Certificate Presentation Deck

A Multi-Factor Access Control & Ownership Transfer Framework

Future Generation Healthcare Systems

Presented by Dr. Anubha Parashar
4th International Conference on Opportunities and Challenges in Business Management (OCBM 2020)
Manipal Academy of Higher Education, Dubai • 25–26 February 2020


MIU MANIPAL INTERNATIONAL UNIVERSITY
MANIPAL ACADEMY of HIGHER EDUCATION DUBAI CAMPUS
MANIPAL INSTITUTE OF MANAGEMENT MANIPAL

Certificate of Presentation

This is to certify that Dr. Anubha Parashar presented on

A Multi-Factor Access control and ownership transfer Framework for future Generation Healthcare systems.

at

the 4th International Conference On "Opportunities and Challenges in Business Management" (OCBM 2020)

25th & 26th February 2020

Organized by The School of Business, Manipal Academy of Higher Education (MAHE)-Dubai

Dr S V Kota Reddy
Academic President

Dr Jason Fitzsimmons
Chairperson, School of Business

Healthcare IoT | Edge Computing | Access Control

Paper at a glance

Securing connected healthcare where devices, users, and data constantly move.

The work proposes a lightweight, multi-factor framework for IoMT environments that combines access control, authentication, key exchange, and ownership transfer.

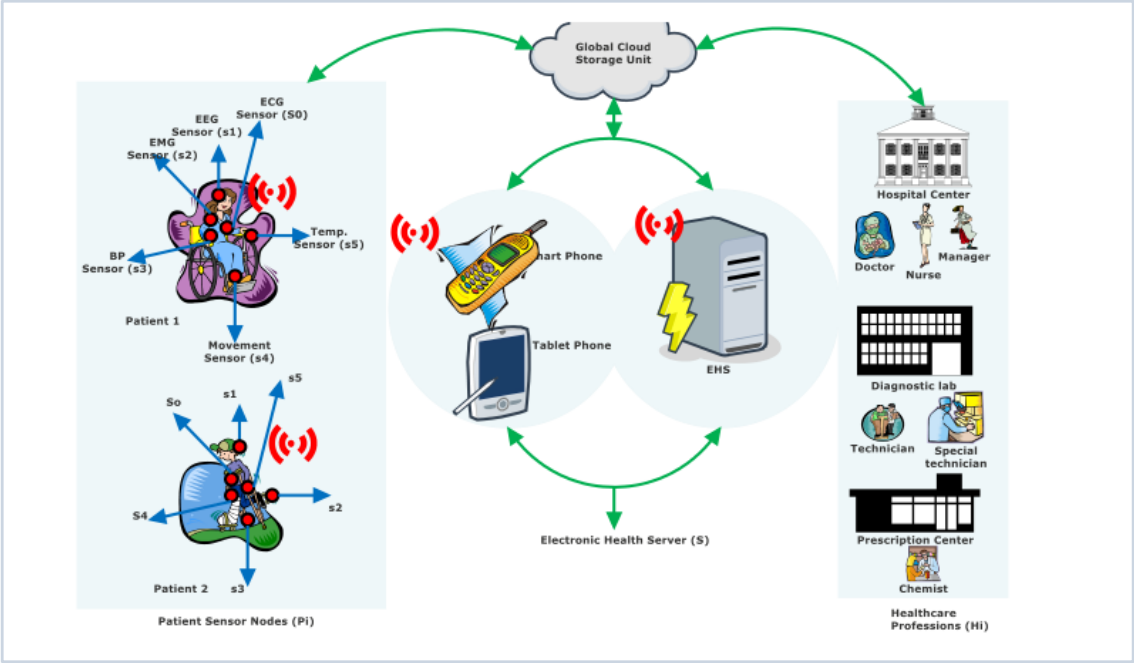
Core contribution

A protocol that lets authorized healthcare users transfer/revoke access rights while preserving patient privacy and system resilience.

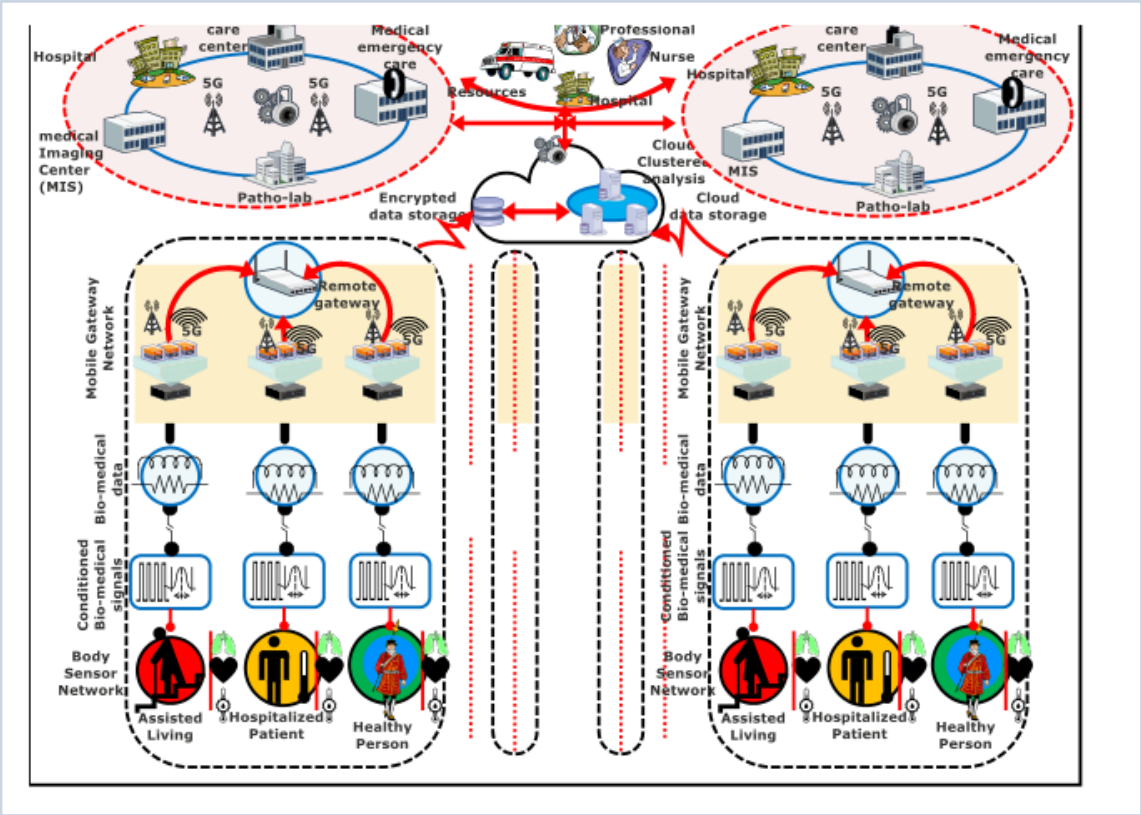
3
system entities
Patient • Professional • EHS

4
protocol phases
E • S • AKE • OTP

5+
attack classes formally/informally assessed



Why healthcare IoT needs stronger access control



IoMT creates value—but also expands the attack surface.

- Body sensors continuously send biomedical signals through wireless gateways.
- Edge computing reduces latency and supports real-time clinical decisions.
- Cloud/EHS storage centralizes data but increases privacy and authorization risk.
- Healthcare users need controlled, auditable, and revocable access rights.

Design goal: secure access without overloading resource-constrained sensors

Threat model and motivation

The model targets failures common in wireless, cloud-connected care.

01

Wireless exposure

Sensitive biomedical packets travel across vulnerable channels and gateways.

02

Credential theft

RFID/smart card data and password guesses are realistic attacker paths.

03

Data manipulation

Captured traffic can be edited, deleted, replayed, or used for traceability.

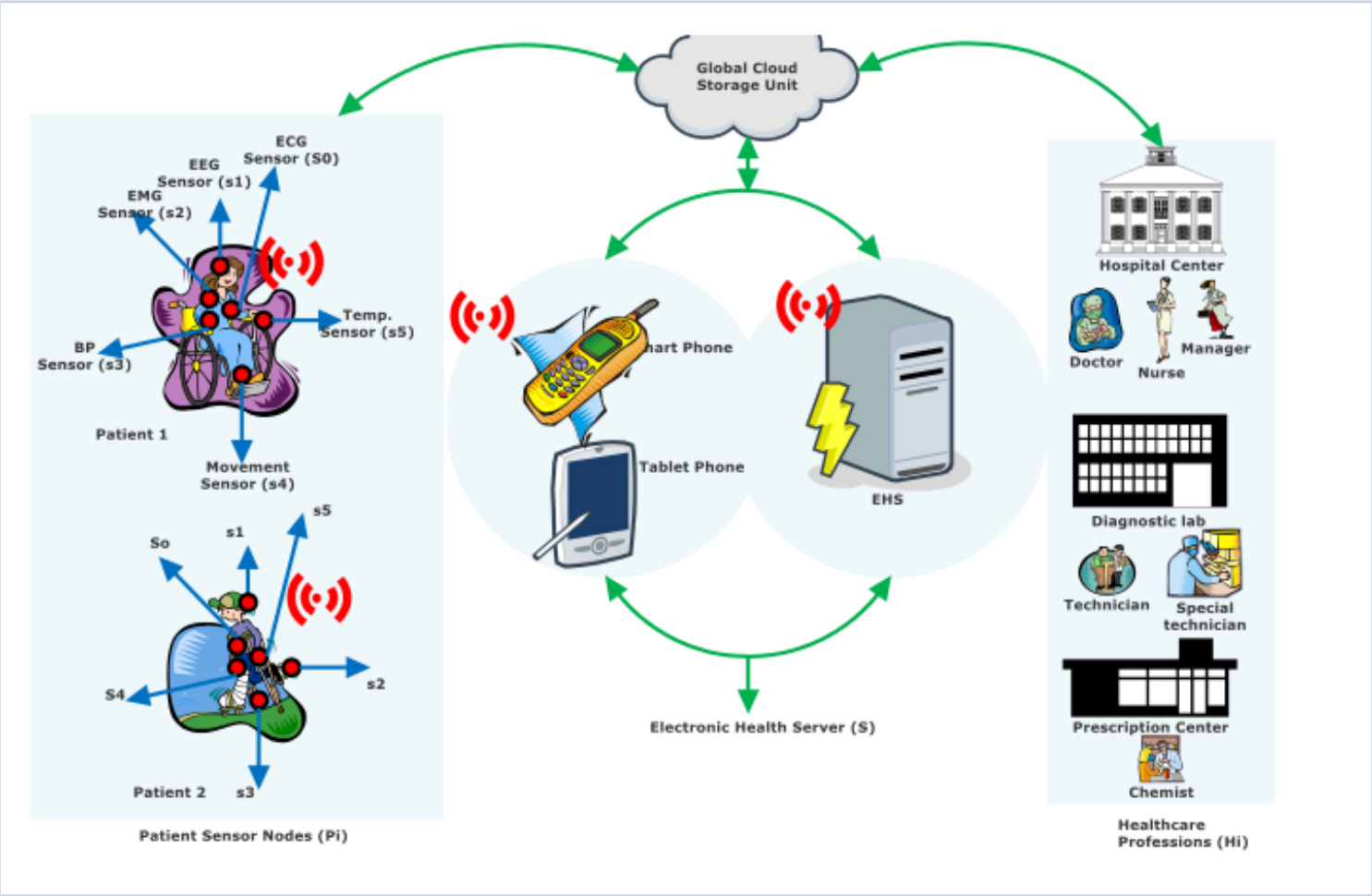
04

Emergency access

Break-glass access must work quickly without permanently weakening policy.

Motivation: combine authentication + access rights + ownership transfer in one lightweight protocol

Proposed architecture



Three entities coordinate access securely.

Patient entity (Pi)

Healthcare sensor nodes attached to the patient capture physiological data.

Healthcare professional (Hi)

Doctors, nurses, lab technicians, chemists, and staff registered through smart radio cards.

Electronic health server (Si)

EHS, gateways, and cloud infrastructure enforce policy, keying, and data availability.

Protocol flow

Access is granted through a staged, policy-aware flow.

1 → 2 → 3 → 4

Enrollment (E)

User ID + credentials + biometric data are bound to the smart card and EHS registration.

Sign-In (S)

The user inserts the card, enters credentials, and supplies biometrics for matching.

Authentication & Key Exchange (AKE)

Timestamps and computed messages verify legitimacy; a shared secret/session key is established.

Ownership Transfer (OTP)

Access rights move to a new legitimate user; old access is revoked but can be restored later.

Outcome: only verified users reach allocated EHS data segments, and rights can change safely over time

UNIQUE FEATURE

Ownership transfer and break-glass access

The framework supports real-world clinical handoffs.

In healthcare, access is not static. Doctors change, emergencies occur, and patient data must remain protected during every transition.

Normal route

Registered professional authenticates with card + password + biometric match before accessing allocated data.

Emergency route

Break-glass access bypasses regular phases only for immediate response scenarios, preserving auditability.

OTP transfer

H_2 supplies credentials and biometrics. EHS validates the new owner and sends H_1 deregistration notification.

Revocation support

The previous user's details remain stored for future revocation/restoration without exposing current owner privacy.

Requirements translated into design choices

The protocol is evaluated through three requirement families.

Functional	Security	Privacy
Access control	**Policy-based authentication**	**Entity privacy**
Energy optimization	Data confidentiality	User non-traceability
Break-glass access	Information integrity	Old owner privacy
Ownership transfer	Data availability	New owner privacy

Design principle: minimize sensor burden while preserving data ownership, access traceability, and patient confidentiality

Security analysis highlights

The framework is designed to resist common IoT attack paths.

✓ Stolen card attack

Smart card alone is insufficient without user ID, password, and biometrics.

✓ Offline password guessing

Critical parameters are additionally protected by biometric details.

✓ Insider attack

Policy-based server checks and cryptographic validation reduce unauthorized access.

✓ DDoS + traceability

Formal/informal analysis targets availability and user non-traceability.

Security message: multi-factor credentials + timestamp checks + hash-based protection strengthen access control in IoMT

Presentation certified at OCBM 2020

4th International Conference on “Opportunities and Challenges in Business Management”
Manipal Academy of Higher Education, Dubai

MIU MANIPAL INTERNATIONAL UNIVERSITY

MANIPAL ACADEMY of HIGHER EDUCATION DUBAI CAMPUS

MANIPAL INSTITUTE OF MANAGEMENT MANIPAL

Certificate of Presentation

This is to certify that Dr. Anubha Parashar *presented on*

A Multi-Factor Acess control and ownership transfer Framework for future Generation Healthcare systems.

at

the 4th International Conference On “Opportunities and Challenges in Business Management” (OCBM 2020)

25th & 26th February 2020

Organized by The School of Business, Manipal Academy of Higher Education (MAHE)-Dubai

Dr S V Kota Reddy
Academic President

Dr Jason Fitzsimmons
Chairperson, School of Business

Key takeaway

- Connected healthcare requires stronger identity and access governance.
- Edge-enabled IoMT systems must balance latency, privacy, and energy limits.
- Ownership transfer is a critical feature for clinical continuity.
- Multi-factor authentication improves resilience against practical threats.

Thank you