Securing Cloud Authentication

Design and analysis of a distributed authentication protocol for cloud services

CHALLENGES: Secure societies – Protecting freedom and security of Europe and its citizens

PRODUCTIVE SECTOR: IT sector, Cloud Service Providers, Healthcare system

PROBLEM DESCRIPTION

Cloud computing is a promising technology in the healthcare industry. However handling sensitive health data is challenging. One of the most important issues is the secure entity authentication. If it is breached, confidentiality and integrity of the data or services may be compromised. A secure mutual entity authentication protocol for a cloud environment is required.

CHALLENGES AND GOALS

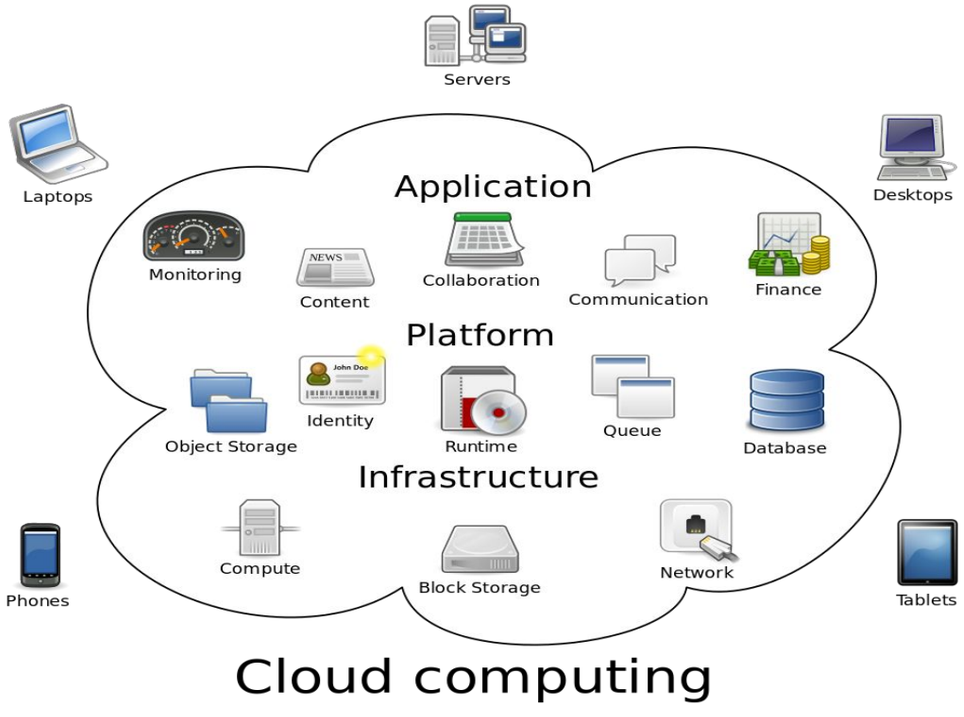
Prevalent single-server solutions might result in single point of failure and vulnerable against offline dictionary attacks. Multiple-server schemes are most of the cases not scalable.

Goal is to design a distribute authentication scheme, where the attackers have to attack multiple servers simultaneously, which increases the attack cost. Also to minimize computational costs by applying fast cryptographic operations and providing robustness and scalability.

MATHEMATICAL AND COMPUTATIONAL METHODS

Design of an advanced key exchange cryptographic protocol according to well-established principles. The protocol is analyzed according to the extended Bellare-Rogaway model. A complexity theoretic reduction is given which turns an adversary against the protocol into an adversary against a cryptographic primitive.

Java implementation is created and tested on Microsoft Azure environment.

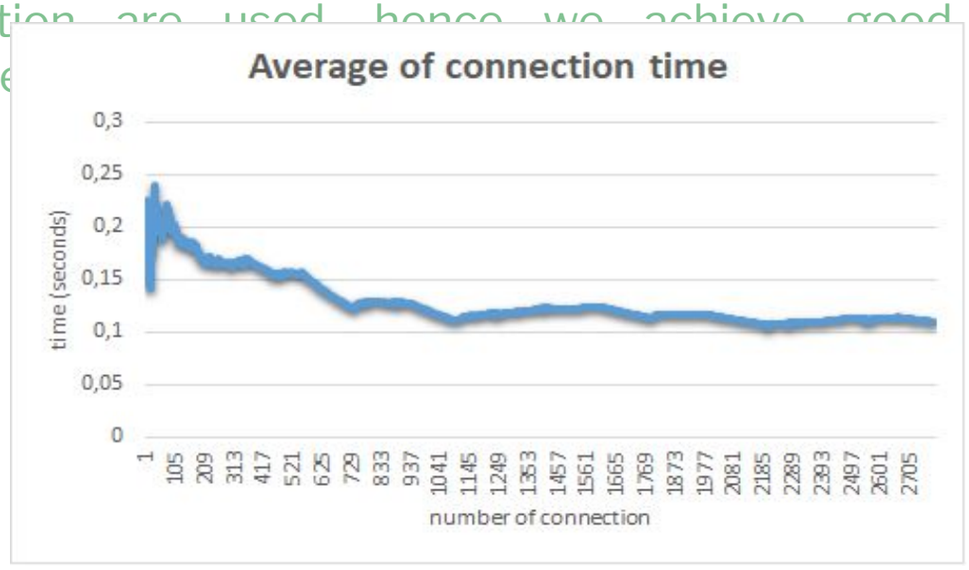


Securing Cloud Authentication

Design and analysis of a distributed authentication protocol for cloud services

Results and Benefits

A mutual entity authentication protocol with key agreement is given where identity verification is carried out by multiple servers applying secret sharing technology on server side. The protocol is provably secure in the threshold hybrid corruption model. We also achieve robustness and scalability as well. We prove that the protocol is secure in the random oracle model, if Message Authentication Code (MAC) is universally unforgeable under an adaptive chosen-message attack, the symmetric encryption scheme is indistinguishable under chosen plaintext attack, moreover Elliptic Curve Computational Diffie-Hellman assumption holds in the elliptic curve group. Due to the fast ECDH key exchange, MAC, xor operations and symmetric encryption are used, hence we achieve good results in computational time.



Efficiency analysis of implementation

The company has a multi-server mutual entity authentication system for clouds. Even if one or more servers are compromised or break down, the service provider will be able to service and authenticate the users securely.

DECRYPT UNIVERSITY OF DEBRECEN

HU-MATHS-IN Hungarian Service Network for Mathematics in Industry and Innovations

UNIVERSITY of DEBRECEN

SZÉCHENYI 2020 BEFEKTETÉS A JÖVŐBE

CCLAB

CCLAB