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments**

**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 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.

**EXISTING SYSTEM:**

* Lee et al. proposed a authentication protocol using smart card.
* Lin et al. and Chang et al. found that Lee et al.’s protocol suffers from the masquerade attack and the conspiring attack, respectively.
* To enhance security, Kim et al. proposed a new biometrics-based authentication protocol using smart card.
* Unfortunately, Scott pointed out that Kim et al.’s protocol can be completely compromised by a passive adversary.
* Later, Khan et al. found that Lin et al.’s scheme also suffers from the server spoofing attack and proposed an improved version. For multi-server architectures,
* Yoon et al. proposed a biometrics-based authentication protocol using elliptical curve cryptosystem (ECC) and smart card.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Authentication and key agreement are critical for the communication security.
* The existing system has high computation and communication costs.
* The password based MAKA protocols suffer from several attacks such as guessing password attack.
* Most of the existing MAKA protocols based on the three factors haven’t a formal proof, but some informal security analysis. And some protocols were embed insecure factors such as key authentication factors easily extracted.
* Some important basic functions, such as dynamic user management, authentication phase without RC, are not considered in most MAKA protocols.
* Some three-factor MAKA protocols didn’t take full account of their actual application environment, which results these protocols are not suited for the limited resource of the devices.

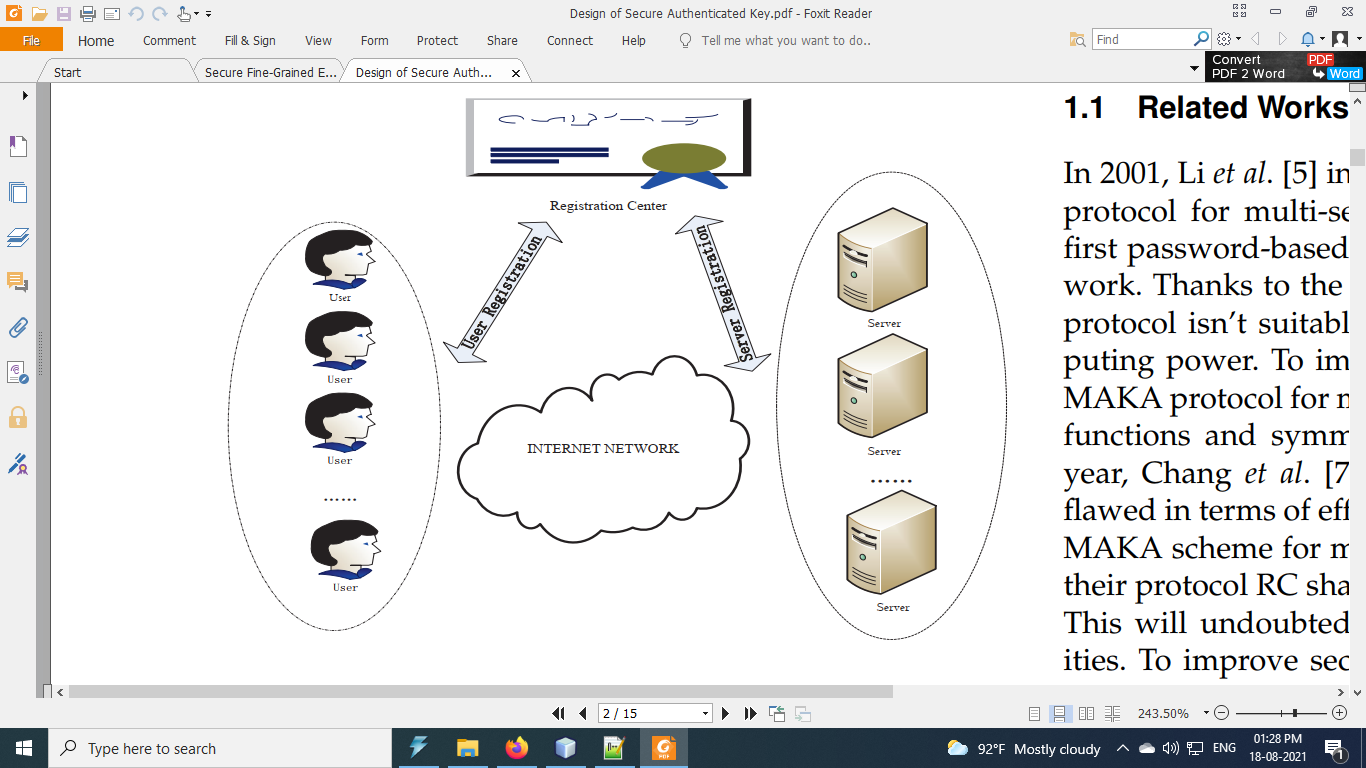
**PROPOSED SYSTEM:**

* 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, non-traceability, 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 our proposed system protocol, the three factors in the authentication process are indispensable. There is no way for the adversary to bypass any factor to complete the login or authentication process. Because only biological information can be used to compute and there is no way to complete the QR Code login without the correct details. Even if the adversary bypasses the QR through complex physical attacks, he/she can’t compute anonymous message delivery and authentication because he/she doesn’t have the permission. Thus, the proposed scheme can achieve three-token security.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The proposed system not only prevents attackers from abusing server resources, but also prevent malicious attackers posing as the server to obtain the user’s information.
* In this project, 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 protocol has 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.

**SYSTEM ARCHITECTURE:**

****

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium i3 Processor
* Hard Disk : 500 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 4 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 10.
* Coding Language : JAVA.
* Tool : Netbeans 8.2
* Database : MYSQL

**REFERENCE:**

Wei Li , Xuelian Li , Juntao Gao , and Haiyu Wang, “Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 18, NO. 3, MAY/JUNE 2021.