Secure Key-composite Cryptosystems through scatter Aggregate Keys for Global secured data

Bondugula Prasanth[1], M. sravanthi[2]
[1]*CSE Department, GYANA SARASWATHI College of Engineering & Technology, Nizamabad*
[2] *Assistant professor, CSE Department, GYANA SARASWATHI College of Engineering & Technology, Nizamabad*

Abstract- **Secure and efficient report garage and sharing through authenticated bodily devices remain challenging to attain in a cyber-physical cloud environment, particularly due to the variety of devices used to get right of entry to the offerings and records. Thus on this paper, we gift a light-weight identity-based totally authenticated information sharing protocol to offer at ease records sharing amongst geographically dispersed bodily gadgets and customers. The seasoned-posed protocol is verified to face up to selected-cipher text attack (CCA) beneath the hardness assumption of decisional-Strong Diffie- Hellman problem. We also evaluate the overall performance of the proposed protocol with present facts sharing protocols in terms of computational overhead, communication overhead, and reaction time.**

Index Terms- Random oracle model, Privacy protecting cloud, Identity-based Cryptography, Data sharing protocol, AVISPA, Cloud computing.

INTRODUCTION

Cloud-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... In such systems, client devices be used to access the relevant 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). 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 is handover to the _central processors connected to the servers for processing. Based on the home agent and mobile subscriber data stored in the relevant databases, mobile network operators can decide whether to provide or decline requests to access particular services. 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. There are, however, a number of security challenges for such an environment, such as the following:

Mutual Authentication: This is one of the most fundamental security attributes required in CPSs (and generally many other systems). It is assumed that the server may be dishonest or not fully trusted. Specifically, both client and server first complete the authorization process by verifying the authenticity of each other, prior to exchanging any confidential data over public networks.

Anonymity: This allows the hiding of the identity of the client or user, even when an adversary has intercepted some messages from the public channel.
Password protection: The need to ensure password protection in password-based authentication systemis clear, and the client device is usually one of the weaker links. Specifically, the client or user generally uses low entropy password to facilitate memorization, and such passwords are vulnerable to password guessing attacks.

Impersonation resilience: Client-server communication protocol runs are executed over an insecure channel, and thus a malicious user can

attempt to impersonate as either the client or the server to the other party.

Data integrity & confidentiality: A secure protocol should provide strong data integrity and confidentiality for every transmitted message. Data integrity assures the receiver that the message has not been modified, and confidentiality_ensures_that only authorized users/devices can have access to the data. There have been a number of studies focusing on the security of CPS in recent years,

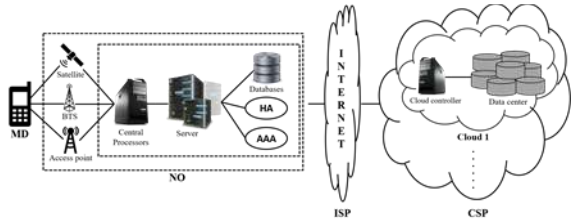


Fig. 1: An example of cloud-assisted cyber-physical computing architecture

collected in urban area (e.g. via house sensors, GPS devices, and weather sensors). In other words, data are being collected from a diverse range of devices, and analyzed to inform decision making. In 2011, the presented a new platform for dealing with urban services. And extended their framework proposed in based on the session_initiation protocol (SIP). A key limitation with SIP is network constraints. As smart mobile (e.g. Android and iOS devices) become increasingly commonplace, there has been a shift from cloud computing to mobile web computing studied provable data possession (PDP) and proposed a mobile based security protocol for cloud-based data sharing. Their protocol is implemented using using bilinear.Pairings and merkle hash tree, and its security proven under the random oracle model (ROM). and also proposed a secure data access mechanism for mobile web, where access control is achieved by combining both static and dynamic attributes. Mobile web has also been studied in a healthcare context and solutions proposed include those based on identity_based_encryption scheme.

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

The protocol is designed to achieve authentication between a physical device & the controller, and provide a secure end-to-end secure communication in the web using IBE scheme. Specifically,

[1] Our 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 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.

PKG: It is responsible for generating system's global parameter, 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 then encode data with keyword in the web storage space.

Data consumer: The DO, who obtains his/her private_key of the P Ktt, allowed to perform the decryption process over then encode data.

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

These entities perform some tasks based on their require- ments. First, user (DO and DC) registers himself/herself through a mobile device. In order to store some data in the cloud, the DO needs to login and performs a mutual communication between the mobile and the CC. Once it is completed, the DO is able to undertake secure (end-to-end) transactions, Any registered user, who act as a DC, wishes and toaccess the stored data will need to login and submit a query to the CC. Only after a successful login, the CC sends then encode data to the DC. In order to decrypt, DC contacts the P Ktt and receives a private key associated with its unique

identity, and then proceeds to decrypt then encode data using that private key. The process is also presented in Figure 2.

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 in distinguishability, an adversary is unable to distinguish between ciphertext pairs based on the chosen-message they have encrypted. In distinguishability under chosen-plain text attack (IND-ID-CPA) for Identity_based Encryption (IBE) scheme, and indistinguishability 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-ID- CCA (ANON-ID-CCA), which is equivalent to the -property semantic security. Next, the structure of IBE scheme is discussed.

EXISTING SYSTEM

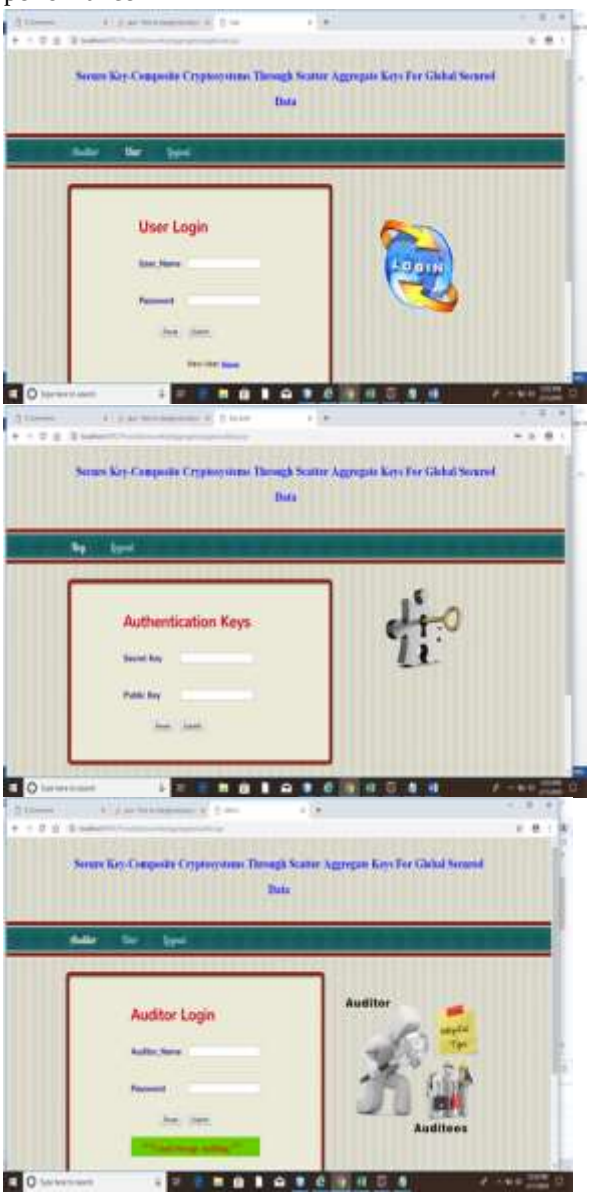
Cloud-assisted cyber-bodily structures (Cloud-CPSs; additionally called cyber-bodily cloud structures) have huge applications, ranging from healthcare to clever electricity grid to smart cities to battlefields to navy, and so on. Secure and efficient report storage and sharing through authenticated bodily gadgets stay tough to acquire in a cyber-bodily cloud environment, specially because of the variety of devices used to get right of entry to the services and facts.

PROPOSED DEVICE

Our proposed protocol presents mutual authentication, and crucial functions together with client registration, login, mutual authentication, password renewal. The protocol additionally guarantees person anonymity. We additionally display its resilience in opposition to known security attacks (e.G., insider assault, impersonation attack, consultation key computation assault), and its correctness using AVISPA simulation device. Once the bodily gadgets are authenticated, the next segment is relaxed stop-to-give up conversation. For this, the proposed encryption technique is used on bilinear pairing with a small public parameter-length. We then display that it is IND-ID-CCA relaxed based totally at the decisional-SDH (Strong Diffie-Hellman) assumption.

CONCLUSION

In_this_paper, a brand new identification-primarily based authenticated facts sharing (IBADS) protocol is designed for cyber_physical cloud systems based on bilinear pairing. In the IBADS, there are phases. First, a brand new data proprietor needs to sign up. Second, the statistics owner sends an encrypted message to the untrusted cloud controller using some customer devices. We then proven the security and correctness of the protocol, as well as comparing its performance



REFERENCES

[1] Nurul Hidayah Ab Rahman, William 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. Cyber- physical systems. Computer Networks, 138:1–12, 2018.

[3] Hoang T Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile web computing: architecture, applications, and approaches. 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, Jiafu Wan, 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. Cyber- physical 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.