Provably Secure and Light Weight Identification Based Data Sharing Protocol in Cloud Environment

[1]Prof.Vishal Shinde, [2]Mr. Rushabh Baranwal , [3]Mr. Vignesh Elagandula, [4]Mr. Shubham Tripathi

[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhale College of Engineering & Technology, Asangaon, Maharashtra, India. *mailme.vishalshinde@gmail.com,* [1]*baranwalrushabh1110@gmail.com,* [2]*vignesh21.er@gmail.com,* [3]*st64751@gmail.com,*

Abstract - In a cyber-physical cloud context, Share and store files that is both secure and efficient via authorized physical devices remains a challenge, especially given the variety of devices to obtain access to the service and data. As a result, we describe a lightweight identity-based authenticated data sharing protocol in this work, which allows for safe data exchange among geographically separated objects and clients. under the assumption of hardness the decisional-Strong Deffie Hellman (SDH) issue, the suggested protocol is shown to withstand chosen-cipher text attack (CCA). In terms of computing cost, transmission overhead, and reaction time, we also compare the proposed protocol to existing data sharing methods.

Keywords – Secure, identification, Data sharing, Cloud.

I. INTRODUCTION

Cloud-assisted cyber-physical systems (Cloud-CPSs; also known as cyberphysical cloud systems) have a wide range of applications, including healthcare, smart grids, smart cities, battlefields, and military, among others. Client devices (e.g., Android and iOS smartphones, or resource-constrained devices like sensors) can be utilized to obtain access to relevant services (e.g., utility use data evaluated and saved in the cloud in the context of a smart energy grid) from/via the cloud in such systems. Client devices also often have lower computational capabilities and, as a result, are less likely to have effective security (technical) safeguards than traditional personal computers (PCs). When a mobile device is used to represent a client device, it is referred to as a client device. The mobile device establishes a connection. A cloud-assisted cyber-physical or cyber-physical cloud computing architecture is an example. When a mobile user demands that certain activities be completed, data (such as identification and location) is passed to central processors linked to the servers for processing. Based on information from the house agent (HA) and cellphone subscribers. At the current world of networking system, Cloud computing is it is important to remember this and developing idea for both the developers and the users

II. AIMS AND OBJECTIVE

a) Aim

To develop a provably safe and lightweight identity-based authenticated data exchange protocol for the cyber-physical cloud. Share and store files that is both secure and efficient via authorized physical devices remains a challenge,, especially given the variety of devices used to access the services and data.

b) Objective

An input described by a user is transformed into a computer-based system through the design process. This design is critical for avoiding data entry errors and directing management as soon as possible for collecting accurate system information from the computer.

It is accomplished by designing user-friendly data entry panels that can manage enormous amounts of data. The purpose of input design is to make data more accessible.

III. LITERATURE SURVEY

Paper 1: **Cyber-Physical Cloud Systems:**

A Forensic-by-Design Framework-Businesses are increasing threats from cyber-physical attacks on cyber physical cloud systems by providing expanded access, improved software capability, and continuing advances managing supply chains options to customers and employees (CPCS). Before conceptualizing forensic-by-design for CPCS methodology, the authors examine the obstacles involved with a attacks such as CPCS emphasize the need for forensic by-design.

Paper 2: Cyber-physical systems with cloud integration for complicated industrial applications-

Cyber-Physical Systems (CPS) may now more firmly integrate cyberspace into the physical world than ever before, thanks to recent breakthroughs in Wi-Fi sensor networks, big data, mobile, and cloud computing. Cloud-based systems can also provide huge storage capacity, low-cost computation,

DOI : 10.35291/2454-9150.2022.0156

and the freedom to customize the operating environment for Complex Industrial Applications (CIA). In our opinion, Cloud-integrated CPS (CCPS) will make it possible to build, deploy, administer, and control hitherto unthinkable application scenarios. In this study, we discuss Technology that allows CIA to operate and suggest a unique architecture for CCPS (dubbed CCPSA). Then, from the CIA's perspective, we evaluate three potential difficulties and offer solutions, incorporating virtualized resource management

Paper 3: A pairing-free and provably secure certificate less signature scheme

The private (KGC) and the signer in the CLS, ensuring that no vengeful KGC poses as the true signer. A variety of CLS systems with bilinear pairing have recently been suggested, and their immunity has been demonstrated using a security and their immunity has been demonstrated using a common security model.

A variety of CLS systems with bilinear pairing have recently been suggested and their immunity has been demonstrated using a common security model. One such pairing process is well known to have Boosted computational power cost than the other cryptographic operations..Includes issues controlling access to a building and key management. Data security in the cloud relates to data confidentiality, integrity, availability, and traceability (CIAT), which are all standards that cloud computing must meet. In the context of data confidentiality information accessible only by logging in or disclosed by authorized individuals, entities, or IT systems. In order for data integrity to exist, data is kept in its original state and the document has not been modified or deleted, either intentionally or accidently.

4) Efficient and provably secure random oracle-free adaptive identity-based encryption with short-signature scheme

Identity-based encryption (IBE) is one of the important public key encryption techniques where not only the identity of the receiver is used for secure and efficient encryption, but it also has several merits over other traditional publickey ones. However, two main disadvantages of many such IBE-based systems are the requirement of a large number of public parameters and different random oracle operations, where it is known that a random oracle due to improper implementation is vulnerable under chosen ciphertext attack. This paper designs an efficient IBE scheme (ROFIBE) with recipient anonymity, reduction in public parameters and random oracle-free operation. The scheme is developed based on a proposed hard problem, named as decisional extended bilinear Diffie-Hellman assumption (DEBDH) and on analysis it is found to be secured under standard security model. In addition, a new short-signature scheme based on the proposed IBE is developed.

Sr No	Author	Project Title	Publication	Technology	Purpose
1	Nurul Hidayah Ab Rahamn	Forensic-by- Architecture for a cyber-physical cloud system	IEEE, 2016	CPCS	Businesses offer increased access and improved software functions to customers and employees.
2	Zhaogang shu	Cloud-integrated cyber-physical system for complex industrial application	IEEE,2015	CCSPA	The cloud-based system it offers low-cost computing and large storage resources
3	GP Biswas	A short signature scheme based on adaptive identity-based encryption that is efficient, secure and Oracle-free	IEEE,2016		Diffe-Hellman's strong q-extended bilinear assumption is difficult to solve
4	Arjit Karati	A pairing-free and provably secure certificateless signature scheme	IEEE,2018		Using Scheme, you can solve the key escrow problem in identity-based cryptography

Table No.1: Comparative Analysis

V. EXISTING SYSTEM

. • With the rise in approval of cloud computing, the question of how to search securely and efficiently data is transmitted over encrypted cloud services has develop a topic.

- The authentication mechanism is discussed in order to verify the client's authorization when logging into the cloud server. Password guessing attacks, impersonation attacks, session key discloser attacks, and other security issues may be encountered using this type of authentication approach.

- Data encryption makes effective data retrieval a difficult task.

VI. PROBLEM STATEMENT

Data security, identity and access control, key management, and virtual machine security are all security concerns in cloud computing. In fact, data security Includes issues controlling access to a building and key management. Data security in the cloud relates to data confidentiality, integrity, availability, and traceability (CIAT), which are all standards.

In fact, data security Includes issues controlling access to a building and key management. Data security in the cloud

DOI : 10.35291/2454-9150.2022.0156

relates to data confidentiality, integrity, availability, and traceability (CIAT), which are all standards that cloud computing must meet.

VII. PROPOSED SYSTEM

•Under the hardness assumption of the decisional-Strong Diffie-Hellman (SDI-I) problem, According to the protocol, shown to withstand chosen-cipher text attack (CCA)

. Identity-based encryption (IBE) is a cryptographic method that applied to make data sharing more secure. As a result, we develop an identity-based authentic data sharing (IBADS) protocol in this work to ensure data security in cyber-physical cloud systems.

According to the protocol, intended to allow safe end-to-end secure communication in the cloud by achieving authentication between a physical device and the cloud controller using the IBE method.

VIII. ALGORITHM

The Diffie-Hellman technique is used assuring a shared secret that may be utilized for secret conversations while transferring data over a public network.

P, G Public Keys are provided for Robin Sam.

P, G are the public keys that are currently available.

Selected Personal Secured Key = r

Selected Personal Secured Key = s

x = G Power of r mod P

y = G Power of s mod P

Step1.START

Step 2: Robin and Sam acquire public telephone numbers. P = 23; G = 9.

Step 3: Robin chose a private key with the value r = 4 and Sam chose s = 3 as his private key.

Step 4: Robin and Sam figure out what the public values are.x = (9 Power of 4 mod 23) = (6561 mod 23) = 6 Robin y = (9 Power of 3 mod 23) = (729 mod 23) =16 Sam

Step 5: Robin and Sam exchange phone numbers with the public.

Step 6: Robin obtains the public key y =16 and follows the instructions. Sam is given the x = 6 public key.

Step 7: Robin and Sam calculate the symmetric keys. kr = y Power of r mod p = 65536 mod 23 = 9 Robin: kb = x Power of b mod p = 216 mod 23 = 9 Sam

STEP 8: STOP

IX. MATHEMATICAL MODEL

The proposed IBE scheme is fair and consistent, in the sense that for a valid ciphertext generated by any registered client device, the decryption algorithm run by another registered client device computes and obtains the correct plaintext.

Proof: In order to obtain the correct plaintext for user i, the decryption algorithm proceeds with CT = {C, T, MD} using the private key Sl<i = g r mod p as follows:

Z = e (Ti , SKi) =e (g IDih) s, ga ß+lDi = e (g IDi ß+lDi =e(g, g) as Now it computes and checks LHS = MO = (C 0 • Z) mod p = (C s 0 2 mod p) • e(g, g) as mod p =

Extract Bc = Ac O h(lDcl I PWc)

Choose randomly, Compute

Anewc = Bc 9 h(lDcl I PWcnew)

Dc = h (lDc O PWcnew)

Ec = Wc O h(PWcnew) Drop Ac

Store hAnewC, Dc, Ec, TlDci hAnewc

Compute

If (DC* 6= Dc), abort the session

Otherwise, Generate a random number Rc

Calculate

Bc = Anewc O h(lDcl I PWcnew) Wc = Ec O h(PWcnew)

Fc = h(lDcl I I Rc) Gc = EWc(lDcl IRC)

If TIDC is not in database abort the session

Extract Wc

Calculate

= h(lDcl Iscc)

= h(lDcl I Rc)

If), abort the session

Otherwise, generate an random number Rcs

Compute

Sl<cs = h (lDcl IRcsl IRC) Kc = h (lDcl ISI<csl I Rcs)

Rccs = Rc O Rcs

Extort

Compute

= h(lDcl I RCS* I IRC)

= h(IDcl ISKC*I I Rcs)

If (KC* 6= l<c) the CC is unauthenticated hKc,Rccsi

DO Data owner with cloud assisted mobile device .

X. SYSTEM ARCHITECTURE

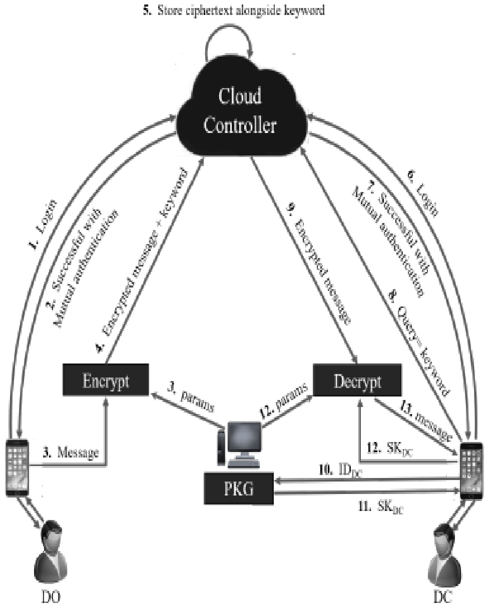


Fig.1.: Network model for assuring cloud data security by the proposed IBADS protocol.

XI. ADVANATGES

1. Cost: Only pay for the resources you utilize.

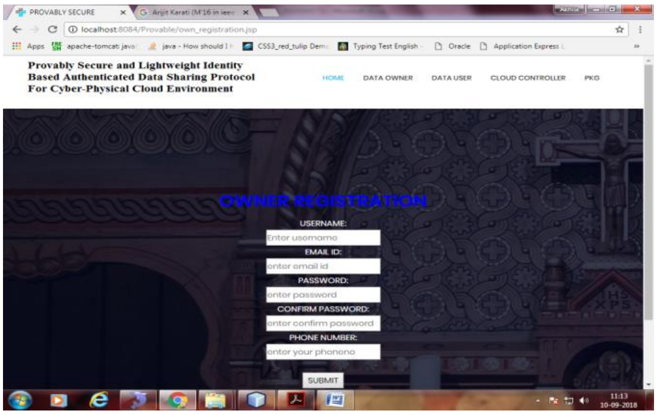
2. Security: To strengthen security, cloud instances are networked separately from other instances.

DOI : 10.35291/2454-9150.2022.0156

3.Performance: For enhanced performance, instances may be created instantaneously. Clients have access to all of the Cloud's main hardware resources.

4.Scalability:Deploy cloud instances automatically as needed.

XII. Design Details :



Provably Secure and Lightweight Identity Based Authenticated Data Sharing Protocol For Cyber-Physical Cloud Environment

OWNER REGISTRATION

USERNAME: Enter username

EMAIL ID: enter email id

PASSWORD: enter password

CONFIRM PASSWORD: enter confirm password

PHONE NUMBER: enter your phonено

Fig.2: Login Page

XIII. CONCLUSION

Thus, we have tried to implement the paper Nurul Hidayah Ab Rahamn, Zhaogang shu, GP Biswas, Arjit Karati, "Forensic-by- Architecture for a cyber-physical cloud system" , CPCS 2016 and according to the implementation, the conclusion is that, for cyber-physical cloud systems, a new identity-based authenticated data sharing (IBADS) protocol pairing based on bilinearity is presented in this study. The IBADS is consist of two phases. A new data owner must first create an account. Second, the data owner encrypts the message it should be sent to an untrustworthy cloud controller using some client devices. The protocol's security and correctness, as well as its performance, were then demonstrated. We intend testing the feasibility of the proposed protocol as part of a real-world scenario by implementing a prototype in a future study.

XIV .REFERENCE

[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.

DOI : 10.35291/2454-9150.2022.0156