International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 7th Mar 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: **A LIGHT WEIGHT AUTHENTICATION SCHEME FOR SECURE DATA SHARING IN CLOUD ENVIRONMENT**

Volume 08, Issue 03, Pages: 89–92.

Paper Authors

MR.Y.SRINIVASA RAO, T.NAGA MALLESWARAO
Vignan's Lara Institute of Technology & Science

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A LIGHT WEIGHT AUTHENTICATION SCHEME FOR SECURE DATA SHARING IN CLOUD ENVIRONMENT

MR.Y.SRINIVASA RAO[1], T.NAGA MALLESWARAO[2]
Assistant Professor[1], Department of M.C.A, Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A, Vignan's Lara Institute of Technology & Science

Abstract:
Secure and efficient file storage and sharing via authenticated physical devices remain challenging to achieve in a cyber-physical cloud environment, particularly due to the diversity of devices used to access the services and data. Thus in this paper, we present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients. The proposed protocol is demonstrated to resist chosen-ciphertext attack (CCA) under the hardness assumption of decisional-Strong Diffie-Hellman (SDH) problem. We also evaluate the performance of the proposed protocol with existing data sharing protocols in terms of computational overhead, communication overhead, and response time.

Introduction:

Loud-assisted cyber-physical systems (Cloud-CPSs; also known as cyber-physical cloud systems) have broad applications, ranging from healthcare to smart electricity grid to smart cities to battlefields to military, and so on [1], [2]. In such systems, client devices (e.g., Android and iOS devices, or resource constrained devices such as sensors) can be used to access the relevant services (e.g., in the context of a smart electricity grid, it may include utility usage data analyzed and stored in the cloud) from/via the cloud. However, client devices generally have less computing capabilities and hence,are unlikely to have adequate security (technical) measures in comparison to the conventional personal computers (PCs)
[3]. One such architecture is illustrated in Figure 1, where the mobile device is used to denote a client device. The mobile device connects to the mobile network via base stations such as the base transceiver station, access point, or satellite.When a mobile user requests for some tasks to be processed,information (e.g., identity and location) is handover to the central processors connected to the servers for processing.Based on the home agent (HA) and mobile subscriber data stored in the relevant databases, mobile network operators can decide whether to provide or decline requests to access particular services (i.e. Authentication, Authorization, and Accounting – AAA). After the mobile subscriber has been authenticated, the mobile user's request(s) will be forwarded to the cloud controllers (CC). The latter processes the requests and provides the relevant services.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Disadvantages:

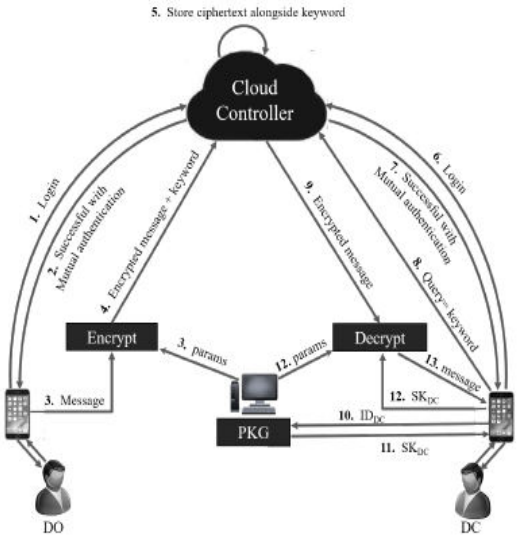
Despite the popularity of cloud computing and its variants(e.g., mobile cloud and cyber-physical cloud systems), security issues (privacy and reliability) in untrusted cloud environment and physical devices remain major concerns. Identity-based encryption (IBE) scheme is a potential cryptographic solutions that can be used to facilitate secure data sharing. Thus, in this paper, we construct an identity-based authentic data sharing (IBADS) protocol to provide data security in a cyber-physical cloud environments. For the rest of the paper, mobile devicesare considered as the client devices as such devices generally have more computational and storage capabilities compared to other Internet-of-Things (IoT) devices

Proposed system:

The proposed protocol is designed to achieve authentication between a physical device and the cloud controller, and provide a secure end-to-end secure communication in the cloud using IBE scheme. Specifically,1) Our proposed protocol provides mutual authentication,and essential features such as client registration, login,mutual authentication, password renewal. The protocol also ensures user anonymity. We also demonstrate its resilience against known security attacks (e.g., insider attack, impersonation attack, session key computation attack), and its correctness using AVISPA simulation tool.

2) Once the physical devices are authenticated, the next phase is secure end-to-end communication. For this,the proposed encryption technique is used on bilinear pairing with a small public parameter-size. We then demonstrate that it is IND-ID-CCA secure based on the decisional-SDH (Strong Diffie-Hellman) assumption.

Architecture:



Advantage:

As confidential data is transmitted to and from client mobile devices via insecure communications, it is required to ensure that the system fulfills several fundamental security properties,such as confidentiality, authenticity, integrity and availability.In indistinguish ability, an adversary is unable to distinguish between ciphertext pairs based on the chosen-message they have encrypted. Indistinguish ability under chosen-plain text attack (IND-ID-CPA) is a basic requirement for Identity-based Encryption (IBE) scheme, and indistinguish ability under the chosen-cipher text attack (IND-ID-CCA) is a harder assumption than IND-ID-CPA. Our protocol is designed to achieve the stronger security, called adaptive anonymous IND-IDCCA(ANON-ID-CCA), which is equivalent to the property of semantic security.

Modules:

PKG: It is responsible for generating system's globalparameter, and private keys for DO and DC.

Data owner: The DO uses a mobile device to access or send encrypted data. Once this action has been performed successfully, the CC can store the encrypted data with keyword in the cloud storage space.

Data consumer: The DO, who obtains his/her private key from the PKG, allowed to perform the decryption process over the encrypted data.

Cloud controller: It is responsible for data processing,such as data computation and storing on behalf of the cloud users.

CONCLUSION

In this paper, a new identity-based authenticated data sharing (IBADS) protocol is designed for cyber-physical cloud systems based on bilinear pairing. In the IBADS, there are two phases. First, a new data owner needs to register. Second, the data owner sends an encrypted message to the untrusted cloudcontroller using some client devices. We then demonstrated the security and correctness of the protocol, as well as evaluating its performance..

References:

[1] Nurul Hidayah Ab Rahman, William Bradley Glisson, Yanjiang Yang,and Kim-Kwang Raymond Choo. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1):50–59,2016.

[2] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. Cyberphysical systems information gathering: A smart home case study.Computer Networks, 138:1–12, 2018.

[3] Hoang T Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile cloud computing: architecture, applications, and approaches.Wireless communications and mobile computing, 13(18):1587–1611,2013.

[4] Qiang Liu, Jiafu Wan, and Keliang Zhou. Cloud manufacturing service system for industrial-cluster-oriented application. 15(3):373–380, 2014.

[5] Daqiang Zhang, JiafuWan, Qiang Liu, Xin Guan, and Xuedong Liang. A taxonomy of agent technologies for ubiquitous computing environments.KSII Transactions on Internet and Information Systems (TIIS), 6(2):547–565, 2012.

[6] Jiafu Wan, Hehua Yan, Di Li, Keliang Zhou, and Lu Zeng. Cyberphysical systems for optimal energy management scheme of autonomous electric vehicle. The Computer Journal, 56(8):947–956, 2013.

[7] Ragunathan Rajkumar. A cyber–physical future. Proceedings of the IEEE, 100(Special Centennial Issue):1309–1312, 2012.

[8] Akshay Rajhans, Ajinkya Bhave, Ivan Ruchkin, Bruce H Krogh, David Garlan, Andr´e Platzer, and Bradley Schmerl. Supporting heterogeneity in cyber-physical systems architectures. IEEE Transactions on Automatic Control, 59(12):3178–3193, 2014.

[9] Burak Demirel, Zhenhua Zou, Pablo Soldati, and Mikael Johansson.Modular design of jointly optimal controllers and forwarding policies for wireless control.

IEEE Transactions on Automatic Control, 59(12):3252–3265, 2014.

[10] Zhaogang Shu, Jiafu Wan, Daqiang Zhang, and Di Li. Cloud-integrated cyber-physical systems for complex industrial applications. Mobile Networks and Applications, 21(5):865–878, 2016.