# PROVABLY SECURE AND LIGHTWEIGHT IDENTITY-BASED AUTHENTICATED DATA SHARING PROTOCOL FOR CYBER-PHYSICAL CLOUD ENVIRONMENT

# 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 DiffieHellman (SDH) problem.

# CONTINUE

- We also evaluate the performance of the proposed protocol with existing data sharing protocols in terms of computational overhead, communication overhead, and response time.

# EXISTING SYSTEM

- 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.
- 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.

# CONTINUE

- A number of security challenges for such an environment, such as the following:
- **Mutual Authentication**
- **Anonymity**
- **Password protection**
- **Impersonation resilience**
- **Data integrity and confidentiality**

# PROPOSED SYSTEM

- 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.
- Once the physical devices are authenticated, the next phase is secure end-to-end communication.

# CONTINUE

- 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.

# HARDWARE REQUIREMENTS

| | | |
|---|---|---|
| Processor | - | Pentium –III |
| Speed | - | 1.1 Ghz |
| RAM | - | 256  MB(min) |
| Hard Disk | - | 20 GB |
| Floppy Drive | - | 1.44 MB |
| Key Board | - | Standard Windows Keyboard |
| Mouse | - | Two or Three Button Mouse |
| Monitor | - | SVGA |

# SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

# 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 cloud controller using some client devices.
- We then demonstrated the security and correctness of the protocol, as well as evaluating its performance.

# 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.

# CONTINUE

[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. Cyberphysical systems for optimal energy management scheme of autonomous electric vehicle. The Computer Journal, 56(8):947–956, 2013.