DEVELOPING A SECURE REMOTE PATIENT MONITORING SYSTEM

Sarmistha Neogy

Sayantani Saha

Jadavpur University
Kolkata, India

AGENDA

- Introduction
- Security issues of the application
- Proposed protocol suite
- Discussions
- Remarks

INTRODUCTION

- Objective

The work in this paper focuses on developing a security protocol suite that takes care of a mobile cloud computing (MCC) system with respect to a specific application area. The protocol considers remote user authentication and subsequently develops secure access to data retained using cloud infrastructure.

INTRODUCTION

- Mobile Cloud computing

Cloud computing offers and allows users to use infrastructure, platforms, and software as services (IAAS, PAAS, SAAS). With the advent of mobile computing, and cloud computing supporting mobile services, a merger of both these computing has opened a new domain of mobile cloud computing.

APPLICATION :
A REMOTE PATIENT MONITORING SYSTEM

- The application focuses on maintaining and monitoring medical data of a remote patient.

- We assume that health worker will monitor a patient in remote location, from time to time and upload relevant data to cloud via cloud-based service.

APPLICATION :
A REMOTE PATIENT MONITORING SYSTEM

- A medical practitioner (sitting in his/her chamber or travelling from one chamber to another) may have a look into the data and prescribe back, via some cloud-based service.
- A patient can also have a look into his/her medical records. Hence they are also users of the cloud computing system.

SECURITY ISSUES

- Mobile networks allow users to move freely and access network seamlessly at the same time. In this scenario security aspects include:
  1. Authenticating users for using network resources
  2. Securing network resources
  3. Securing access to the resource
  4. Maintaining privacy of user

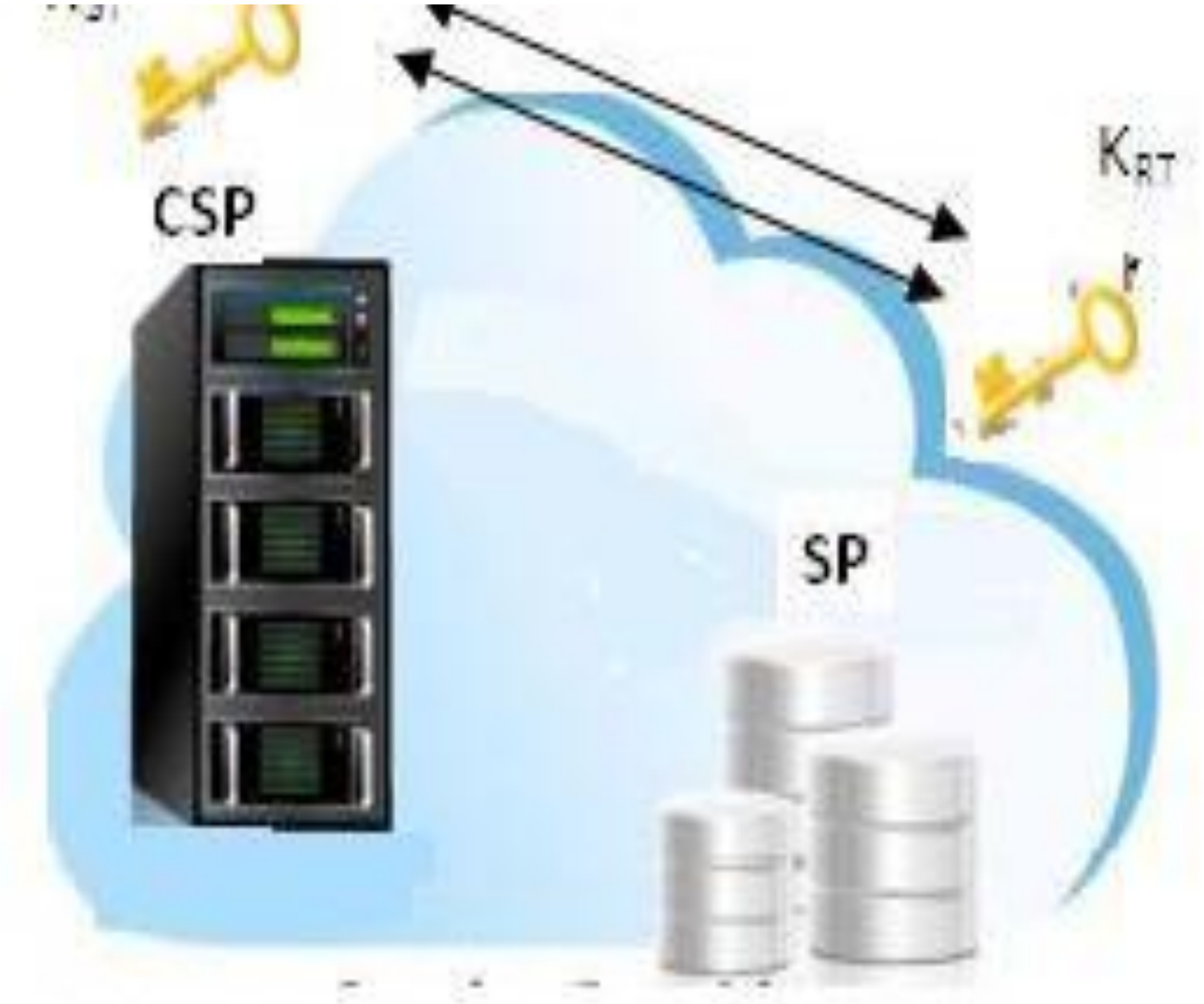
SECURITY ISSUES

- The tasks of the Cloud Service Provider (CSP) include :

  1. Storing the credentials for each user in secured storage (Storage Provider SP)
  2. Authenticating the remote user before giving him/her access to the network
  3. Protection of user privacy

PROPOSED PROTOCOL SUITE :: PROTOCOL I

- Phase I
  - Handshaking between CSP and SPs
    - Symmetric key K_{st} (storage) and K_{rt} (Retrieval) exchange
- Phase II
  - User Registration
    - CSP generates credential for user
    - CSP encrypts information
    - SP stores this encrypted information



HandShaking: Key Exchange

PROPOSED PROTOCOL SUITE :: PROTOCOL I ..

- Phase III
  - Mobile User Request (query)
  - Step – I (User authentication)
    - CSP asks SP for user information
    - SP retrieves and sends the encrypted information to CSP
    - CSP authenticates the user

PROPOSED PROTOCOL SUITE :: PROTOCOL I ..

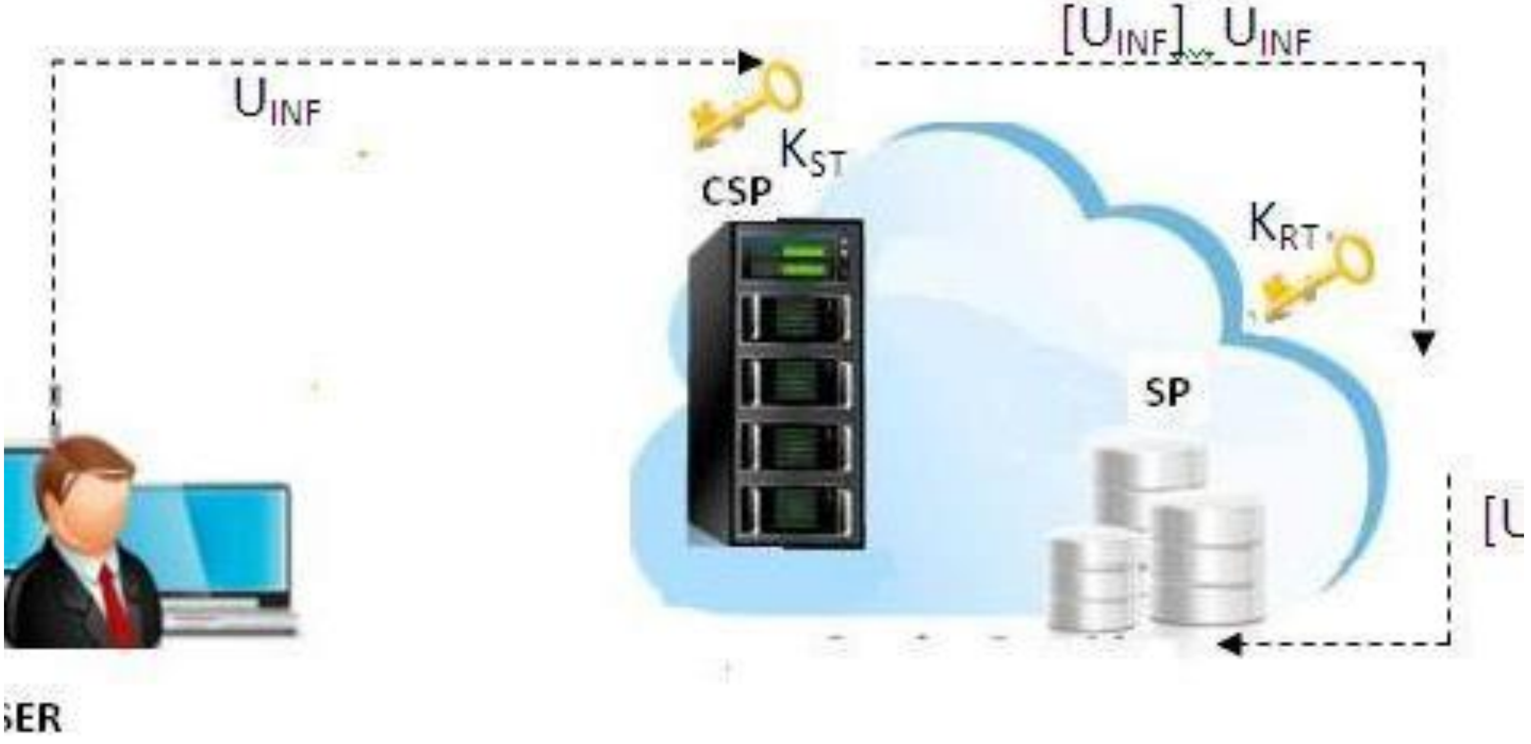
- Phase IV
  - Step – II (Query processing)
  - If user is authenticated
    - Authenticated user is granted request
    - Result to query is retrieved and sent back to user

USER REGISTRATION

- When user registration is done, user information (U_{inf}) is generated and encrypted ([U_{inf}]) using K_{st} by CSP.
- Both the information (U_{inf}) and ([U_{inf}]) is sent to the SP.
- SP checks the integrity of (U_{inf}).
- Encrypts (U_{inf}) using K_{rt} and stores it.
- If integrity is questionable, SP and CSP both initiate the generation of a new K_{st}.

USER AUTHENTICATION

- During information retrieval (for user authentication), SP sends both [U_{inf}] (stored with itself using K_{rt}) and U_{inf} to CSP.
- CSP checks the integrity of (U_{inf}).
- If any discrepancy is found, SP and CSP both initiate the generation of a new K_{rt}.



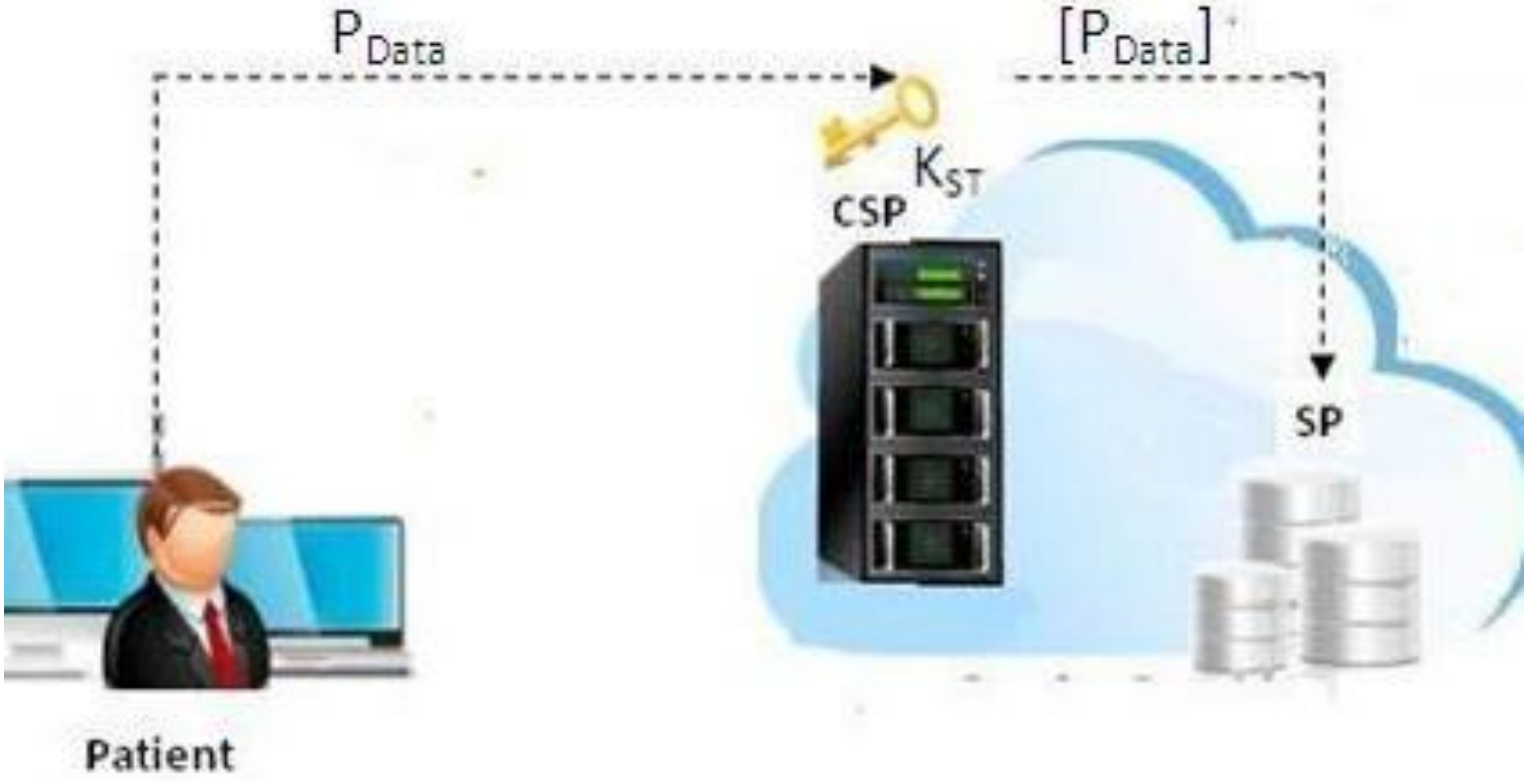
User Registration

PROTOCOL II

- *This protocol is concerned about firstly, the storage of remote patient data, and secondly, accessing the same by authorized user. Data will be stored presumably by health workers and accessed for monitoring purposes by doctors at their own conveniences.*

PROTOCOL II…

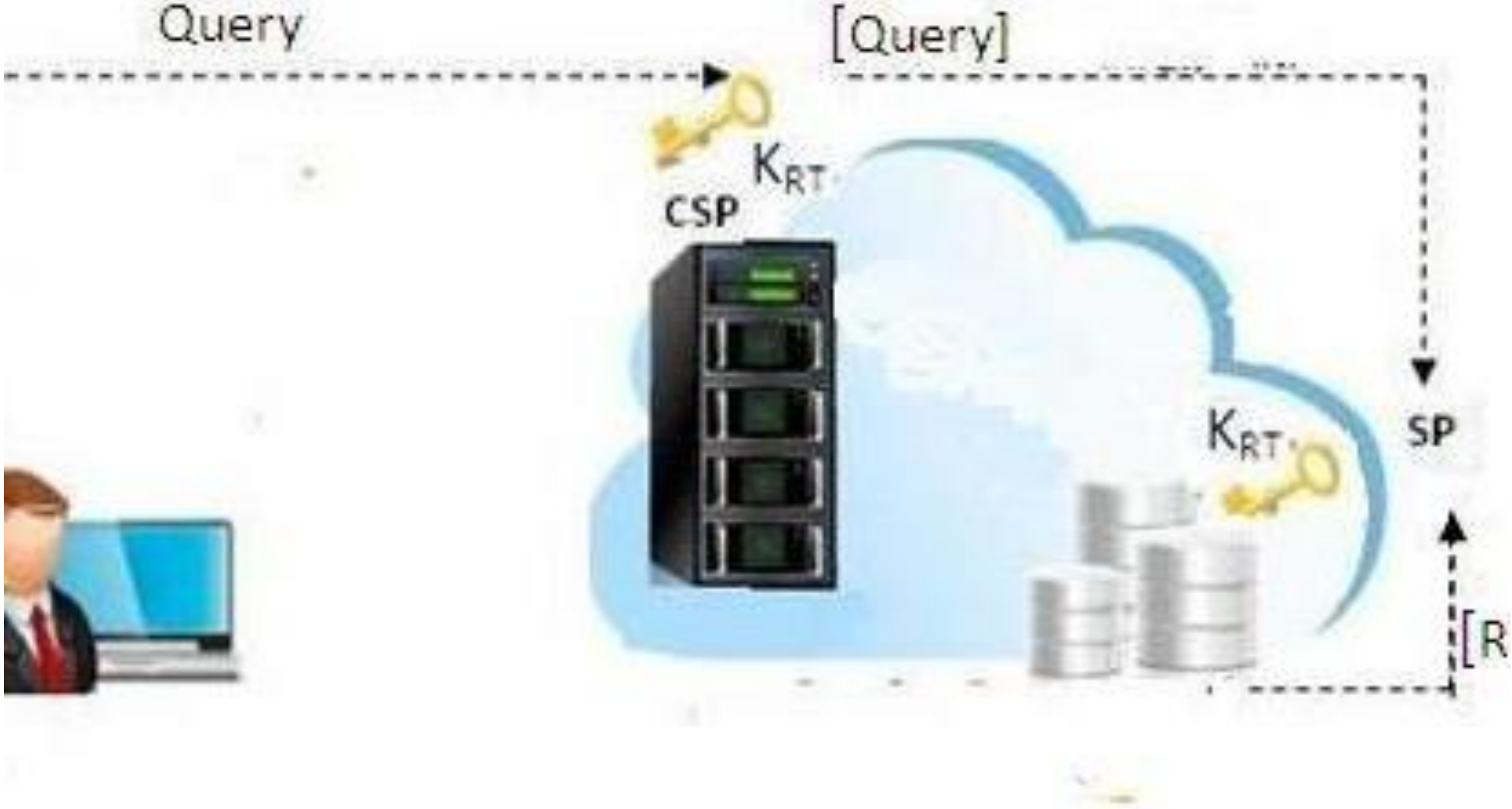
- Phase I : Data Storage
  - CSP maintains metadata about the patient information to be stored (homomorphic encryption).
  - The homomorphic data is further encrypted using K_{st} and sent to the SP.
  - New data of same patient to be appended to the already existing data.



Data Storage

PROTOCOL II (CONT..)

- Phase II (Data Retrieval)
  - The query posted by the user, is first encrypted using K_{rt} by CSP.
  - CSP sends the encrypted query to the SP.
  - The response generated by the SP is again encrypted using K_{rt}
  - SP sends encrypted result of query to CSP
  - CSP provides the response to the user.



Data Retrieval

CONCLUSION

- Security issues of mobile cloud computing with respect to a specific application of remote patient monitoring are discussed here.
- A protocol suite is proposed that covers the security aspects of the entire system.

CONCLUSION..

- Remote patient monitoring is required in cases where a patient is unable to move and a doctor can not also reach the patient frequently.
- Hence patient data being in cloud facilitates the doctor to access it as and when required, and take action accordingly.

REFERENCES

- [1] Biswas, K. Vallipuram, M. Sithirasenan, E. & Singh, K. (2014). A Simple Lightweight Encryption Scheme for Wireless Sensor Networks, *Lecture Notes in Computer Science Volume 8314*, 499-504
- [2] Dean, J. & Ghemawat, S. (December 2004). MapReduce: Simplified Data Processing on Large Clusters. In *OSDI'04: Sixth Symposium on Operating System Design and Implementation*.
- [3] Diffie, W.; Hellman, M. (1976)."New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644–654.
- [4] Dinh, Hong T., Lee, Chonho, Niyato, Dusit& Wang, Ping. (December 2013). *Wireless Communications and Mobile Computing, 13 (18)*, 1587-1611.

Thank You