Development of an Advanced Digital Medical Platform to monitor and manage diseases within populations: legal and ethical issues

Dr. Glenford Mapp
Associate Professor
Department of Computer Science
School of Science and Technology
Middlesex University

Outline of This Talk

- Motivation
- The New Framework for Cloud Storage
- The Capability System
- Tele-Health Project
- The Advanced Digital Medical Platform
- Conclusions
- Questions

Motivation – The Age of Big Data

- Cloud Computing will be defined as computing in the age of Big Data
- Big Data will be driven by new networks such as social networks, sensor networks and eHealth systems
- Cloud Storage, Data Management and Control will be key issues

Benefits of Big Data

- The Cloud Platform is very efficient
  - Better use of computing resources (60-80%)
    - Computation may happen in parallel
    - Computation may happen in different locations
- Aggregate and analyse large amounts of data in real-time or close to real-time
  - Potential to provide new insights and treatments
- Large interconnection networks allow data to be moved at high speeds between clouds.

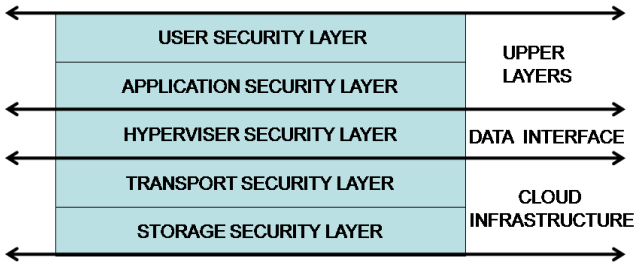
Challenges of Big Data

- Large Data Movement
  - Must move data to and from compute engines
  - Compute Engines may be anywhere
  - Data may need to flow across International Boundaries
- Cloud Infrastructure managers must be able to maximize infrastructure
  - must be able to move, replicate , or cache data without compromising the security of that data
- eHealth Data is so large that we will have to use Public Clouds

Legal and Ethical Issues for managing and storing eHealth data

- Who is responsible for your data in the Cloud
  - Is it you
  - Is it The Cloud Provider
  - Is it both
- Who can manage your data in the Cloud
- Who can use the data
  - What about data for medical research
  - What restrictions should be placed on how Big Data is used in medical research
  - Who benefits from the development of new treatments from Big Data techniques
- Need a new technological and legal/ethical framework

The New Cloud Storage Framework



User Security Layer

- Users will have to identify themselves first to the device.
- Users might have to identify themselves to an application or might need to show some sort of authorization to use the application as well as some QoS parameters agreed between the application or service and user via an SLA

Application Security Layer

- This layer needs to ensure that the application can run on Cloud Infrastructure.
  - So the Application needs register when it is installed on a machine
  - Going in this direction for mobile phones
- Provides data integrity for the user and the application
  - Encode and decode data blocks stored in the Cloud

Hypervisor-Layer Security

- This layer provides the bridge between the Upper Layers (User and Application) and the Lower Layers (Transport and Storage).
- Hypervisor must first authenticate itself to the Cloud Infrastructure and then check that applications running on it are authorized to access the relevant resources.

Transport Layer Security

- Responsible for moving data within the Cloud and between Applications and the Cloud Infrastructure
- Ensuring secure communication between any two endpoints
- Must ensure that no transport connection is made between unauthorized entities.
- All connections must be made through this layer

Storage Security Layer

- Ensures that whether data is replicated, migrated or copied, security is not compromised.
  - This layer cannot decode the contents of a block if encoded by the application.
- If there is more than one copy of the block; it uses distributed caching algorithms to make sure that blocks are kept synchronized.
  - Finer granularity than Google File System

The design of the Capability System

- Everything (including people) in the system must be represented by a capability
- Capability should include not just the object but which server administers the object
- Should be possible to narrow capabilities
  - Proxy capabilities
- Should be able to revoke capabilities
- Should prevent casual tampering

Capability Fields

TYPE	PROPERTY FIELD	OBJECT ID	RANDOM BIT FIELD	HASH FIELD

TYPE = 8 BITS

PROPERTY FIELD = 12 bits

OBJECT _ID = 72 bits

RANDOM BIT FIELD = 24 bits

HASH FIELD = 12 bits

More Detailed Capability Fields

PROPERTY FIELD

P	M	C	OBJECT SPECIFIC PROPERTIES

P = PRIVATE CAPABILITY

M = MASTER : ORIGINAL CAPABILITY

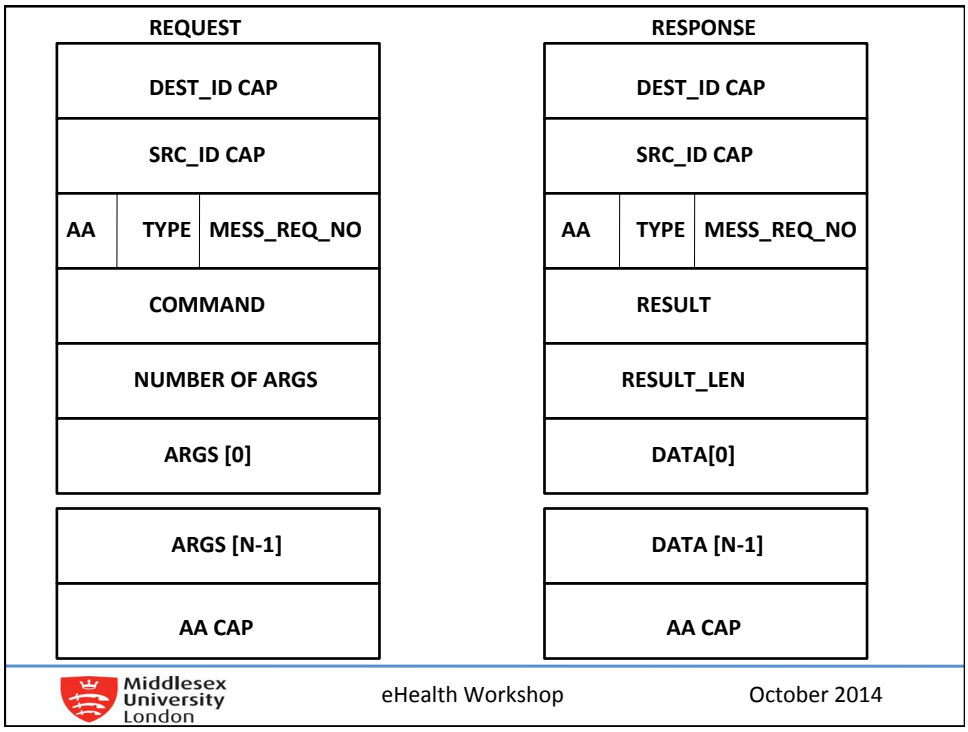
C = CHANGE : CAN NARROW

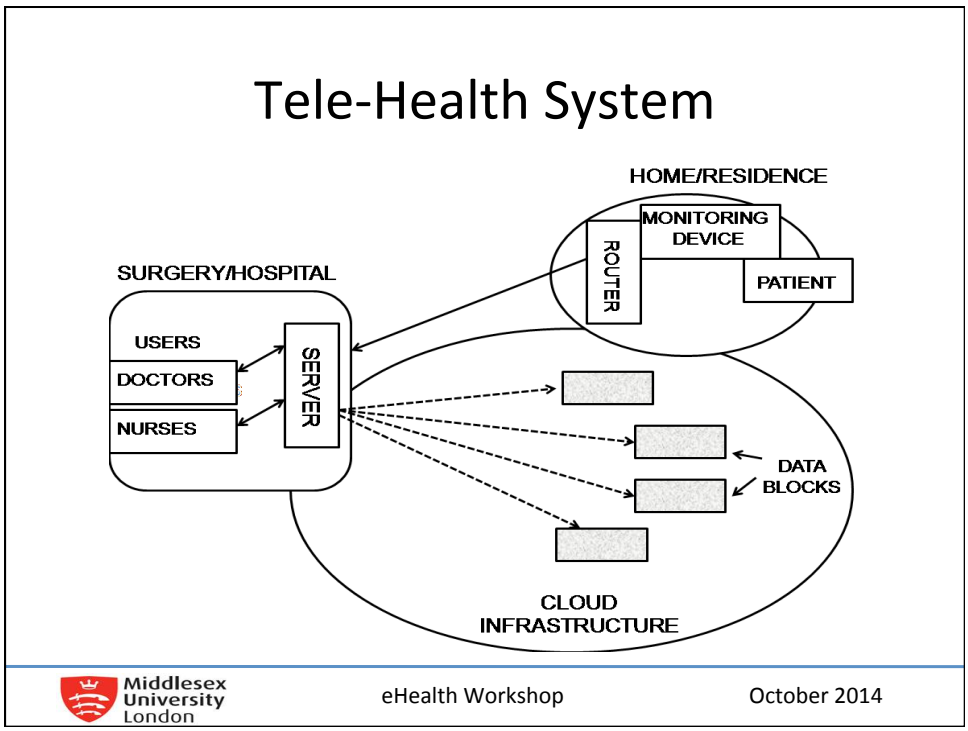
OBJECT_ID FIELD

IP ADDRESS	UNIQUE OBJECT NO

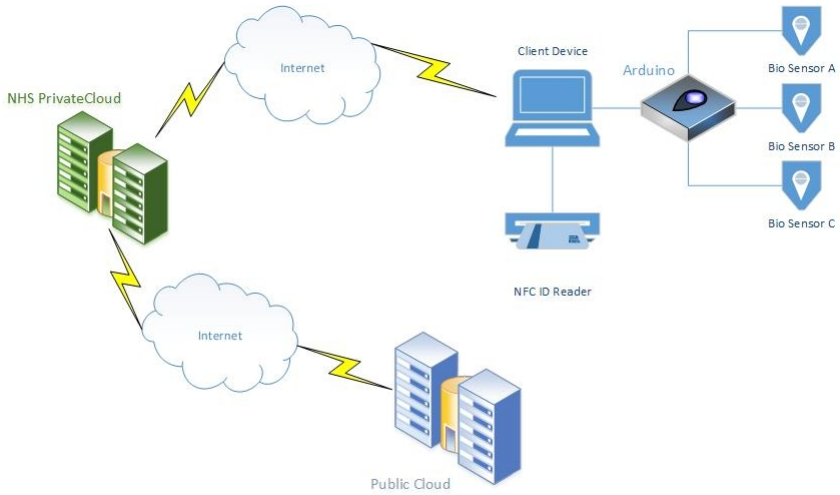
Rules about Capabilities

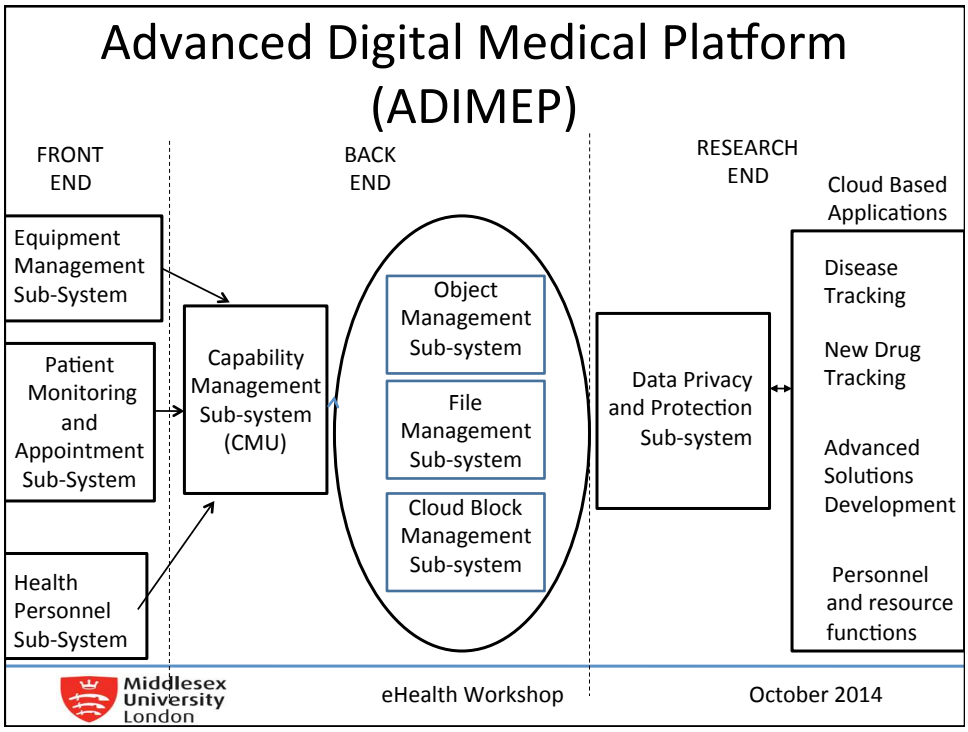
- If the Change bit is set; Proxy capabilities can be derived from Master capabilities
- Proxy capabilities have a new Random Bit Field and new Hash Bit Field
- Cannot derive Proxy capabilities from other Proxy capabilities
- Capabilities are revoked by changing the Random Bit Field and re-computing a new Hash Bit Field value


REQUEST
DEST_ID CAP
SRC_ID CAP
AA
TYPE
MESS_REQ_NO
COMMAND
NUMBER OF ARGS
ARGS [0]
ARGS [N-1]
AA CAP
RESPONSE
DEST_ID CAP
SRC_ID CAP
AA
TYPE
MESS_REQ_NO
RESULT
RESULT_LEN
DATA[0]
DATA [N-1]
AA CAP
Middlesex University London
eHealth Workshop
October 2014


Tele-Health System
HOME/RESIDENCE
MONITORING DEVICE
ROUTER
PATIENT
SURGERY/HOSPITAL
USERS
DOCTORS
NURSES
SERVER
DATA BLOCKS
CLOUD INFRASTRUCTURE
Middlesex University London
eHealth Workshop
October 2014

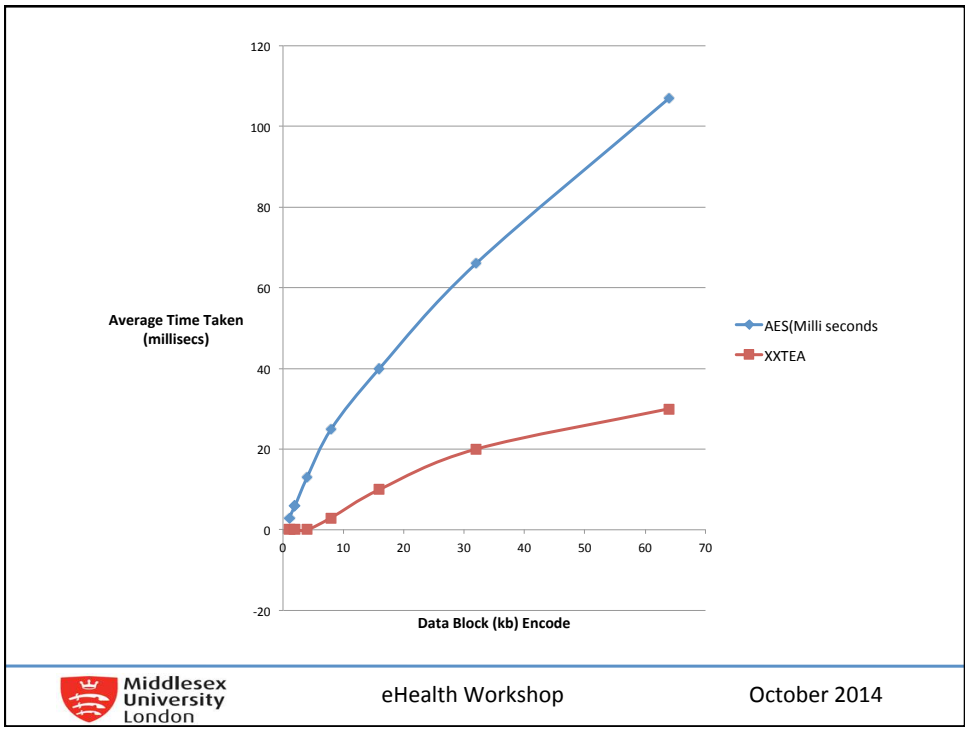
The Components of the System

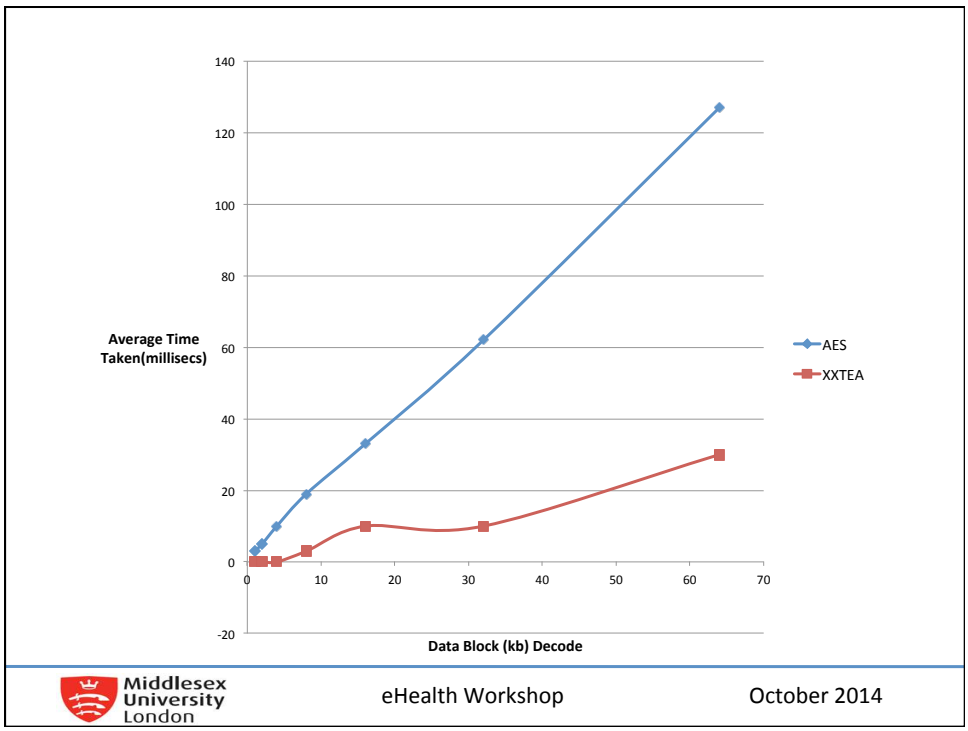




Current Work – Transport Security and Storage Security

- Transport security
  - Providing security for communications
  - Need to be secure
  - Need to be fast
  - XXTEA – medium level security but fast
  - Administered by Cloud Provider?
- Storage security
  - Storage of Individual blocks
  - Needs to be very secure
  - Does not need to be fast as blocks are encrypted when stored; only decrypted when used
  - AES – US Government Security Standard
  - Administered by the User?


120
100
80
60
40
20
0
-20
0
10
20
30
40
50
60
70
Average Time Taken (millisecs)
Data Block (kb) Encode
AES(Milli seconds
XXTEA
Middlesex University London
eHealth Workshop
October 2014


140
120
100
80
60
40
20
0
-20
0
10
20
30
40
50
60
70
Average Time Taken(millisecs)
Data Block (kb) Decode
AES
XXTEA
Middlesex University London
eHealth Workshop
October 2014

Conclusions

- Currently trying to build a small prototype
  - Working with Malcolm Clarke from Brunel
- Working on Data Privacy and Protection Subsytem.
  - Defining the concepts of virtual subsets
  - Looking to work with others
- Need a Legal and ethical framework to address new realities of eHealth and Cloud

Thanks for Listening

QUESTIONS ?