**Identity-based authenticated data sharing protocol for cloud Server**

**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.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The existing data sharing protocols in terms of computational overhead, communication overhead, and response time. * 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 indistinguishability, an adversary is unable to distinguish between ciphertext pairs based on the chosen-message they have encrypted. | * Proposed an architectural framework for CPS, using structural semantic mappings to assure consistency. * The proposed protocol is demonstrated to resist chosen-ciphertext attack (CCA) under the hardness assumption of decisional-Strong Diffie-Hellman (SDH) problem. * we present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients. |
| **EXISTING ALGORITHM**  Decisional-Strong Diffie-Hellman (SDH) | **PROPOSED ALGORITHM:-**  ID-based encryption, or identity-based encryption (IBE) |
| **ALGORITHM:**  Negligible function [48]). A function is  called negligible if, for every there exists. | **ALGORITHM DEFINITION:-**  ID-based encryption, or identity-based encryption (IBE), is an important primitive of [ID-based cryptography](https://en.wikipedia.org/wiki/ID-based_cryptography). As such it is a type of [public-key encryption](https://en.wikipedia.org/wiki/Public-key_encryption) in which the [public key](https://en.wikipedia.org/wiki/Public_key) of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user. |
| **DRAWBACKS:-**   * A key limitation * with SIP is network constraints. | **ADVANTAGES:-**   * Then the advantage * of the algorithm in solving CDH in G1 is defined |

**System model with a cloud server, a data owner and data users.**

****

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE