Department of
Computer Engineering

Amirkabir University of Technology
(Tehran Polytechnic)

PSMPA

Jun Zhou, Xiaodong Lin, Xiaolei Dong, Zhenfu Cao

Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System

Cloud Computing Course Presentation

Course Instructor: Dr. Kalbasi

By: Amir Abas Kabiri Zamani

Agenda

- Problem Statement
- Related Works
- Solution Description
- Performance Analysis
- Conclusion
- References

Problem Statement

What is the field of study?

Distributed m-healthcare cloud computing system:

Problem Statement

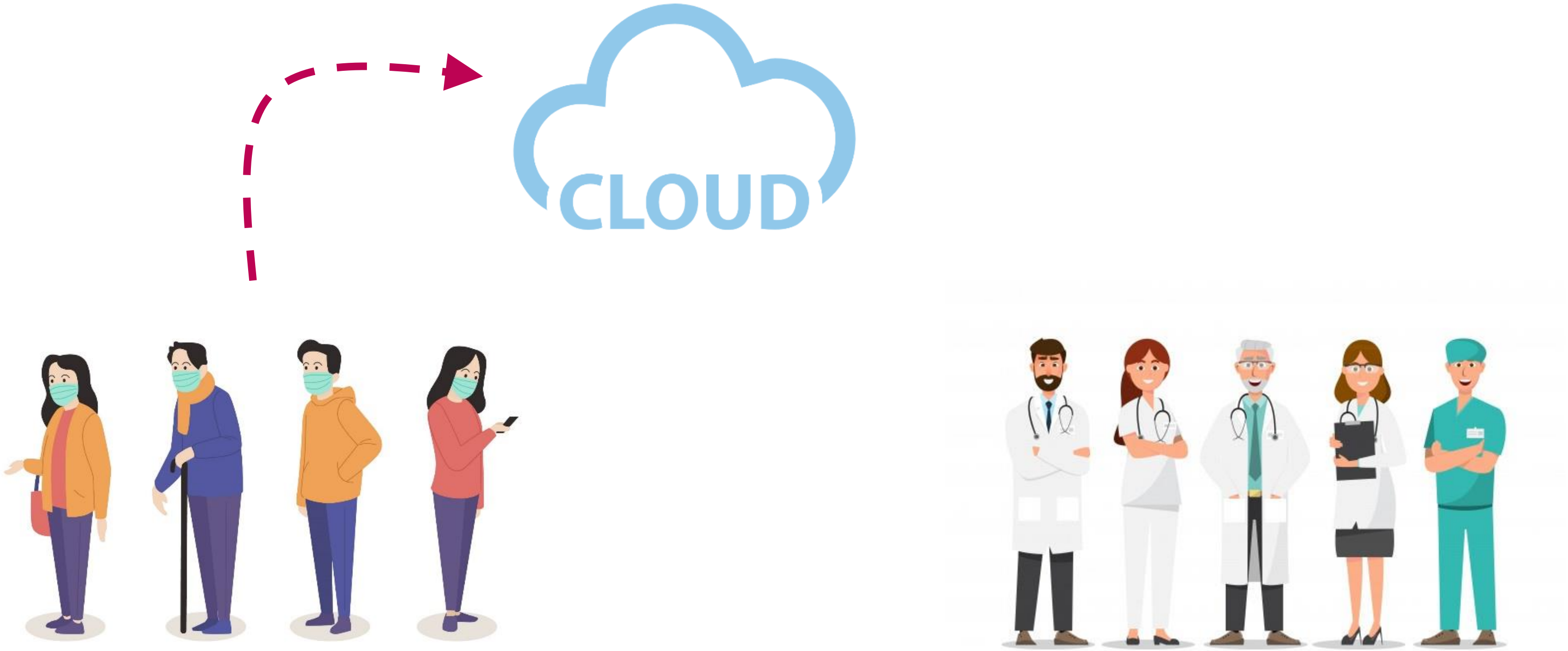
What is the field of study?

Distributed m-healthcare cloud computing system:

Problem Statement

What is the field of study?

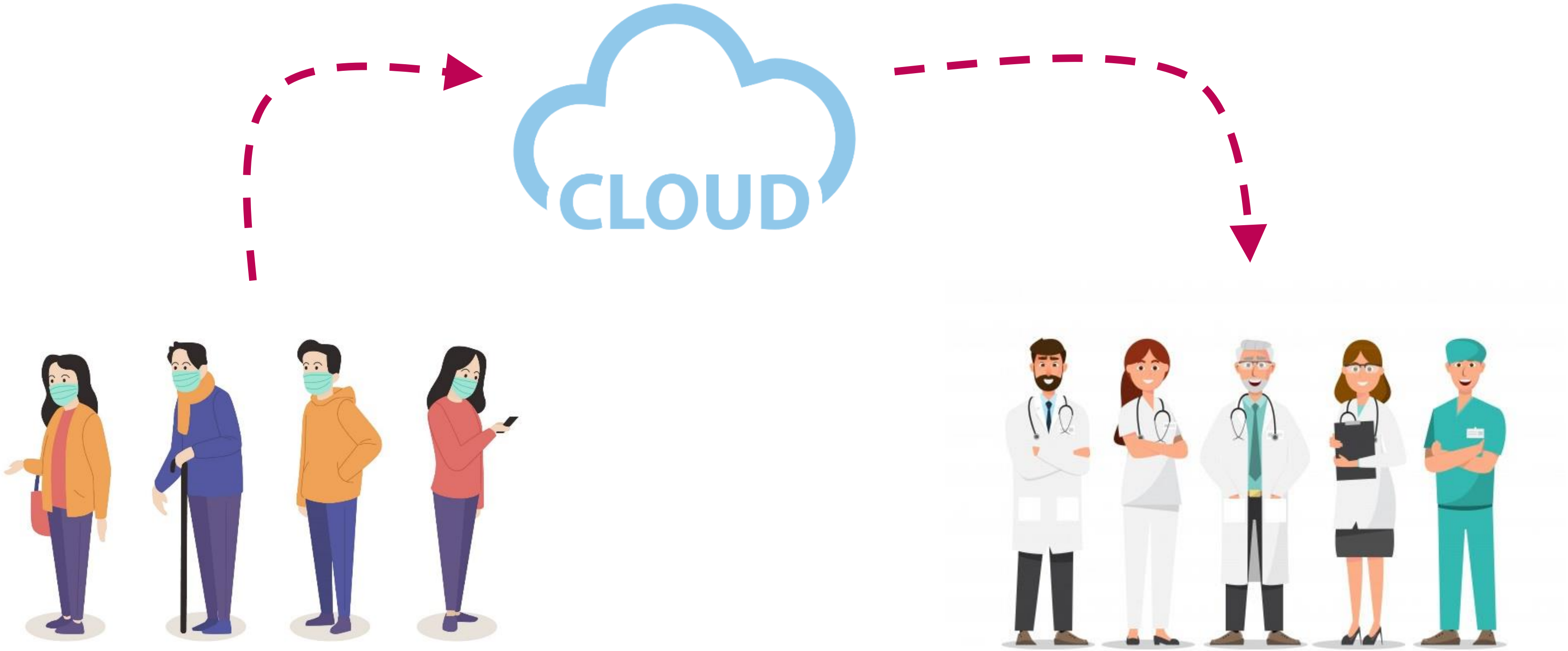
Distributed m-healthcare cloud computing system:



Problem Statement

What is the field of study?

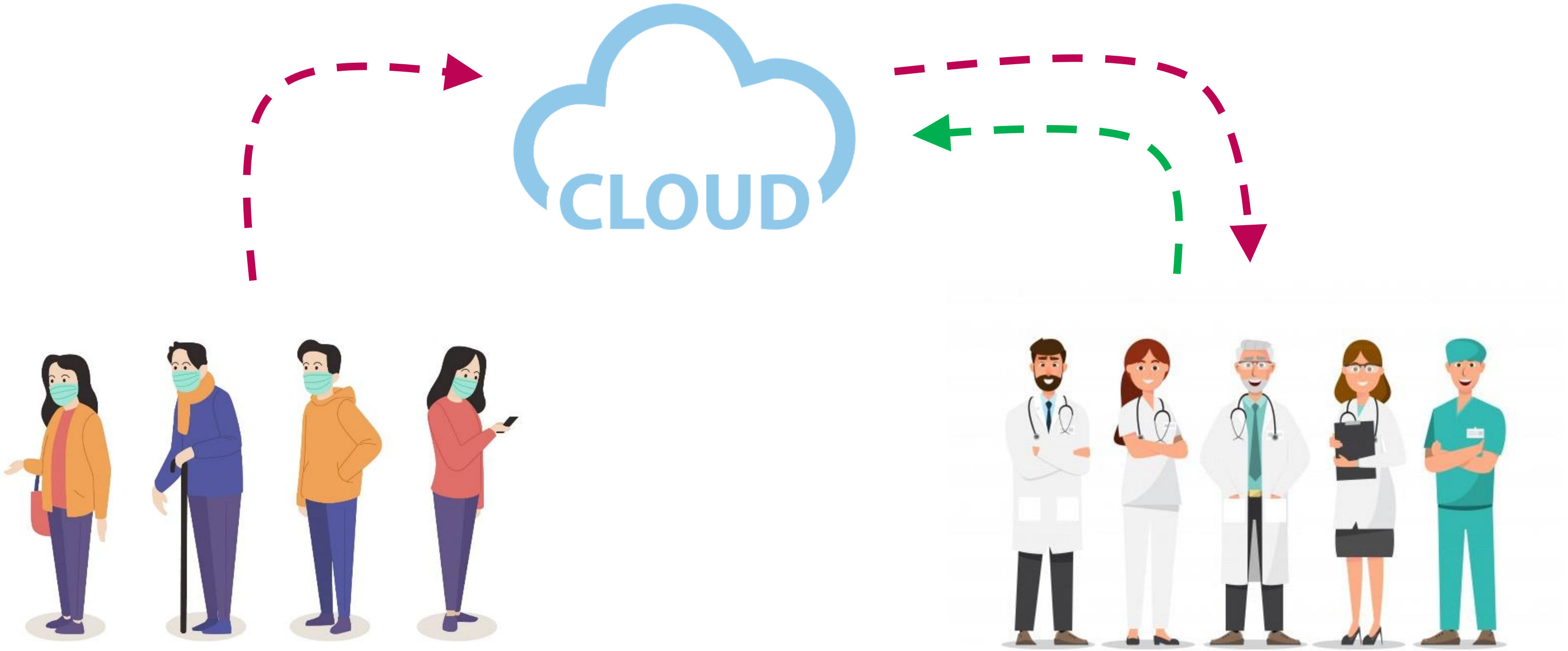
Distributed m-healthcare cloud computing system:



Problem Statement

What is the field of study?

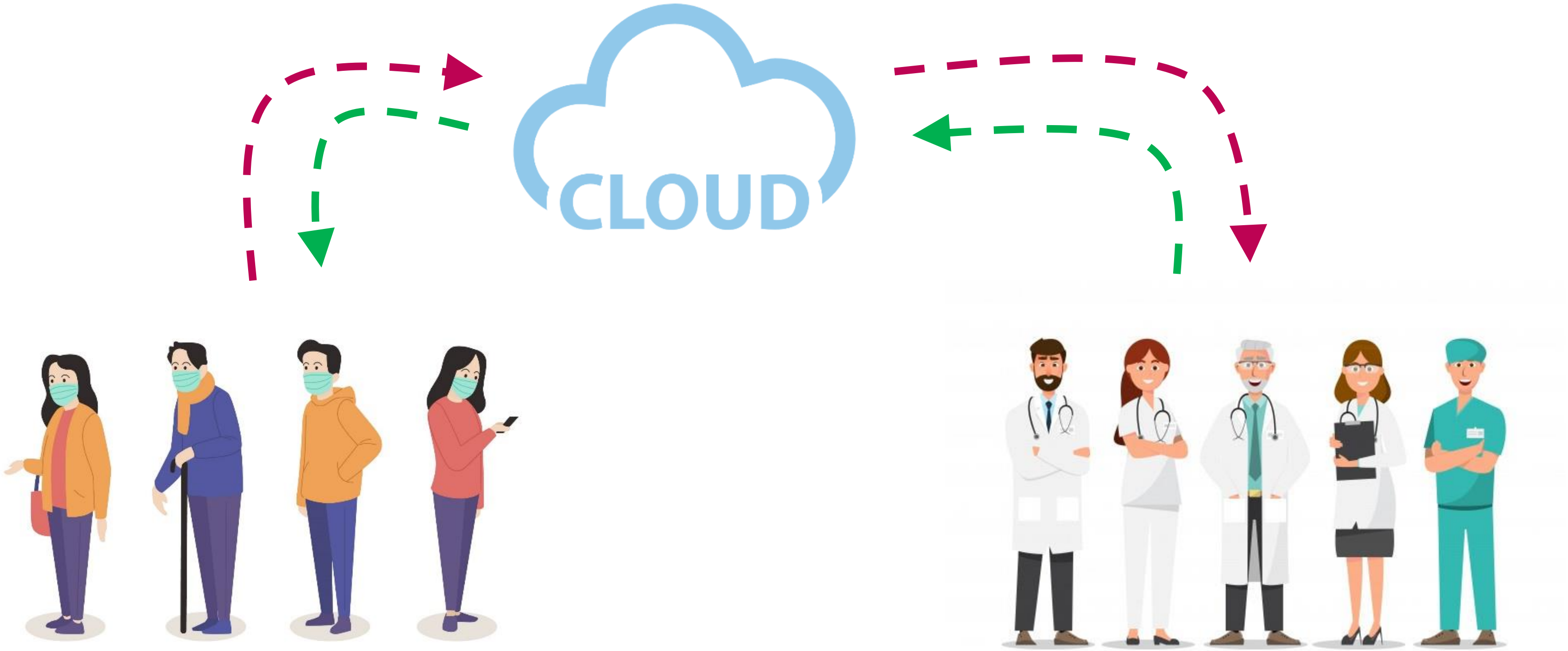
Distributed m-healthcare cloud computing system:



Problem Statement

What is the field of study?

Distributed m-healthcare cloud computing system:



Problem Statement

What are the challenges?

Distributed m-healthcare cloud computing system:

Problem Statement

What are the challenges?

Distributed m-healthcare cloud computing system:

- ❌ Data Confidentiality
- ❌ Patients Identity Privacy

Related Works

Previous works:

- *Pseudo Trust* [2]: Proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof
    - Cannot be straightforwardly exploited
    - Only consider data confidentiality in the central cloud computing architecture
- *Securing Personal Health Records in Cloud Computing* [3, 4] :Suggested patients have to consent to treatment and be alerted every time
    - Affects user experience

Solution Description

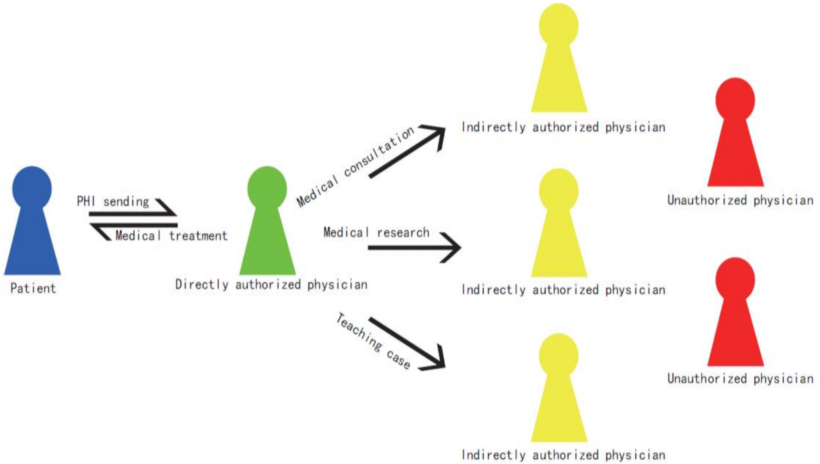
How PSMPA solves these challenges?

- A novel authorized accessible privacy model (AAPM)
- Patients can authorize physicians by setting an access tree supporting flexible threshold predicates
- Then, based on it, by devising a new technique of attribute-based designated verifier signature, PSMPA, is proposed:
  - Self-controllable
  - Multi-level
  - Privacy-preserving

Solution Description

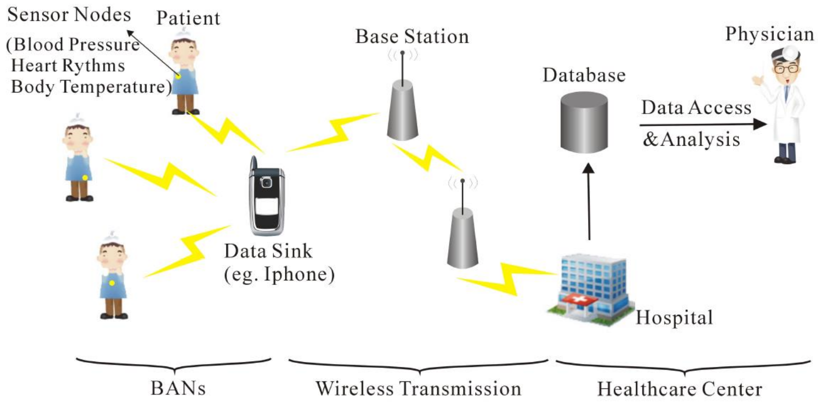
How PSMPA solves these challenges?

- The *directly authorized physicians*, the *indirectly authorized physicians* and *the unauthorized persons* in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets

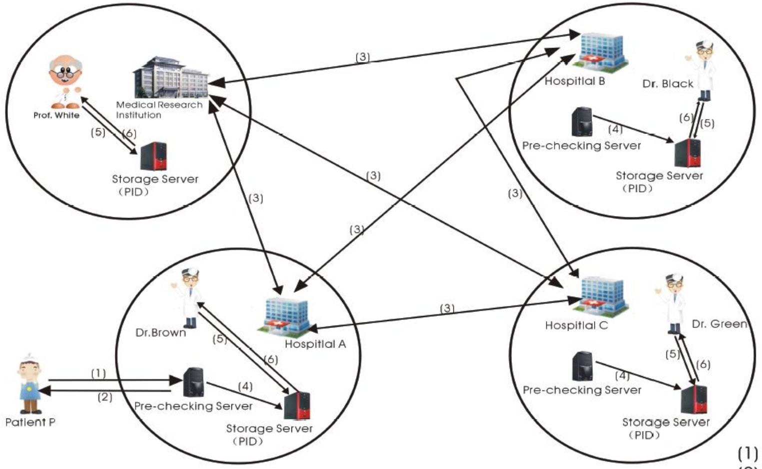


Solution Description

How PSMPA solves these challenges?



Basic architecture of the E-health system

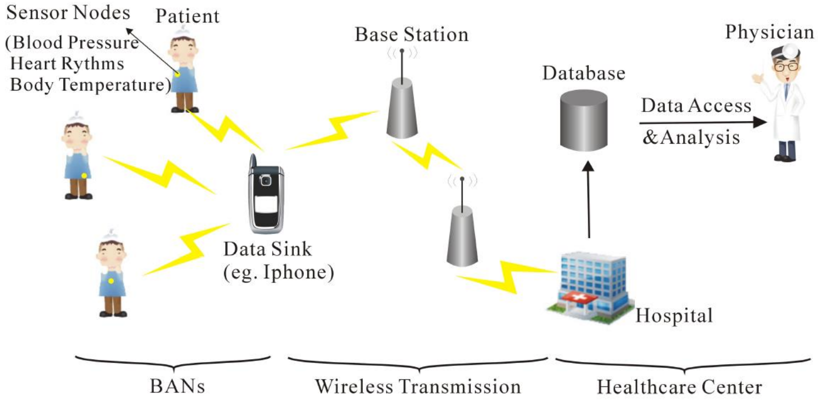


(1) PHI sending
(2) Medical treatment
(3) PHI sharing
(4) PHI storing
(5) PHI accessing
(6) PHI updating

The distributed model proposed within article

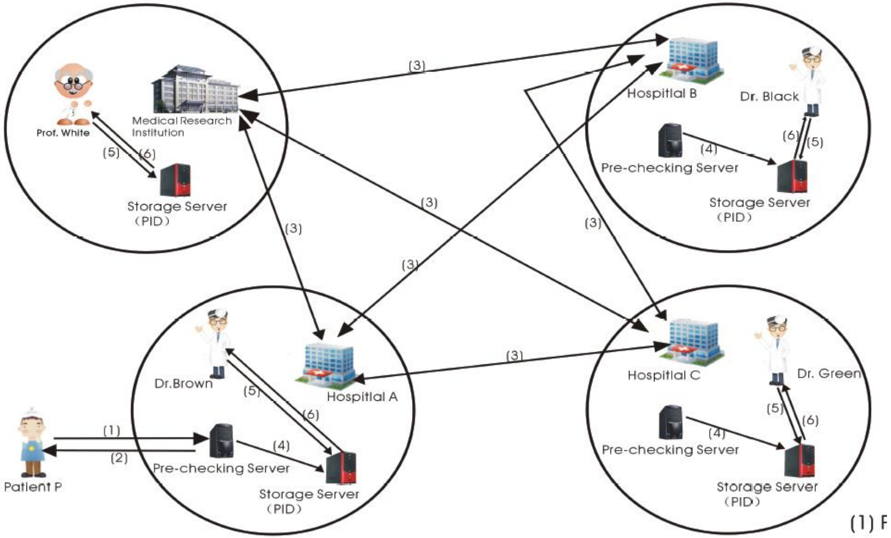
Solution Description

- The basic e-healthcare system illustrated in Fig. 2 mainly consists of three components:
  - Body Area Networks(BANs)
  - Wireless transmission networks
  - The healthcare providers equipped with their own cloud servers



Solution Description

- Distributed m-healthcare cloud computing systems
- All the personal health information can be shared among patients suffering from the same disease for <u>mutual support</u> or among the authorized physicians in distributed healthcare providers and medical research institutions for <u>medical consultation</u>

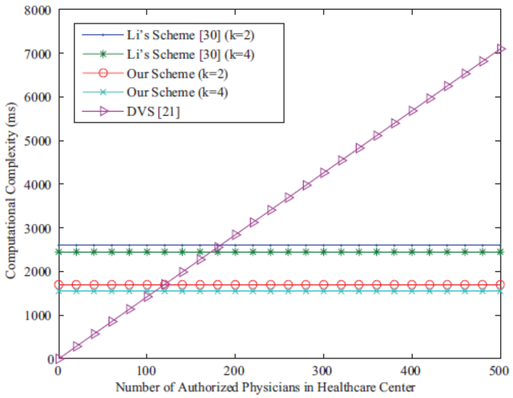


Solution Description

- Anonymity level of our proposed construction is significantly enhanced by associating it to the underlying GBDH problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed
- Every physician has a key constructed with respect to its attributes, in contrast to using a public key for entire physicians (Whom ever can access the key, also has access to data)
- As a result, the authorized physicians whose attribute set satisfies the access policy can recover the PHI

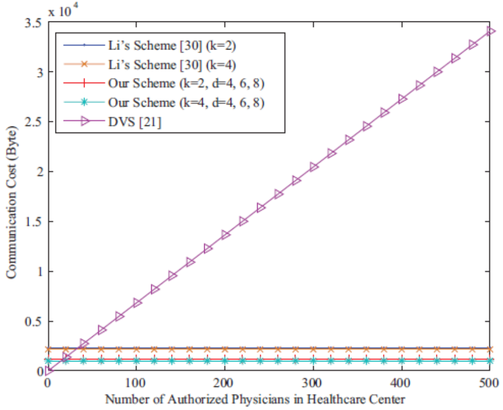
Performance Analysis

- Efficiency of PSMPA in terms of storage overhead, computational complexity and communication cost



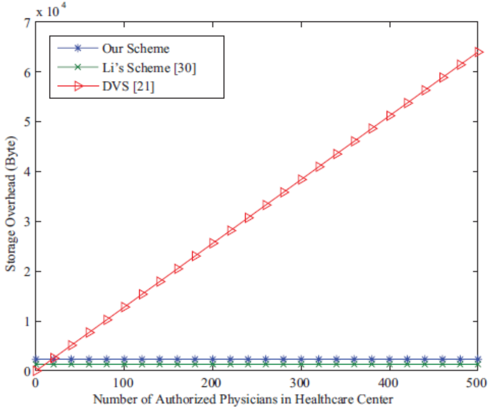
Comparison of

Computational Overhead



Comparison of

Communication Overhead



Comparison of

Storage Overhead

Conclusion

- In this paper:
    - Authorized accessible privacy model (AAPM)
    - Patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA)
    - Formal security proof
    - Efficiency evaluations

References

[1]: J. Zhou, X. Lin, X. Dong and Z. Cao, "*PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System*," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 6, pp. 1693-1703, 1 June 2015, doi: 10.1109/TPDS.2014.2314119.

[2]: L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L.M. Ni and J. Ma, *Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps*, IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.

References

[3]: J. Misic and V. Misic, *Enforcing patient privacy in healthcare WSNs through key distribution algorithms*, Wiley InterScience Security and Communication Networks Journal, Special Issue on Clinical Information Systems (CIS) Security, 1(5):.417-429 , 2008.

[4]: J. Misic and V. B. Misic, *Implementation of security policy for clinical information systems over wireless sensor networks*, Ad Hoc Networks, vol.5, no.1, pp.134-144, Jan 2007.