



सत्यमेव जयते

Ministry of Electronics and Information Technology
Government of India

BEST TECHNICAL POSTER AWARD



GCCS 2017

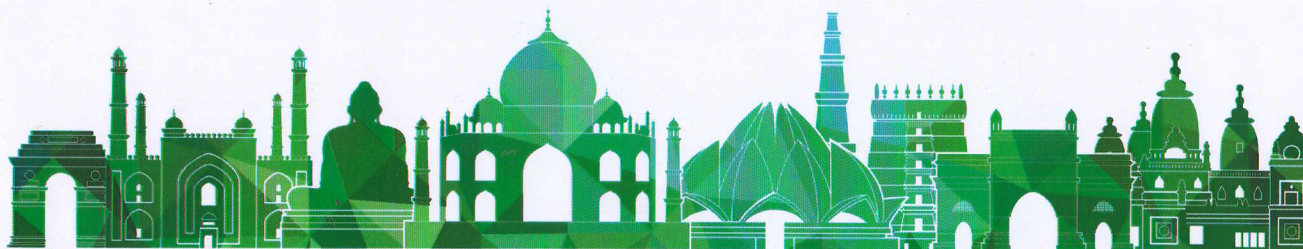
GLOBAL CONFERENCE ON CYBERSPACE, NEW DELHI, INDIA

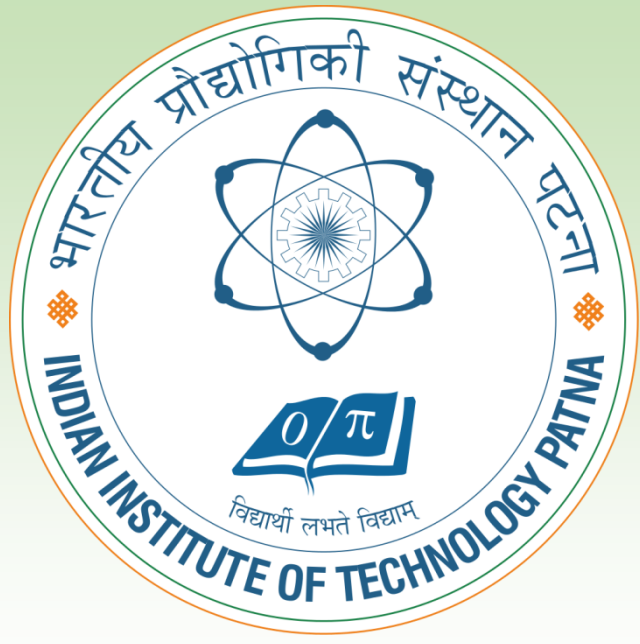
This is to certify that

SANJEET KUMAR NAYAK
INDIAN INSTITUTE OF TECHNOLOGY PATNA

Has been awarded **1st Best Technical Poster Award** for the poster titled "**On Solving Data Possession Issues in Cloud based Electronic Health Record System**" with co-author/s **Somanath Tripathy, Indian Institute of Technology Patna**, presented in the Global Conference on Cyber Space (GCCS), held on November 23-24, 2017 at New Delhi

Sanjeev Gupta IAS.
President & CEO,
Digital India Corporation
(Additional Secretary to the
Government of India)





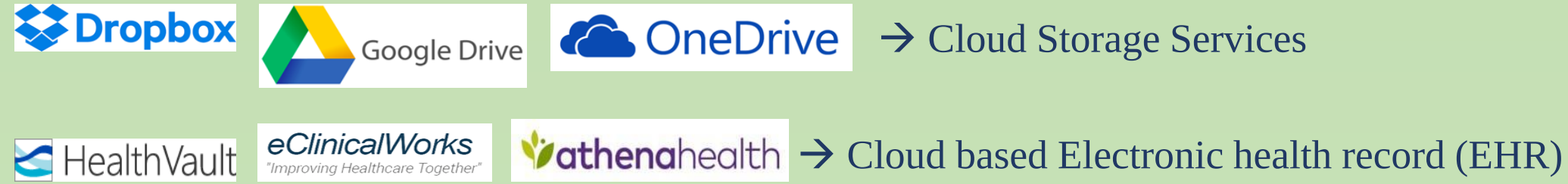
On Solving Data Possession Issues in Cloud based Electronic Health Record System

Sanjeet Kumar Nayak (Supervisor: Dr. Somanath Tripathy)

PhD Scholar, Department of CSE, IIT Patna, India

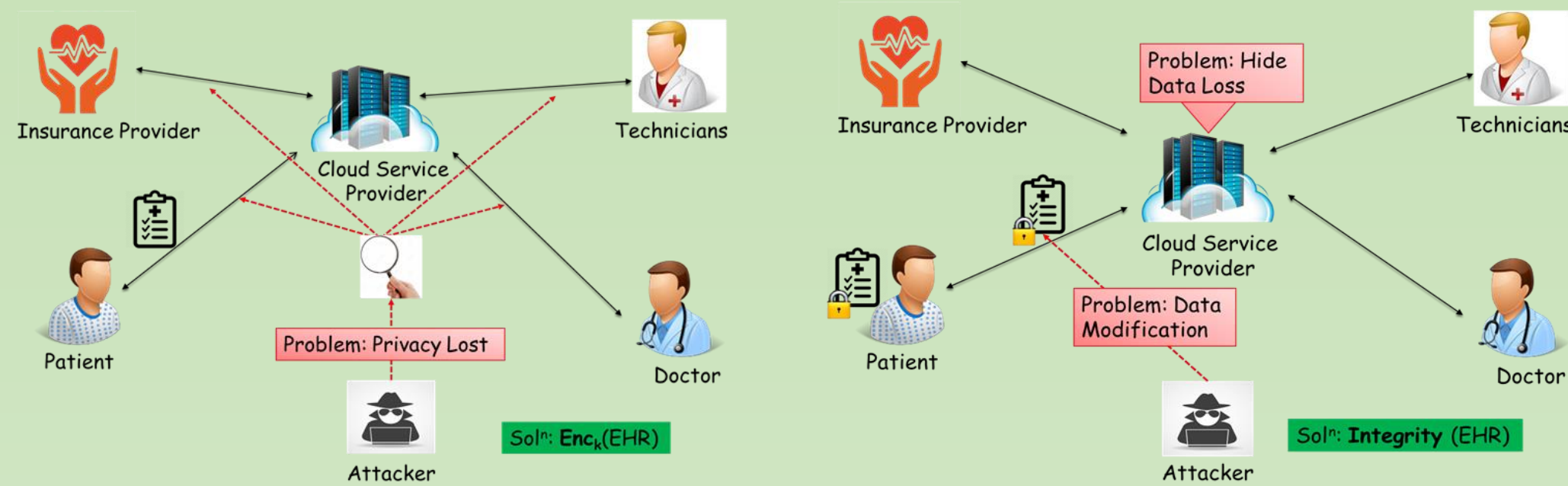
Email: sanjeet.pcs13@iitp.ac.in

INTRODUCTION



Major benefits of EHR

1. Up-to-date and complete information
2. Less medical errors
3. Reliable prescription



How to efficiently verify the correctness of outsourced data?

- Simply downloading the EHR data and verifying is not practical

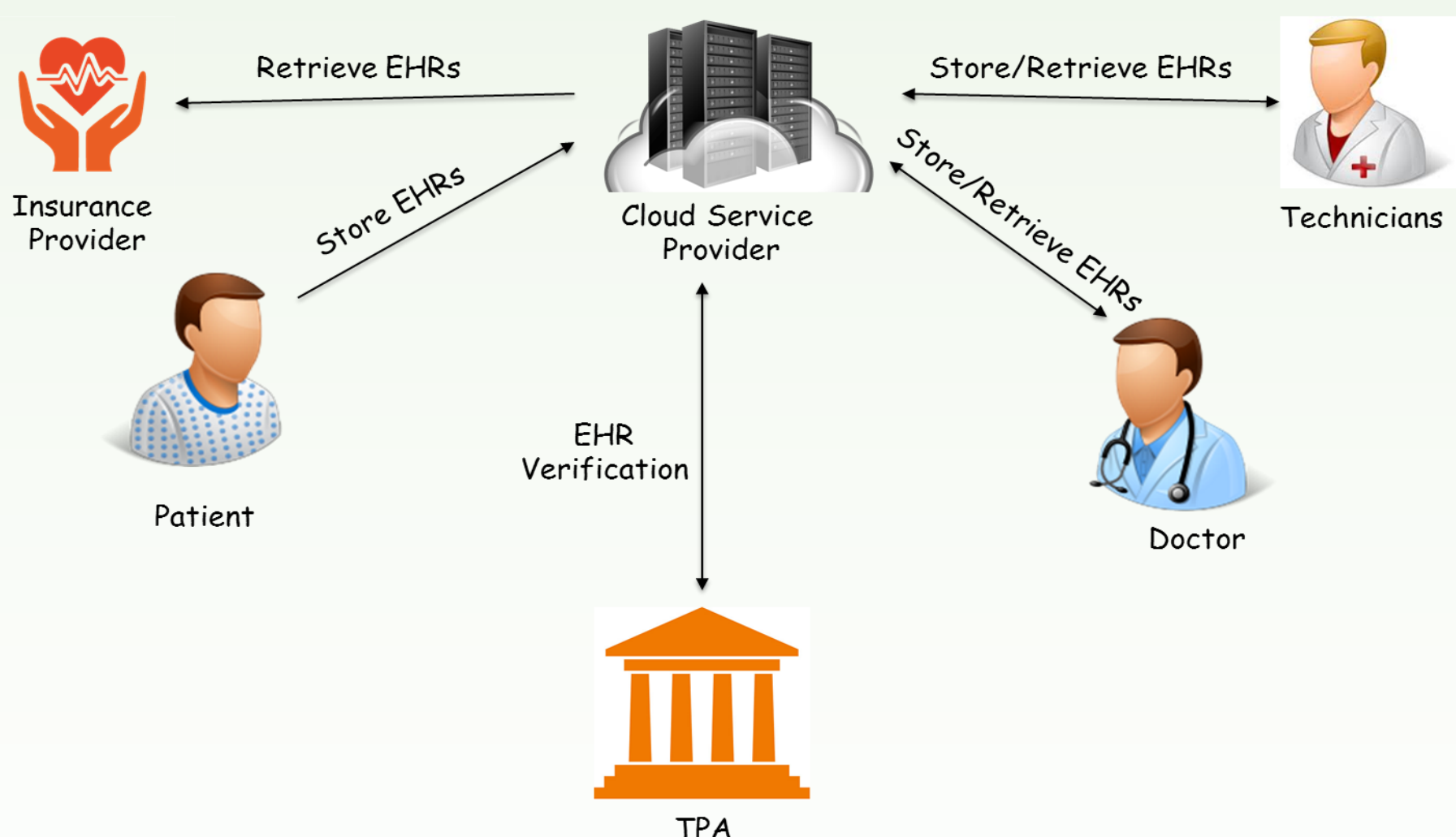
LITERATURE REVIEW

Schemes	Blockless Verification	Public Auditability	Privacy Preserving	Data Dynamics	Batch Auditing	Lightweight Verification
Shacham et al. Scheme – 1 [2]	Yes	No	No	No	No	No
Shacham et al. Scheme – 2 [2]	Yes	Yes	No	No	No	No
Wang et al. Scheme [4]	Yes	Yes	Yes	No	Yes	No
Zhu et al. Scheme [3]	Yes	Yes	Yes	Yes	No	No
Wang et al. Scheme [4]	Yes	Yes	Yes	Yes	Yes	No
Yang et al. Scheme [5]	Yes	Yes	Yes	Yes	Yes	No

MOTIVATION

- Verification consist of time consuming pairing operations
- Not suitable for performing verification in mobile devices
- Can we verify without pairing operation? (Lightweight Verification)

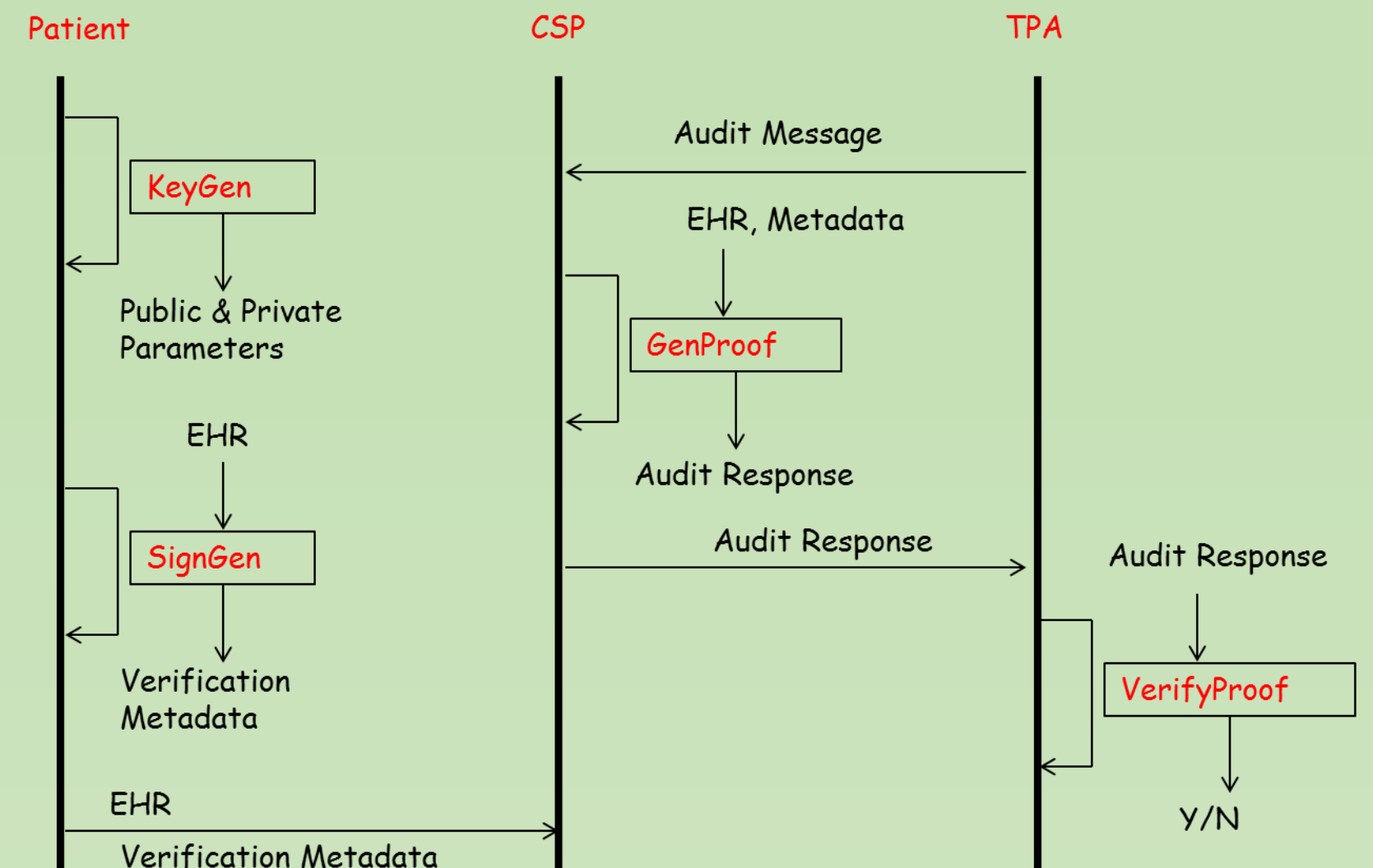
SYSTEM MODEL



SELECTED REFERENCES

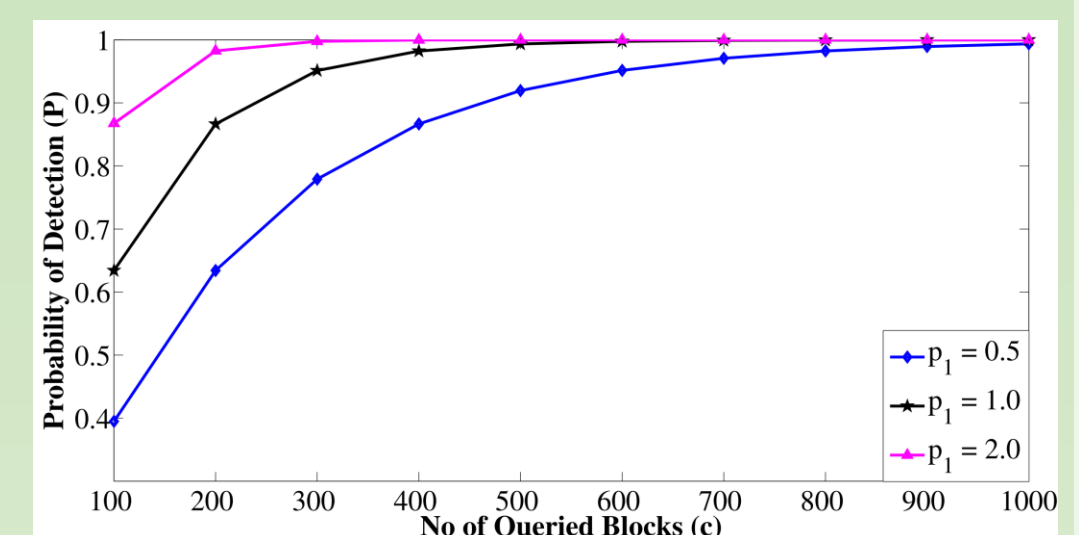
- [1] S. K. Nayak and S. Tripathy, "Privacy Preserving Provable Data Possession for Cloud Based Electronic Health Record System," In Proceedings of 15th IEEE TrustCom-16, Pages: 860-867, 2016.
- [2] H. Shacham and B. Waters, "Compact proofs of retrievability," In Proc. of 14th ASIACRYPT, Pages: 90-107, 2008.
- [3] Y. Zhu, H. Hu, G. J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Transactions on Parallel and Distributed Systems, 23(12), Pages: 2231-2244, 2012.
- [4] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, 62(2), Pages: 362-375, 2013.
- [5] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, 24(9), Pages: 1717-1726, 2013.
- [6] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," IEEE Transactions on Mobile Computing, 13(9), Pages: 1927-1941, 2014.

PROPOSED SCHEME – OVERVIEW



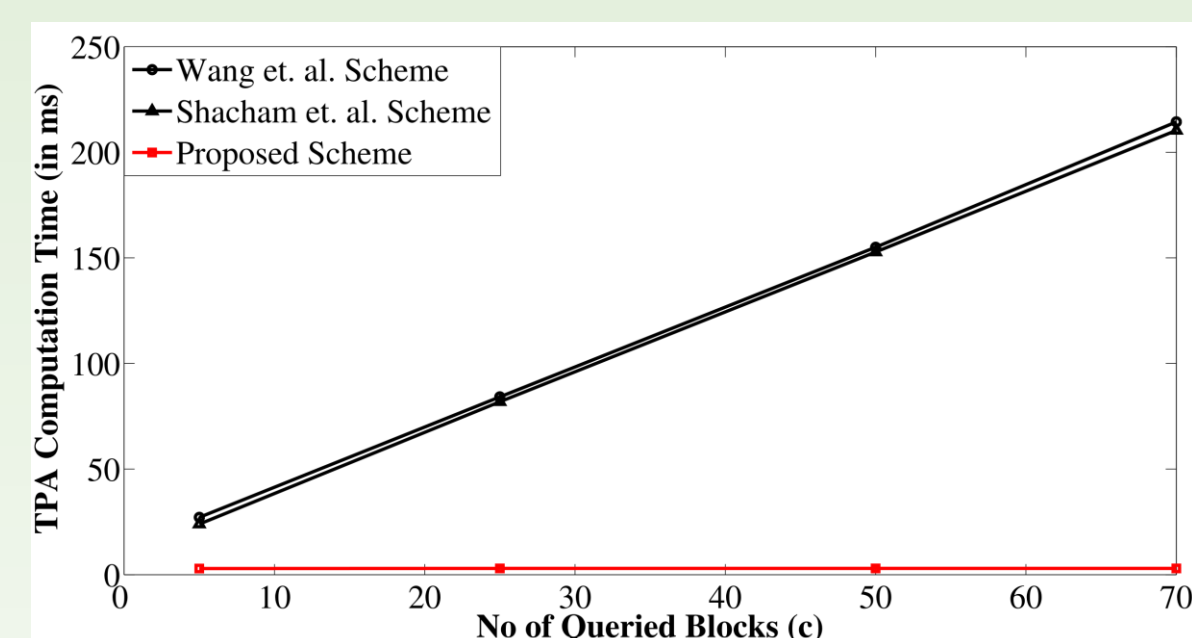
SECURITY ANALYSIS

- Storage Correctness
- Blockless Verification
- Unforgeability
- Privacy Preserving
- Misbehavior detection



COMPUTATION COST COMPARISON

Schemes	Overall Computation Cost
Shacham et al. Scheme [2]	$2T_p + (2n+2c+2)T_e + (n+3c-1)T_m + (n+c)T_h$
Zhu et al. Scheme [3]	$4T_p + (2n+2c+6)T_e + (2n+4c-1)T_m + (n+c+2)T_h$
Wang et al. Scheme [4]	$2T_p + (2n+2c+5)T_e + (n+3c+1)T_m + (n+c+2)T_h$
Yang et al. Scheme [5]	$3T_p + (n+2c+6)T_e + 2cT_m + (n+c)T_h$
Proposed Scheme	$5T_e + (2n+3c+1)T_m + (n+c)T_h + T_i$



CONCLUSION & FUTURE WORK

- A privacy preserving provable data possession scheme for cloud storage based EHR is presented.
- The proposed scheme provides lower computation overhead for the TPA as compared to the other existing schemes.
- Applications
 - Audit network log
 - financial banking data
- Future Work
 - Extend the proposed scheme, where multiple stakeholder of the cloud based EHR are present considering access control for each one of them.
 - Further, we also need to study the behaviour of batch auditing and data dynamics requirement