IMPLEMENTING CROSS-ENTERPRISE DOCUMENT SHARING (XDS) BASED ON BLOCKCHAIN TECHNOLOGY

PETNATHEAN JULLED

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(CYBER SECURITY AND INFORMATION ASSURANCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2019**

Thesis
entitled

IMPLEMENTING CROSS-ENTERPRISE DOCUMENT SHARING (XDS) BASED ON BLOCKCHAIN TECHNOLOGY

…….....
Mr. Petnathean Julled,
Candidate

…….....
Assadarat Khurat,
Dr. –Ing. (Computer Security)
Major advisor

…….....
Pattanasak Mongkolwat,

Co-advisor

…….....
Asst. Prof. Thitinan Tantidham,
Dr.rer.nat. (Computer Science)
Co-advisor

…….....
Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

…….....
Assoc. Prof. Vasaka Visoottiviseth,
Ph.D. (Computer Engineering)
Program Director
Master of Science Program in Cyber Security and Information Assurance
Faculty of Information and Communication Technology
Mahidol University

IMPLEMENTING CROSS-ENTERPRISE DOCUMENT SHARING (XDS) BASED ON BLOCKCHAIN TECHNOLOGY

PETNATHEAN JULLED 5936474

M.Sc. (CYBER SECURITY AND INFORMATION ASSURANCE)

THESIS ADVISORY COMMITTEE: ASSADARAT KHURAT, Ph.D.,
PATTANASAK MONGKOLWAT, Ph.D., THITINAN TANTIDHAM, Ph.D.

ABSTRACT

On the increasing demand for better quality of healthcare service, there is the topic that involve healthcare information technology in term of operation efficiency. Healthcare information sharing and interoperability between healthcare organizations is one of major solution to improve healthcare service quality. But, there still many challenge inhibit the solution to become reality. There found initiatives to standardize healthcare information sharing method. To address issue about health document sharing between different enterprises, Integrating Healthcare Enterprise (IHE) initiative have proposed Cross-Enterprise Document Sharing (XDS.b) Profile. The profile allow the adopted organizations to share health document between each other simultaneously.

As well as other industry, there also emerging cyber-security threats threatening healthcare information domain. These threats increase difficulty to development of health information sharing network and causing damage to healthcare enterprises. These cyber-threats can cause damage to the industry in many aspect, especially those cyber-attack that targeting integrity and availability of data. These kind of cyber-attack can severe the continuity of medical operation which potentially can result as the cost of patient's life. There are many solutions technology proposed to deal with these kind of cyber-attacks. One of the technology that on the trend to deal with cyber-threats threatening integrity and availability of data is Blockchain technology.

There are several researches and concepts that proposed about using Blockchain technology to solve health information sharing issue. But there still many limits prevent Blockchain technology to effectively integrated with data like health information. In this work, we propose another approach for integrate Blockchain technology with health information. We see that standard like IHE XDS.b profile could be use with Blockchain technology to allow health document sharing through decentralized network while address cyber-security issue through unique characteristics of Blockchain technology.

KEY WORDS: HEALTH INFORMATION / INTEROPERABILITY / INFORMATION SHARING / INFORMATION SECURITY / BLOCKCHAIN / SMART CONTRACT / IHE / XDS

40 pages

CONTENTS

CHAPTER I
INTRODUCTION

On the increasing demand for better quality of healthcare service, there is the topic that involve healthcare information technology in term of operation efficiency. Healthcare information sharing and interoperability between healthcare organizations is one of major solution to improve healthcare service quality. Patient's health document data are scattered across different healthcare organizations, due to the foundation of healthcare informatics are separately developed by different organizations. Each healthcare organizations have their own method to process and handle healthcare information. This make it hard for one healthcare information to interoperate with other. To enable health information sharing from just one organization with one another can cost much more than benefit they can gain. This even did not regard concern about business value. Sharing health information with not fully-trusted party exposing vulnerabilities to business model. The risk that benefit the organization gain from sharing their patient information with other may not sustain the risk and cost they need to take. This create high friction for one organization to share their information with others. It even more difficult for individual patient to integrate their healthcare between different providers. It revealed that these interoperation problem cause huge decrease in efficiency on healthcare operation and result as lower quality of healthcare service [1]–[8].

That why there are many initiative that start to standardize healthcare information technology with the goal to allow healthcare organization to be able to interoperate with each other. Integrating Healthcare Enterprise (IHE) is one of well-known initiative that provide materials for healthcare informatics standardization. IHE provide implementation framework and guideline for developing health informatics system. For health document sharing between different organizations, they provide Cross-Enterprise Document Sharing (XDS.b) profile. The profile act as guideline for system developer to implement their system to meet the requirement where the system can share health document with other organizations. This profile will be the main tool for this work, to deal with health information sharing problem.

1.1 Motivation

In the current age of information digitalization, cybersecurity has become an issue for many organizations and individual. Anyone can become a target of cyber-attacks. Amongst many kind of organization, healthcare industry is one of major target that become victim of cyber-attacks each year [9]. Followed by digitalization of hospital operation and information system, amount of cyber-attack and variation rise as the technology developed. These incidents variant from breached in personal health information to larger size of attack which can potentially halt hospital operation for a period of time. Halted in operation surely cause damage in various kinds. It may cost hospital for more than million, or even cost individuals' life as a result of the incident for the worst.

There are many kinds of incidents targeting healthcare industry. In recent years, one of major incidents found throughout the industry is hospital data breach. Data breach often appeared in a form that hospital data got compromised by hacker unnoticed by hospital employees. The compromised data can be valuable in dark market as it can be further used for various kind of more advanced attacks like identity theft, blackmailing, or social engineering, due to these data mostly included patients' personal information and their health condition. This kind of incident can potentially cost hospital 'a trust' from their customer if they showed a poor quality of incident mitigation, as individuals' safety and privacy are being put on the stake. Also, there are the case that not just gain unauthorized access to patient's private data but, take over the data or even wipe all important data out of existence. 'Ransomware' and 'Wipeware' are the main cause of these threats. Ransomware take over an ownership over data away from hospital system and encrypt all the data which often take an important roles on hospital operation. At the same time, Wipeware will delete all the data from the victim machine. This mostly cause great disruption on hospital operation as consequence. Incidents that showed up in recent years seem to target healthcare organization more frequently, as the industry still have poor cybersecurity practices [10]. Many incidents [10]–[12] showed that social engineering launched on healthcare employees are on risen. The threat have potential to seamlessly blend into hospital workflow and made it hard to be noticed. However, follow these incidents, many stakeholders in healthcare domain start to implement cyber-security to their organization infrastructure.

At the foundation, each organization must start with educating their employees on cyber-security awareness to reduce risk of cyber-incident that may cause by human error or human vulnerabilities. Next, define organization policy and management plan that help prepare against cyber-incident. When employees and management level of organization have prepared cyber-security, then, the organization will focus on cyber security of technology

layer. There are various kind of tools and technology that was invented to mitigate cyber-incidents. Some may have been made to prevent exploitation of existing technology while some may have been made to directly deal with known and upcoming threats.

One of many concept invented to mitigate these threats is decentralization of data. The concept of decentralization was made to mitigate most incident and threat that involve single-point of failure vulnerability. For the case of healthcare industry where loss of patient's data can cause many major damage to the affected organization and their patient, decentralization of data can help reduce damage caused by the case. There are more than one benefit that healthcare document data can gain from decentralization. Decentralization allow patient's data that scattered across healthcare domain in different organization to link to each other. As healthcare document data can scattered across different organization within healthcare industry, it also increase a chance that its copies can survive cyber-incidents. Even in case that document in one organization got compromised, there is a chance that copies of compromised data also exist in other organization. The survived copies can make substitute for the original that got compromised. However, this only possible if there are the point that let every organization in the network known which document exist in which organization. This is where the concept of IHE Cross-Enterprise Document Sharing Profile fit in. Combined with Blockchain technology that make the Document Registry entry persist and immutable, this ensure that every organization in the network will always know whereabouts of document they need within the network while the entry itself cannot be tempered or deleted by any actor with ill intention.

This work will introduce another way to allow health document sharing between healthcare organizations with increased protection against cyber-threats, by using combination of Blockchain and IHE Cross-Enterprise Document Sharing (XDS.b) Profile.

1.2 Problem statement

To allow sharing of healthcare document between different healthcare organizations which require maintain of its confidentiality while mitigate emerging cyber-threats on healthcare domain that tamper with integrity and availability of data, there need document registry that have distributed, decentralized, persistent, and immutable characteristics.

1.3 Objective

1.3.1 Design and implement Document Registry Blockchain that follow requirement for document registry defined in XDS.b integration profile from IHE.

1.3.2 Design and implement Blockchain smart contract that give main function to Document Registry Blockchain as healthcare document registry.

1.3.3 Design and implement Blockchain smart contract that give additional function to record healthcare document exchange between participate node.

1.3.4 Deploy and evaluate functionality of Document Registry Blockchain.

1.4 Scope of project

1.4.1 Design and implementation of Document Registry Blockchain that followed requirement defined in XDS.b integration profile from IHE.

1.4.2 Design and implementation of Blockchain smart contract within Document Registry Blockchain that give main function as healthcare document registry and additional function as healthcare document exchange history record.

CHAPTER II
LITERATURE REVIEWS

2.1 State of Cyber Security and Cyber Threats in Healthcare Domain

2.1.0 Digital transformation of healthcare

Transition from the age of paperwork, healthcare industry is now undergoing digital transformation. Efficiency and continuity is the main factors that driven healthcare industry to change. Paperwork start falling behind when the huge amount of data are produced by healthcare service operation from day to day. Health information undeniably becoming an important component on developing efficient healthcare service. [13]–[18]

2.1.1 Interoperability of healthcare information

One of major issue that are common amongst healthcare industry is the issue about interoperability between each unit of healthcare system. Especially, the interoperability between different organizations. Lack in interoperability, prevent many opportunities for healthcare service quality improvement. Patient may need to take extra repetitive care procedure when visit new hospital. Mistake in communication between different physicians can cause misdiagnosis. So, there are many demand from patient side that want their health journey to be connected together and allow improvement in healthcare service quality. However, interoperability is extremely difficult issue for each single organization to solve. The foundation of healthcare informatics was developed separately by each organizations. Each system have their own design and method to handle health information. That mean there still have open issue on how to solve interoperability in the field of healthcare. [1], [3]–[5]

2.1.2 Assets in healthcare domain and cyber-security risks

In order to define effective risk mitigation plan, the first step is to identifying key assets that require protection against cyber threats. In healthcare domain, the most critical asset is patients' health. Patients can be permanently or temporarily injured through direct actions such as launching attack to turn off critical active medical devices or indirect actions

aiming at disrupting care such as altering patient health records, compromising medical information systems, or cutting off power supply in operating room; can cause harmful consequence toward patients' health [9].

The next important asset in healthcare domain is patients' health record. This record mostly contains valuable information personally identifiable information (PII) included social security number, health care provider information, credit card information, name, address, date of birth, etc. Patients' health record also contains protected health information (PHI) which potentially included information about patients' physical or mental health condition, and etc. which can be used to identify the patient. This mean, Patients' health record can potentially be used for variety of harmful activities included identity theft, insurance fraud opportunities, social engineering, or even terrorism.

Availability of healthcare services is also a major asset in healthcare domain. There are two distinct categories: critical services and administrative services. The critical services ensure continuity of care including active/passive medical devices, medicine delivery systems, and surgery equipment. The disruption of these services may result as disaster of patients' health. The administrative services are services that keep efficiency of healthcare operation included work orders control, medicine management, financial transactions, and medical appointment. It is less critical if the system become unavailable for a short duration of downtime.

In some case, healthcare facilities can host research labs. Activities of research labs will involve intellectual property assets. For example, experimental procedures for surgery, test and studies results, test subject information or drug formulas. These kind of asset can be valuable amongst competitor parties which lead possibility of the assets to become cyber-attacks target. Researchers' contribution and money invested in the research can be wasted to nothing in the case of successful cyber-attacks. At the same time, alteration of these assets can lead to miserable consequences or even cause negative impact to patients' health during the research.

Eventually, as patient place their health and their lives in the hand of medical staff. They need to know that they can trust their care provider. Failing to secure the service against cyber-attacks can cause great negative impact to the reputation of the care provider if it disclosed to the public. It can even damage reputation and career of medical staff in the case of identity theft where identity of specific medical staff is used to perform the attack (such as impersonation, credential theft, etc.).

2.2 Integrating the Healthcare Enterprise (IHE) and IHE Profiles

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. This help enable seamless and secure access to health information that is usable whenever and wherever needed. IHE providing specifications, tools and services for interoperability. IHE also engages clinicians, health authorities, industry, and users to develop, test, and implement standards-based solutions to vital health information needs. [19] IHE initiative have purpose to provide convenient and reliable way of specifying a level of compliance to standards sufficient to achieve truly efficient interoperability.

2.2.1 IHE Process

IHE brings together users and developers of healthcare information technology (HIT) in an annually recurring four-step process [20]:

I. Clinical and technical experts define critical use cases for information sharing.
II. Technical experts create detailed specifications for communication among systems to address these use cases, selecting and optimizing established standards.
III. Industry implements these specifications called IHE Profiles in HIT systems.
IV. IHE tests vendors' systems at carefully planned and supervised events called *Connectathons*.

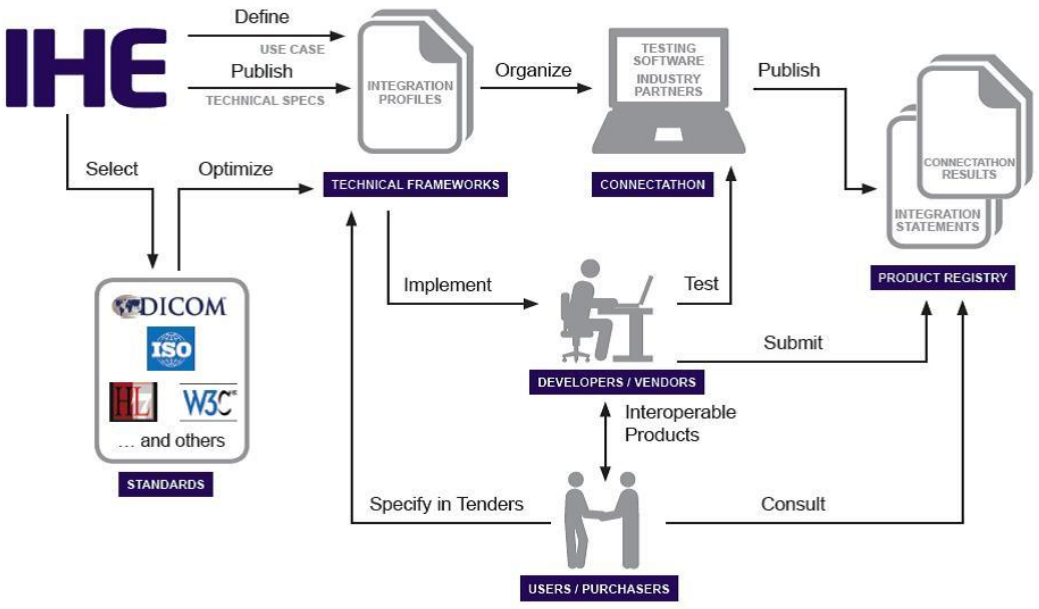

Figure 1 IHE Process to create guideline for implementation of health information technology [20]

The process ensure that the resulting IHE Profiles provide benefit for implementer and make it compatible with unique environment of healthcare industry.

2.2.2 IHE Profiles

IHE Profiles are set of specification and implementation guide that produced from IHE four-step process. IHE Profiles organize and leverage the integration capabilities that can be achieved by coordinated implementation of communication standards, such as DICOM, HL7 W3C and security standards. They provide precise definitions of how standards can be implemented to meet specific clinical needs. [21] IHE Profile offer a clear implementation path for IT developer to develop and implement IT system for healthcare organization that meet the need and compatible with environment of healthcare industry. At the same time, IHE Profiles also help reduce the cost which can be wasted if organization need to go through trial and error in development of their IT system. The Profile also help reduce workload for IT developer on various kind of communication standard exist within healthcare IT domain.

2.2.3 Cross-Enterprise Document Sharing (XDS) Profile

The Cross-Enterprise Document Sharing (XDS) IHE Integration Profile facilitates the registration, distribution and access across health enterprises of patient electronic health records. [22] The profile is focused on providing a standards-based specification for managing

the sharing of documents between any healthcare enterprises, ranging from a private physician office to a clinic to an acute care in-patient facility.

2.2.4 XDS, XDS.a, XDS.b, and XDS-I

XDS is generic term to reference all XDS profiles which are Cross-Enterprise Document Sharing Profiles. XDS.a and XDS.b are implementation profiles that describe technically how the implementation will be done. XDS-I is an XDS implementation specifically for medical imaging. [23] In IHE IT Infrastructure Technical Framework Vol.1 latest published in 2018 declared that term XDS within the ITI Technical Framework refers generically to any flavor of XDS, currently only XDS.b. [22]

2.3 Cross-Enterprise Document Sharing (XDS) Profile Implementation

The main goal of XDS.b profile is to allow XDS Affinity Domain members to share health document via XDS Document Registry. That mean, its process mainly about make metadata of document within XDS Document Repository available on XDS Document Registry entry. This allow any XDS Document Consumer to visit XDS Document Registry and seek for the document they need, before retrieve it from the XDS Document Repository that the document belong to.

2.3.1 XDS Process Flow

The process overview of Cross-Enterprise Document Sharing (XDS.b) profile is described in Figure 2. The figure also showed sequence of process along with involving XDS actors and XDS transaction format. At the beginning, each health document will be created from its sources along with its metadata attributes. These sources will be called ‘XDS Document Source actor’ which can be any machine involved in healthcare service. For example, CT scanner, laptop in each physician office, or central computer in medical lab. Next, these created documents along with its metadata will be sent to data storage which act as document repository. These repositories will be called ‘XDS Document Repository actor’ which usually be some kind of computer or server that was assigned to keep medical document available for use. According to XDS.b profile, XDS Document Source will send document metadata in the format of Provide and Register Document Set-b (ITI-41) format. In some case, XDS Document Source and XDS Document Repository may integrated together.

This made it called ‘XDS Integrated Document Source Repository actor’. The XDS Integrated Document Source Repository function the same way as XDS Document Source and XDS Document Repository will do but, combined together.

After the document and its metadata was sent to XDS Document Repository, the repository will index and make the document available for usage. At the same time, XDS Document Repository register metadata along with identifier and locator of the repository itself to local document registry. The message transaction in this process will follow format of Register Document Set-b (ITI-42). The document registry will be called ‘XDS Document Registry actor’. XDS Document Registry is software or machine that keep all document metadata and its corresponding repository from all connected repositories available for discovery. Commonly, XDS Document Registry should be database that keep document metadata from all connected repositories available for discovery through database query. However, there are no restriction from XDS.b profile for method to keep these data and how to discover each document metadata using specified document metadata attributes. There are just requirement that require XDS Document Registry to be able to accept value of specified document attributes from XDS Document Consumer and return the matched document to the consumer.

In XDS.b profile, ‘XDS Document Consumer actor’ can be any kind of software or machine that allow user like healthcare employees to access health document or medical document they need. There are no restriction in XDS.b profile that specified XDS Document Consumer actor to be different software or machine from other actors. XDS Document Consumer actor will just require user to specify value of known document metadata attributes which will allow XDS Document Repository to search for matching document metadata in its database. After received document attributes value from its user, XDS Document Consumer actor will send the specified attributes to XDS Document Registry. This message transaction will follow format of Registry Stored Query (ITI-18). Then, XDS Document Registry process received attributes by search for matching document metadata and return full document metadata which it found to XDS Document Consumer. XDS Document Consumer actor show founded result to its user. The user pick the right document they need and issue to XDS Document Repository corresponding to the document for document retrieval via XDS Document Consumer actor. XDS Document Consumer will send document retrieval request transaction in the format of Retrieve Document Set-b (ITI-43). After XDS Document Repository received document retrieval request from XDS Document Consumer, the repository will seek for the specified document and return the document to XDS Document

Consumer. XDS Document Consumer actor will make the retrieved document available for user to use.

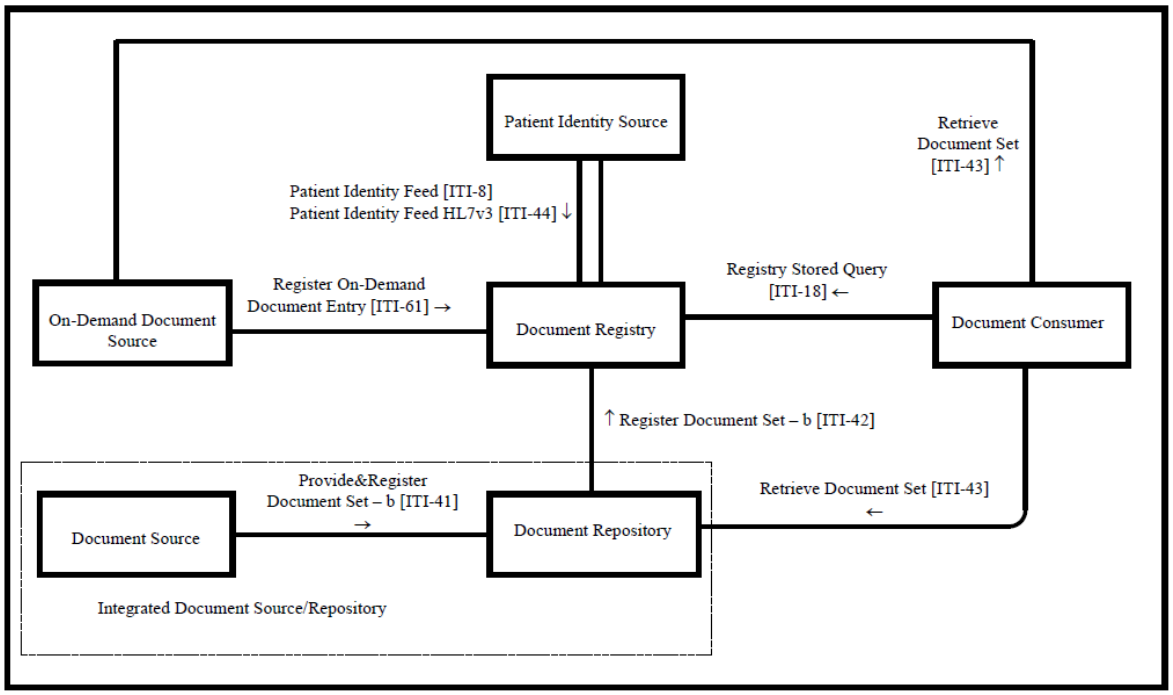

Figure 2 Cross-Enterprise Document Sharing - b Diagram [22]

2.3.2 XDS Transaction Format Types

In XDS.b profile, all messaging transaction will be in the form of XML format with schema depend on each types of transaction. Types of XDS transaction format vary upon involving actors and its purpose.

2.3.2.1 Provide and Register Document Set – b (ITI-41)

Provide and Register Doccument Set – b (ITI-41) transaction format define XML schema for message that send metadata of document from XDS Document Source actor to XDS Document Repository actor for store into document repository. This type of transaction mainly require XDS Document Source to include all available metadata attributes of created document for other XDS actor. XDS Document Repository actor will need to acknowledge to XDS Document Source if it successfully received document and its metadata.

2.3.2.2 Register Document Set – b (ITI-42)

Register Document Set – b (ITI-42) define XML schema for message that send metadata of available document in repository from XDS Document Repository actor to XDS Document Registry actor to register the document into document registry entry. Main purpose of this type of transaction is to pass document metadata stored in repository to XDS Document

Registry actor addition with attributes about the repository. XDS Document Registry actor will need to respond back to XDS Document Repository actor when received the transaction and register it to document registry entry.

2.3.2.3 Registry Stored Query (ITI-18)

Register Stored Query (ITI-18) is general XML schema format that used by one actor to query for data from other actor in entire IHE IT Infrastructure Framework. In this work, the transaction will be used by XDS Document Consumer actor to request for document metadata it seek from XDS Document Registry actor. Any document metadata attributes known by XDS Document Consumer will be included in the transaction. XDS Document Registry will use specified metadata attributes to search for matching document metadata inside document registry entry. XDS Document Registry will need to respond to XDS Document Consumer actor that it received the request. XDS Document Registry also need to return search result to XDS Document Consumer.

2.3.2.4 Retrieve Document Set (ITI-43)

Retrieve Document Set (ITI-43) define XML schema for XDS Document Consumer to request document retrieval from XDS Document Repository. Different to other transactions involved in XDS.b profile, Retrieve Document Set transaction only contain few essential attributes to allow retrieval of document from document repository. XDS Document Repository will need to acknowledge to XDS Document Consumer when received the transaction before return the requested document.

2.3.3 Transaction Object Type and Attributes

In each transaction, there are set of metadata attributes that represent the document. These metadata attributes are categorized to three sections. SubmissionSet represent information associated with submission of document since it was created by the source. Folder represent group that the document belong to. DocumentEntry represent the document itself.

2.3.3.1 SubmissionSet

SubmissionSet Metadata Attributes	**Description**
author	The humans and/or machines that authored the SubmissionSet. This attribute contains the sub-attributes: authorInstitution, authorPerson, authorRole, authorSpecialty, authorTelecommunication.
availabilityStatus	The lifecycle status of the SubmissionSet.
comments	Comments associated with the SubmissionSet.
contentTypeCode	The code specifying the type of clinical activity that resulted in placing the associated content in the SubmissionSet.
entryUUID	A globally unique identifier used to manage the entry.
homeCommunityId	A globally unique identifier for a community.
intendedRecipient	The organizations or persons for whom the SubmissionSet is intended.
limitedMetadata	A flag that the associated SubmissionSet was created using the less rigorous metadata requirements as defined for the Metadata-Limited Document Source.
patientId	The patientId represents the primary subject of care of the SubmissionSet.
sourceId	Identifier of the entity that contributed the SubmissionSet.
submissionTime	Point in time at the creating entity when the SubmissionSet was created
title	The title of the SubmissionSet.
uniqueId	Globally unique identifier for the SubmissionSet assigned by the creating entity.

2.3.3.2 Folder

Folder Metadata Attributes	**Description**
availabilityStatus	The lifecycle status of the Folder.
codeList	The set of codes specifying the type of clinical activities that resulted in placing DocumentEntry objects in the Folder.
comments	Comments associated with the Folder.
entryUUID	A globally unique identifier used to manage the entry.
homeCommunityId	A globally unique identifier for a community.
lastUpdateTime	Most recent point in time that the Folder has been modified.
limitedMetadata	A flag that the associated Folder was created using the less rigorous metadata requirements as defined for the Metadata-Limited Document Source.
patientId	The patientId represents the primary subject of care of the Folder.
title	The title of the Folder
uniqueId	Globally unique identifier for the Folder.

2.3.3.3 DocumentEntry

DocumentEntry Metadata Attributes	**Description**
author	The humans and/or machines that authored the document. This attribute contains the sub-attributes: authorInstitution, authorPerson, authorRole, authorSpecialty and authorTelecommunication.
availabilityStatus	The lifecycle status of the DocumentEntry
classCode	The code specifying the high-level use classification of the document type (e.g., Report, Summary, Images, Treatment Plan, Patient Preferences, Workflow).
comment	Comments associated with the document.
confidentialityCode	The code specifying the level of confidentiality of the documented.
creationTime	The time the author created the document.
entryUUID	A globally unique identifier used to manage the entry.
eventCodeList	This list of codes represents the main clinical acts, such as a colonoscopy or an appendectomy, being documented.
formatCode	The code specifying the detailed technical format of the document.
hash	The hash of the contents of the document.
healthcareFacility TypeCode	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred.
homeCommunityId	A globally unique identifier for a community.
languageCode	Specifies the human language of character data in a document.
legalAuthenticator	Represents a participant within an authorInstitution who has legally authenticated or attested the document.
limitedMetadata	Indicates whether the DocumentEntry was created using the less rigorous requirements of metadata as defined for the Metadata-Limited Document Source.
mimeType	MIME type of the document.
objectType	The type of DocumentEntry (e.g., On-Demand DocumentEntry).
patientId	The patientId represents the subject of care of the document.
practiceSettingCode	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g., Family Practice, Laboratory, Radiology).
referenceIdList	A list of Identifiers related to the document
repositoryUniqueId	The globally unique identifier of the repository where the document can be accessed.

serviceStartTime	The start time of the service being documented.
serviceStopTime	The stop time of the service being documented.
size	Size in bytes of the document.
sourcePatientId	The sourcePatientId represents the subject of care's medical record identifier (e.g., Patient Id) in the local patient identifier domain of the creating entity.
sourcePatientInfo	This attribute contains demographic information of the source patient to whose medical record this document belongs.
title	The title of the document.
typeCode	The code specifying the precise type of document from the user perspective (e.g., LOINC code).
uniqueId	Globally unique identifier assigned to the document by its creator.
URI	The URI for the document.

2.4 Blockchain Technology

Blockchain is a list of records, or "blocks", that are linked to one another and cryptographically secured [24]. Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer basis. Structurally, Blockchain data can be consulted, shared and secured thanks to consensus-based algorithms [25]. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [26]. Blockchain is tamper evident and tamper resistant digital ledgers implemented in a distributed fashion and usually without a central authority. At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the Blockchain network no transactions can be changed once published [27]. Participants in a Blockchain network have records of every transaction and these records are stored locally on the computers of all participants in that Blockchain network. Any kind of regime or protocol change to a Blockchain network requires consensus between the users of the network. In 2008, the Blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies which is electronic cash protected through cryptographic mechanisms instead of a central repository or authority.

This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital information that represents electronic cash takes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another

user and the Bitcoin Blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin Blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the Blockchain resilient to attempts to alter the ledger later (these include modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum. Because of this, Blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for a broader variety of applications and is being investigated for a variety of sectors. [27]

According to the document “Blockchain Technology Overview” which published by National Institute of Standards and Technology from U.S. Department of Commerce, Blockchain can be informally define as: A distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

2.4.1 Key components of Blockchain

2.4.1.1 Transaction and ‘Block’

Each of individual information represent change or cause of actions in information system are stored within Blockchain as “Transaction”. Several transaction being publish to Blockchain within the same time interval are put in the same “Block”. To form each single block, miner or validator need to hash transaction together. The resulting hash value represent integrity of each blocks. If there are any change apply to transaction in the block, it will cause hash value of the block to change. Format of block vary depend on each Blockchain platform and its use case. Some platform may published in a form of plaintext just to act as the source of truth for every participating node to look without constraint. Some platform may bound transaction or block to unique address to extend variation in accessibility. Some platform may encrypt block to maintain confidentiality of data. Transaction and Block are the key component which determine purpose and application of Blockchain.

2.4.1.2 Cryptographically hashed ‘Chain’

Other than the concept of “Block”, The Blockchain concept also introduced the concept of “Chain. As integrity of each Block represent by its hash value, integrity of entire Blockchain represent by all hash value of all Block within “Chain”. The foundation of

“Chain” concept is by chaining hash value of all block together. This can be done by include hash value of block formed in previous time interval into the current block to generate its hash value. Any changes made to any one single block will alter hash value of the entire chain that come after. This make it harder to alter data that published within Blockchain. It require anyone who want to alter the data to apply change to all block that come after the target block until the current one to make the change valid. Combined with decentralization characteristic of Blockchain network, this make data exist in Blockchain nearly impossible to alter.

2.4.1.3 Distributed network of participate ‘Node’

Any machine participate in the Blockchain network are call “Node”. Node represent population of each Blockchain network. Each node keep the exact same copied of data in Blockchain. If there are any different in data between nodes, the version of data being held by minority of participating node will be clarify as false and will not be accepted by the entire Blockchain network. In each Blockchain network, some node may participate as miner or be elected as validator of the network at each different time interval. Miner node and validator node have duty to perform task assigned by the network to maintain its consensus. The Blockchain can be alive only if there at least one participating node maintain it, while strength of its immutability depend on number of participating node. More participating node mean stronger immutability.

2.4.1.4 Consensus

Each Blockchain network have its own method to maintain consensus within the network. Consensus mostly maintain by let participating node to perform computational task upon publishing of every block. There are many variation of consensus invented. The most commonly used method is Proof of Work (PoW). Proof of Work require miner node to solve mathematical problem before allow it to publish Block of current time interval. For example, in the most notable Blockchain network like Bitcoin, the Proof of Work require miner node to randomly find ‘nounce’ number that included in Block and result as hash value with selected amount of ‘0’. The task can only be performed effectively by investing computational resource. Only the fastest node that found the right ‘nounce’ number by chance can validate block at the time interval. This guarantee that there are no specific miner to process any specific block exist in the network, render man-in-the-middle attack to become nearly impossible in Blockchain (this is not included data in transition before reaching Blockchain).

2.4.2 Key characteristics of the Blockchain

Key characteristics of the Blockchain can be vary depend on its setup and environment of usage. According to many sources, key characteristics of the Blockchain may be summarized as followed:

2.4.2.1 Decentralization

Decentralization is the foundation of Blockchain technology as response to problem of centralized system. In centralized system, especially centralized database, there is a chance that the database got compromised by hacker. Other than rely on backup data, there are very few options to deal with the incident. This make the compromised database become single point of failure which prevent follower system to operate. Decentralization of data was proposed to scatter the chance of single database from getting compromise. This make decentralized database network have more resistant against incident threatening centralized data. Even hit by incident that aim to compromise the data. If at least half of decentralized network survived the incident, the data survive the attack.

2.4.2.2 Immutability

With utilization of cryptographically hashed chain combined with decentralized network, the Blockchain technology ensure that any data published on Blockchain cannot be deleted or modified. If there are any modification made to content of published data, it will cause change on the hash chain and detected the network. Any action that cause change to hash chain will be negate by majority of the network. This mean if anyone want to temper with published data on Blockchain, they will need to compromise the entire network at once. Any survived node have chance to notify the abnormal to the entire network.

2.4.2.3 Transparency

As the foundation of Blockchain is to have all participant nodes have the exact same copy of Blockchain ledger, it passively give transparency to published data. It is impossible for anyone to secretly hide something inside Blockchain without let other participants in the Blockchain network know.

2.4.2.4 Distributed

Blockchain have distributed characteristic by design. All node will have exactly the same Blockchain ledger. Any content published to Blockchain ledger are passively distributed to all Blockchain node. With consensus algorithm, it require that the publishing content either sent to all nodes before accept to publish or being accepted then send to all node, to complete consensus. So, Blockchain ensure that any data published to the chain are distributed to all connected node.

2.4.2.5 Trust

In public network where anyone can participate or in permissioned network where participants are not completely trust each other, trust is the main factor that define usability of decentralized network. Along with Blockchain technology, consensus solve the issue about trust by eliminate the chance of any single node participate in Blockchain to have absolute control over publishing data when certain condition are met. It can rely either on randomness or specially designed algorithm depend on each consensus method. When none of any single node can have absolute control over publishing data on the Blockchain, made it extreme difficult for someone to temper with target data. Many consensus method ensure that it will much more expensive for anyone to attempt on tempering with publishing data when compare to benefit they can get. This passively establish trust between all participant nodes.

2.4.3 Blockchain variant and community – move public private here

Followed the trend about decentralizing data, many Blockchain communities has been developed and growth respectively. Each platforms and communities have their own technical design and use case. Many Blockchain platform developed specifically to use as cryptocurrency while other was created to act as backend infrastructure of various applications.

2.5 Ethereum

Ethereum are one of well-known open source Blockchain platform. The platform initially invented by developer named Vitalik Buterin and further develop by Ethereum community. Main approach of Ethereum Blockchain is about use Blockchain technology for application other than cryptocurrency. The platform proposed concept about ‘smart contract’.

2.5.1 Smart Contract

The concept of smart contract was initially proposed by Ethereum. Now the word ‘smart contract’ become common word to describe feature that allow developer to design the content that publish to Blockchain and its computational behavior. In Ethereum, smart contract code written with Solidity programming language. Smart contract define what behavior the contract will do when open/view by user. Smart contract rely on Ethereum Virtual-Machine (EVM) which allow host machine of Ethereum client to be able to execute smart contract Solidity code. EVM was designed to allow portability of Ethereum platform and always packed with Ethereum client. Now there are many interface tools developed by Ethereum

community that allow Ethereum client to work with major programming languages. This further extend usage of smart contract to infinite possibilities.

2.5.2 Solidity – Ethereum Blockchain programming language

Solidity is javascript-like programming language that specifically design to use with Ethereum smart contract. The main purpose of the programming language is to act as the middle between human-understandable language and computer language. It reduce difficulty for developer to design behavior of their smart contract on Ethereum Blockchain. The language is update and maintain by Ethereum community.

2.6 Related Work

There are many research proposing about decentralize healthcare information with Blockchain technology. The goal of decentralization and implementation of each work have many variant. These are several works that proposed interesting idea and concept about implement healthcare informatics system based on Blockchain technology.

2.6.1 A Blockchain-Based Approach to Health Information Exchange Networks [28]

The work proposed about using Blockchain like central hub for health information exchange. The main goal of this Blockchain concept is to connect all bread and crumb of patient health information together by allow participate node to discover health information data they seek and its location within Blockchain ledger. Increase interoperability in health information exchange. Their main contribution is the concept that suggest use of FHIR health information exchange standard combine with Blockchain technology. Each transaction on Blockchain will contain FHIR locator of actual data along with its index which make each transaction available for search. Due to the limit of health information that it require certain amount of confidentiality, this make it not really compatible with platform open to public like Blockchain. Store actual data somewhere else outside Blockchain and put its locator into Blockchain for use. With known secure index, this Blockchain help connect patient information that scattered across healthcare industry together. The work also gave suggestion about how health information Blockchain should look like and what it should have by common. There also other major contributions that proposed about using secure index for searching on encrypted data and ‘Proof of Interoperability’. This work suggest that if health information are kept within Blockchain in encrypted form, it should also contain secure index which will allow data search even the data is encrypted. This should reduce the difficulty of

implementing health information with Blockchain. And other major concept proposed in this work is ‘Proof of Interoperability’. Based on Proof of Work consensus, the work suggest that computational resource should not be wasted unnecessarily. Instead of put computational resource to competition for consensus, it should be used to verify interoperability of participate health data instead. However, they didn’t proposed about how the consensus should work in detail. This work gave a good example of how Blockchain can have potential to solve issue that common in healthcare industry like interoperability. Additionally, they also proposed many concepts that can be a good foundation for using Blockchain technology with health information.

2.6.2 A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data [29]

Main goal of MedRec is to provide Blockchain that act as a middle for health information exchange while allow Blockchain participants to gain benefit from participation. They chose Ethereum as Blockchain platform for the system. Ethereum provide smart contract and address based access for the work. This work assume that miner/validator nodes are health institution that have demand for large amount of health information data to use in their research. Miner/validator node will be rewarded with anonymized health data which can be used in research involve health data analysis. Additionally, MedRec proposed about allowing patient to have consent about usage on their data. Give more control over individual health data. The work also adopted cryptographic key scheme proposed by Zyskin et al. [30], to ensure that only authorized party can access patient health information published on Blockchain. Additional to these main contributions, they also gave suggestions about factor that should keep continuity of Blockchain and how Blockchain element provided by platform like Ethereum can be useful. One of interesting concept is about using Ethereum address as patient identifier. Due to all identity exist on Ethereum Blockchain are assigned with unique address, these unique address can reduce complexity in patient identifier management if designed properly. MedRec gave a good example of concept that needed to maintain continuity of Blockchain network by allow participant to gain benefit from participation in some way. At the same time, MedRec is another good example that using Blockchain technology to aid health information exchange issue. And the last, MedRec have shown flexibility of smart contract and how it can be useful when implement with healthcare information.

2.6.3 Blockchain-Based Data Preservation System for Medical Data [31]

This work proposed about using Blockchain to keep data that need to have confidentiality preserved. Regardless of what kind of data, this Blockchain allow user to design what data they want to keep in Blockchain. The chosen data will be encrypted before publish into Blockchain. The goal of this Blockchain concept is to preserve medical data inside Blockchain away from any tempering attempt while keep it secret and always available for its owner. Instead of let data available to public, this work have demonstrated how Blockchain technology can be used in different approach like keeping medical data available to only authorized entity.

CHAPTER III
METHOD

This chapter will explain about method of how the Blockchain was designed to operate under IHE XDS.b profile process flow. The chapter is separated to three parts. The first part introduce about architecture design and roughly define how we integrate Blockchain components into IHE XDS.b profile process flow. The second part will explain the first part further into the aspect of Blockchain components. This part will more focus about how we adopt and setup existing Blockchain platform to match our requirement for usage in our scenario. The last part will further explain the first part in term of integrating IHE XDS.b profile with Blockchain. This part focus on how we create and adapt each components in our work to meet the requirement specified by IHE XDS.b profile.

3.1 Architecture Design

This work can be roughly described as “Document Registry Blockchain”, as the main purpose of the Blockchain is to keep document registry that shared between participating hospitals. XDS Document Registry actor of each hospitals act as Blockchain node and connected to each other in the form of Blockchain network as shown in **Error! Reference source not found.**.

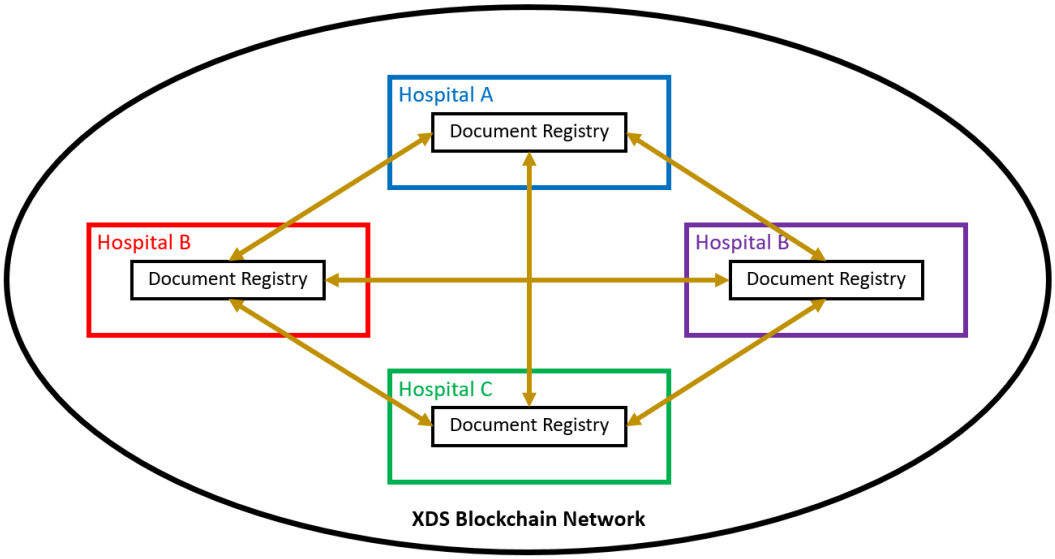

Figure 3 Document Registry of each hospital connected to other as Blockchain

There are two layers of software on each system, as shown in Figure 4. The first layer is Blockchain Client (right side of Figure 4) which allow the Blockchain node to communicate with other nodes using Blockchain specific communication protocol. The second layer is local application layer (left side of Figure 4). Local application layer compose of four main local applications. First one is XDS Document Repository which have access to local database that contain actual healthcare document which its registry was registered in XDS Document Registry Blockchain. Second local application is XDS Document Registry Searcher that will search registry entry for matching registry with specified index. At the same time, XDS Document Registry Searcher will have its own database to remember address of registry in XDS Document Registry Blockchain it ever searched and found. This allow faster process when user need to access the same registry for next time. The third local application is XDS Document Registry Query. XDS Document Registry Query will query for specified registry using its address on Document Registry Blockchain. The querying process can be done by XDS Document Registry Query application issue new smart contract to interact with target document registry smart contract.

After received query smart contract, target registry smart contract will response by send back network address of document repository where actual healthcare document associated with the registry is contained. The last local application is Document Exchange History Recorder. This application will record exchange history of healthcare document between organizations to the Blockchain. Healthcare document exchange history that recorded on the Blockchain will act as evidences like system audit. If any incident happened and

organization need to trace back for document exchange history, this ensure that the history cannot be tampered or deleted by anyone.

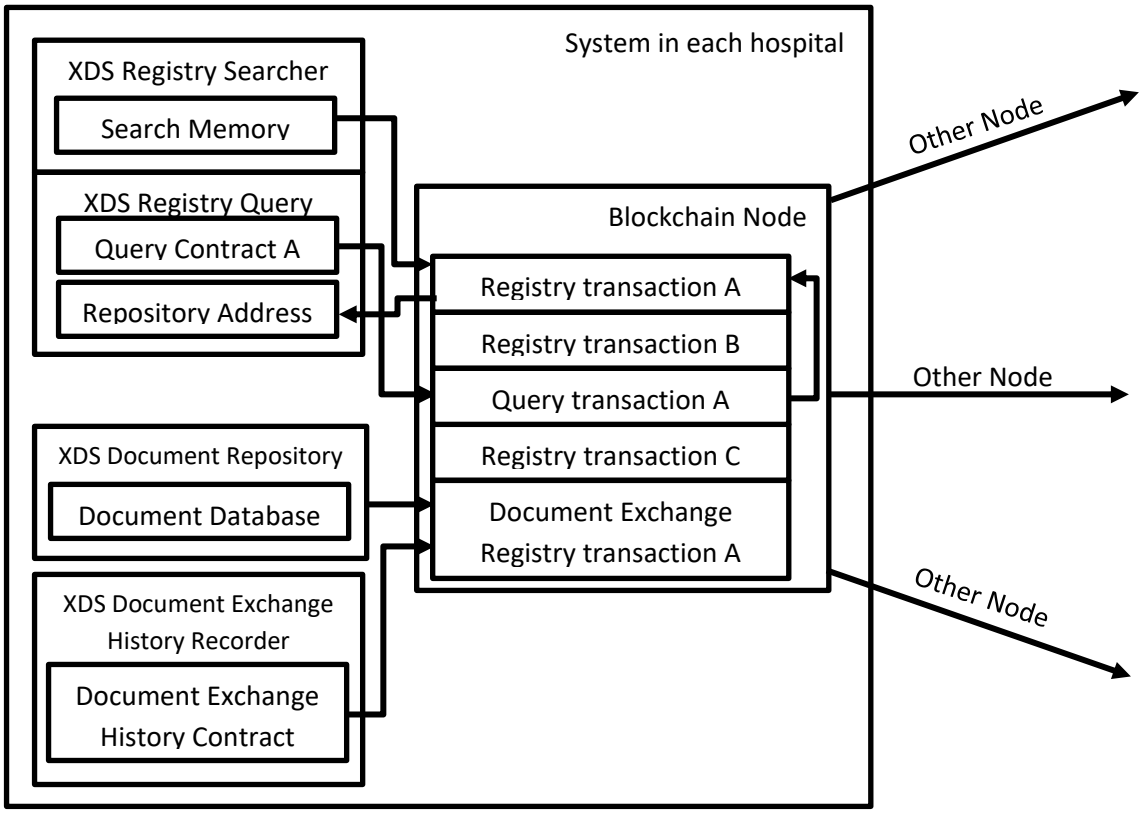

Figure 4 Component applications in each hospital system

Process flow of Document Registry Blockchain consist of 3 main phases. At the beginning when Document Repository received healthcare document from its source, Document Repository store the document into database while generate document registry which is metadata of the document. After document registry was generated, it will be transmit to all participating Blockchain node in the form of document registry smart contract. Elected Blockchain miner or validator node will gather all transactions of the smart contract within each time period and contain them into current candidate block before enter consensus algorithm. The smart contract will need to be approved by consensus algorithm of the Blockchain before getting published. Approved by consensus algorithm mean that the block is accepted by all Blockchain nodes to be published. If the block is not approved by consensus algorithm, this block will be rejected. In this case, all node that tried to publish its transaction within this block may need to attempt again with the same transaction on next block. Otherwise if the block got approved by consensus algorithm, all Blockchain node will add this

block to the Blockchain. That mean, the smart contract that contain document registry which was generated by Document Repository was published to the Blockchain together along with the published block. When someone seek for document within the network, they will need to seek for document registry that associated with the document. Then, reach Document Repository specified within the associated document registry to exchange for actual document. For example, Hospital A seek for the last hospital visit of Mr.Bob within the Document Registry Blockchain network.

User at Hospital A need to start with specify indexes that unique to Mr.Bob and use it to search for associated registry using Document Registry Searcher application. Document Registry Searcher will use specified indexes to find for registry transaction that smart contract response to these indexes. When the matching registry transaction was found, Document Registry Searcher will return Blockchain address of the transaction to user at Hospital A. In this case, it may return more than one registry that associated with Mr.Bob. User at Hospital A may need to seek for the one with latest timestamp. When the registry was found, Hospital A will need to query to the Blockchain to access the transaction. This process require Hospital A to use Document Registry Query application to issue smart contract to the Blockchain. This smart contract will be called “query contract” and it act as evidence as someone was queried for specific transaction. After that, smart contract of the transaction will response by allow Hospital A to access its content. After Hospital A accessed the transaction, it reveal that document of the last hospital visit of Mr.Bob kept in document repository of Hospital B. Hospital A then contact Hospital B and request for document exchange to retrieve document of Mr.Bob last visit. This process will require Hospital A to declare to the Blockchain that it is now exchanging Mr.Bob document with Hospital B by publish Document Exchange History smart contract to the Blockchain. Smart contract can also be programmed to allow patient control over sharing of their data. However, this depend on each organization environment and business model.

3.2 Blockchain Design

This section will explain about how we prepare Blockchain components to meet requirement in our scenario.

3.2.1 Blockchain platform and participant node

A requirements that need to be setup to meet our scenario included type of Blockchain network, who is participant node, and consensus for publishing block into the chain. In our scenario, we assume that participant node are machine host by members of XDS Affinity Domain. Each participant node will take the main role as XDS Document Registry actor which will maintain Blockchain ledger where document registry entry are kept. As the Blockchain allow only XDS Affinity Domain members to participate as node, this make the Blockchain type classified as permissioned chain. For consensus, there need more explanation on considering the right one. So, consensus will be further explain in next part.

3.2.2 Consensus

Consensus take an important role to ensure that all participant node are accepting the same Blockchain ledger while prevent malicious action that try to temper with integrity of the ledger. Poor choice of consensus that not suitable with characteristics of selected network can cost efficiency of the Blockchain and gave vulnerability to malicious action. Considering the Blockchain in our work, it is permissioned Blockchain that priority integrity of document registry entry exist on the Blockchain. Additionally, for prototype, there will be few participant nodes introduced for concept demonstration. According to [33], [34], the Practical Byzantine Fault Tolerance (PBFT) consensus method is the most suitable one. And when considering in detail of PBFT, there also variant that made to use with Blockchain platform named Istanbul Byzantine Fault Tolerance (IBFT) [35], [36]. IBFT was Byzantine Fault Tolerance consensus that specifically made to use with Blockchain platform like Ethereum. The main different of IBFT from PBFT is that PBFT is kind of general word referred to Byzantine Fault Tolerance that being used with ordinary decentralized network without adoption of Blockchain technology while IBFT is made for Blockchain. With Byzantine False Tolerance as consensus, it allow few numbers of XDS Affinity Domain node to effectively maintain integrity of Blockchain network without unnecessarily wasting computational resource. This make our Blockchain more compatible with continuous operation in healthcare field. IBFT was not included in classic Ethereum but, there are community-made variant of Ethereum platform named Quorum [37] that have IBFT available as consensus by default. That mean, in our implementation, we will adopt Quorum for our work.

3.3 Design of XDS.b profile integrated with Blockchain

This section will contain further explanation of how we create and adapt each components in our work to meet the requirement specified by IHE XDS.b profile. Main goal of the design is to make our Blockchain concept function as similar as common XDS.b profile complied system.

3.3.1 Defining XDS actor

In this work, XDS Document Source actor and XDS Document Repository are assumed to be the existing system that have its functional process complied with XDS.b profile. The strict requirement is that XDS Document Repository should be able send Register Document Set-b (ITI-42) to assigned XDS Document Registry actor in the local system. At the same time, XDS Document Registry actor will be assigned as Blockchain node which can interact with Blockchain ledger using tool like Geth client and Web3js. The machine hosting XDS Document Registry will need to be provided with enough data storage capacity to keep full-chain version of the Blockchain ledger. For demonstration, the node also need to act as consensus node which using IBFT method for accepting block into the chain. If there are any real adoption of this concept, any participant node can be consensus node. That mean, any node belong to XDS Affinity Domain members can help maintain the Blockchain network even it have no function of XDS Document Registry. However, as requirement from our scenario, each XDS Affinity Domain member will need to have at least one node that participate in the network as XDS Document Registry actor and consensus node. For XDS Document Consumer, it must be ordinary system that can communicate with Registry Query (ITI-18) transaction and Document Retrieval (ITI-43) transaction. So, it can communicate normally with XDS Document Registry Blockchain node and XDS Document Repository actor of other system. We assume that all XDS Affinity Domain members are using the same patient identifier mapping so, we can eliminate the need for Patient Identity Feed actor and reduce complexity of our demonstration. We exclude XDS On-Demand Document Repository from our demonstration, due to complexity of on-demand type document that require usage of other XDS transaction type. This can be further developed with almost the same pattern as stable document from XDS Document repository if anyone want to adopt concept in this work and put it to real usage. In our implementation, each XDS actor will represent the software program that have behavior following characteristic of the actors. And for lessen complexity, each program will host by separated server to give significant view of the concept.

3.3.2 Design of Blockchain following XDS.b process flow

Design of XDS.b Blockchain will be separate to 6 steps. These step are the process following XDS.b process flow. This section will explain how the design be in each step of XDS.b process flow.

3.3.2.1 Receiving Register Document Set-b (ITI-42) transaction from XDS Document Repository

XDS Document Registry actor must be programmed to receive ITI-42 transaction from local XDS Document Repository in the system via Transmission Control Protocol. XDS Document Registry must be able to parse the transaction which written in XML format and translate it into javascript object form. After that, used attributes specified in the object to create XML format response message before send back to the sending XDS Document Repository. The response message structure will follow the requirement specified for ITI-42 transaction response message. This will let the sending XDS Document Repository know that the message was accepted and finish the process.

3.3.2.2 Publishing received Register Document Set-b (ITI-42) transaction

XDS Document Registry use received javascript object to create smart contract. Then, attempt to publish the contract into Blockchain. The attempt must continue until the smart contract is successfully published into Blockchain ledger. The smart contract will have two main part that will function when the contract was called. The first part is smart contract code that will compare approaching attributes value for the matching one. It will notify the searcher application if there are any matching attribute found while not allow user to directly see the value of those attributes. The second part of smart contract is where it store XML message that will be used to respond to XDS Document Consumer actor, containing all available metadata attributes of corresponding document. Each smart contract will be assigned with unique Ethereum address after being published to the Blockchain.

3.3.2.3 XDS Document Consumer send Registry Query (ITI-18) transaction to XDS Document Registry

Jump to XDS Document Consumer side, it will require user to specify metadata attributes of health document they seek along with its value. XDS Document Consumer accept the input and use it to create ITI-18 transaction. XDS Document Consumer then send the created transaction to XDS Document Registry via TCP.

3.3.2.4 XDS Document Registry search document registry entry

Additional from 3.3.2.1, XDS Document Registry must be able to receive ITI-18 transaction then parse and translate it to javascript object. XDS Document Registry also need to be programmed with document registry entry search function. The function will accept javascript object derived from ITI-18 transaction and use it to search for matching document registry that have only matching attributes specified in ITI-18 transaction. For our work, the searcher application will adopt the same search pattern as the one proposed in [39] which simply sequentially search smart contract one by one. Any document registry smart contract with mismatch metadata attributes value will be excluded from found result. At the same time, all document registry with metadata attributes value match with all specified attributes will be marked as found result.

3.3.2.5 XDS Document Registry return Registered Document entry to XDS Document Consumer

XDS Document Registry derive XML message in second part of all smart contracts marked as found results. XDS Document Registry then send all XML message of found results back to XDS Document Consumer via TCP.

3.3.2.6 XDS Document Consumer send Document Retrieval (ITI-43) to XDS Document Repository that keep the document

After received found results from XDS Document Registry, XDS Document Consumer will need to parse these XML message then translate it into human-understandable form before present it to user. The user will need to manually pick for the right one that belong to the document they seek. When the document was selected, the user can use XDS Document Consumer actor to issue ITI-43 transaction to XDS Document Repository that keep the document. Then, the XDS Document Repository can return the document to XDS Document Consumer and allow user to access the document. In this work, we also proposing about use Blockchain ledger as additional audit trail. When one XDS Document Consumer retrieve document from XDS Document Repository, there should be some kind of document exchange evidence published into Blockchain. This will not just allow tracking traffic of health document exchange, but also provide evidence that allow XDS Affinity Member to find for document substitution if there are any problem happen to the document they have.

Chapter IV

IMPLEMENTATION

This chapter will focus on technical explanation on concept implementation. This chapter divided into three parts. The first part introduce about XDS Toolkit which is the source of XDS transaction sample for our implementation and also act as validation tool to verify if our implementation comply to XDS.b profile. The second part will explain about technical setup of Blockchain platform for our implementation. The third part then jump to implementation of software that act as component to integrate Blockchain to XDS.b process flow. These software will act as the middle between function of XDS Document Registry actor and function as Ethereum Blockchain node. The last part will explain behavior of smart contract that we designed in technical aspect.

4.1 XDS Toolkit

XDS Toolkit was provided by United States National Institute of Standards and Technology (NIST) [40]. The toolkit was developed to allow developer to test their software if it comply with IHE XDS.b profile and can communicate with other system. XDS Toolkit provide many tools that can send sample XDS transactions to specified location and wait for proper respond defined in XDS.b profile. These tools came in variant depend on what type of XDS actor that the testing software is.

4.1.1 XDS Toolkit as XDS Document Repository

In our implementation, XDS Toolkit will act as XDS Document Repository actor. It will send out Register Document Set-b (ITI-42) to our developed XDS Document Registry and wait for respond. This passively allow it to be validator to test if our XDS Document Registry actor can communicate with XDS Document Repository in common XDS system.

4.1.2 XDS Toolkit as XDS Document Consumer

XDS Toolkit will test that if our XDS Document Registry can communicate with XDS Document Consumer in common XDS system.

4.2 Blockchain Setup for Implementation

Before start integrate Blockchain to XDS.b process flow, we need to make Blockchain ready for implementation first.

4.2.1 Blockchain platform

For implementation in this work, we chose Ethereum Blockchain as platform to demonstrate the concept. Ethereum allow interaction with local Ethereum Blockchain node via Geth client. A protocol that each node use to sync data of Blockchain ledger with each other is ÐΞVp2p Wire Protocol [32] which is default to Ethereum. Other infrastructure of Blockchain will rely on Ethereum.

4.2.2 Interact with Blockchain and smart contract

To directly command behavior of each Blockchain node, we require Geth client which allow user to issue command to the node like start-stop mining and start sync Blockchain data with other node. For programming smart contract, Ethereum providing IDE for Solidity language that can compile and deploy smart contract to local Ethereum node. To interface our program to Ethereum smart contract, we can use Ethereum API tools like Web3js [38] as a middle. Web3js allow smart contract control through javascript language and transition variable from javscript to Solidity. Then, Blockchain platform is ready for smart contract design and implementation of XDS.b profile.

4.3 XDS Document Registry Actor

In the implementation of this work, XDS Document Registry actor will be the main actor that will be converted from using common database to use Blockchain ledger to keep associated data. The software program must be able to communicate with XDS Document Repository actor and XDS Document Consumer actor. At the same time, the software will need to act as the middle between XDS system and Blockchain.

4.3.1 Receive message from XDS Document Repository

XDS Document Registry Actor will communicate with XDS Document Repository via TCP connection. The message that used for communication will be XML formatted message that have XML schematic defined in ITI-42. After received the message from XDS Document Consumer, XDS Document Registry will need to parse the message to retrieve metadata attribute and reserve it for next step. The retrieved metadata attribute will be in the

form of javascript object. We adopted xml2js javascript module as parser algorithm. The xml2js will store retrieved object within RAM that the program is running.

4.3.2 Respond to XDS Document Repository

XDS Document Registry will use javascript object from 4.3.1 to create XML formatted message with schematic defined in ITI-42 for responding message. The actor then send the created message back to XDS Document Repository that sent the message in 4.3.1. This will notify XDS Document Repository that the message it sent was received by XDS Document Registry and allow XDS Document Repository to finish its task.

4.3.3 Create document registry smart contract

XDS Document Registry use javascript object from 4.3.1 to create smart contract using Web3js API tool. As mentioned in chapter 3, smart contract will consist of two main parts. The first part will allow smart contract to cooperate with search application while second part will keep XML message that will be respond to XDS Document Consumer. XDS Document Registry pass metadata attribute variable from the javascript object into the first part of smart contract. After the first part of smart contract, XDS Document Registry construct XML formatted message which schematic defined in ITI-18 as respond message. Then, pass the entire constructed message into the second part of smart contract.

4.3.4 Receive message from

Similar to 4.3.1, XDS Document Registry will parse the received XML formatted message and retrieve metadata attributes in the message as javascript object. XDS Document Registry will immediately create XML formatted message similar to 4.3.2 and send it back to XDS Document Consumer as acknowledge that the message was received.

4.3.5 Search for matching document registry

XDS Document Registry pass javascript object from 4.3.4 to document registry searcher function. The search function will sequentially call published document registry smart contract started from the recent one backward to the oldest one. On each call, the search function compare metadata attributes and its value in javascript object with metadata attributes kept by the smart contract. Any smart contract with at least one mismatch metadata attribute value will be neglected by search function. At the same time, all smart contract that have its metadata attributes value match with all metadata attribute specified in javascript object will be marked as found result. XDS Document Registry then retrieved XML message from the

second part of each found result and send it to XDS Document Consumer. The pattern of messaging will be as defined for ITI-18.

4.4 Document Registry Smart Contract

This section will further explain the detail of document registry smart contract in technical term and explain how it interact with XDS Document Registry actor.

4.4.1 How Ethereum smart contract work

To execute the behavior defined in Ethereum smart contract that published to Blockchain, it require tool to execute the code. This tool can be Ethereum client like Mist which directly show behavior of smart contract to user, or can be API tool like Web3js which integrate smart contract behavior with javascript program. Ethereum only allow execution of smart contract via calling the unique Ethereum address assigned to each smart contract when it was being published. Otherwise, there will be only JSON-RPC language exist on the transaction in Blockchain which is human cannot understand. That mean, if someone want to know content or know the behavior belong to each contract, they will need to know its Ethereum address. That is the reason why we need to sequentially search document registry smart contract from one address to other address instead of directly query for matched data like people do it in database such as SQL.

Ethereum smart contract can be programmed to do anything that ordinary computer program can do, with the limit that it require someone to call for its Ethereum address and executed it at least once. It also limit by agreement between Ethereum communities that it should not run the infinite loop. This can be prevent through usage of ‘Gas limit’. Each smart contract Solidity code will be marked with its Gas cost when compiled. Gas value represent amount of computational resource that the machine executing the smart contract will require to complete task. That mean, infinite loop will result as extremely expensive Gas value. Any smart contract with exceed Gas value defined by each Ethereum network will be negate from publishing into Blockchain. Surely, smart contract can be designed to store certain value of programming variable and return the value to the one who execute the smart contract. This is the function that we use for our implementation in this work. Note that variable stored within smart contract can be categorized as non-SQL as have its structure similar to JSON format.

4.4.2 Implementation of Smart Contract as document registry

As mentioned, in 4.4.1 that smart contract can be designed to store any kind of programming variable. So, we design smart contract which when executed, it will spawn smart contract that store given document metadata attributes value within specific Ethereum address. When these spawned smart contract was called, it will simply return the stored metadata attributes value back. This is how the first part of smart contract in our implementation work. At the same time, the second part of smart contract will instead store the entire XML message and ready for use. By these methods, it allow document registry to store within Ethereum Blockchain. The first part of smart contract will allow search function of XDS Document Registry to discover matching registry by compare with its metadata attributes value. The second part allow XDS Document Registry to simply send the stored message back to XDS Document Consumer. These composed to function as Document Registry Smart Contract.

REFERENCE

[1] Carestream Health, “Interoperability : Connecting the Healthcare Enterprise to Deliver Responsive Patient Care,” pp. 1–9, 2015.

[2] PolicyMedical, “Interoperability in Healthcare: To Have or Not to Have.” [Online]. Available: https://www.policymedical.com/interoperability-healthcare/. [Accessed: 22-Sep-2018].

[3] D. H. Interoperability, “Digital Healthcare Interoperability,” no. October, 2016.

[4] Healthcare Information and Management Systems Society, “Definition of Interoperability,” *Himss*, p. 2013, 2013.

[5] Oracle, “Interoperability : A Key to Meaningful Use,” *Solutions*, no. November, 2010.

[6] HIMSS, “What is Interoperability?” [Online]. Available: https://www.himss.org/library/interoperability-standards/what-is-interoperability. [Accessed: 27-Apr-2019].

[7] Paige Goodhew, “Why Healthcare Interoperability Matters | Redox.” [Online]. Available: https://www.redoxengine.com/blog/why-healthcare-interoperability-matters/. [Accessed: 27-Apr-2019].

[8] Dr.David Hay, “Why is interoperability so important for healthcare organisations? | Orion Health.” [Online]. Available: https://orionhealth.com/global/knowledge-hub/blogs/why-is-interoperability-so-important-for-healthcare-organisations/. [Accessed: 27-Apr-2019].

[9] A. Le Bris and W. El Asri, “STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS Applied Cybersecurity Strategy for Managers,” *ESSEC Bus. Sch.*, p. 13, 2017.

[10] Healthcare IT News, “The biggest healthcare breaches of 2017.” [Online]. Available: https://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1. [Accessed: 11-Sep-2018].

[11] HIPAA Journal, “Largest Healthcare Data Breaches of 2018.” [Online]. Available: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/. [Accessed: 27-Apr-2019].

[12] Healthcare IT News, “The biggest healthcare data breaches of 2018 (so far).” [Online]. Available: https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far. [Accessed: 27-Apr-2019].

[13] B. Weinelt, “Digital Transformation of Industries. Logistics Industry,” no. January, 2016.

[14] A. Marcelo, D. Medeiros, K. Ramesh, S. Roth, and P. Wyatt, “Transforming Health Systems Through Good Digital Health Governance,” *adb Sustain. Dev. Work. Pap. Ser.*, no. 51, pp. 1–15, 2018.

[15] T. Shaw, M. Hines, and C. Kielly, *Impact of Digital Health on the Safety and Quality of Health Care*, vol. 5, no. January. 2000.

[16] Cisco, “The Digitization of the Healthcare Industry: Using Technology to Transform Care,” *Cisco*, vol. 1, p. 12, 2017.

[17] G. Bullhound, *Digital healthcare*, no. November. 2015.

[18] B. Meskó, Z. Drobni, É. Bényei, B. Gergely, and Z. Győrffy, “Digital health is a cultural transformation of traditional healthcare,” *mHealth*, vol. 3, pp. 38–38, 2017.

[19] IHE International Inc, “About IHE.” [Online]. Available: https://www.ihe.net/about_ihe/. [Accessed: 11-Sep-2018].

[20] IHE International Inc, “IHE Process.” [Online]. Available: https://www.ihe.net/about_ihe/ihe_process/. [Accessed: 11-Sep-2018].

[21] IHE International Inc, “Profiles.” [Online]. Available: https://www.ihe.net/resources/profiles/. [Accessed: 17-Sep-2018].

[22] IHE International Inc, “IHE IT Infrastructure (ITI) Technical Framework Volume 1 Integration Profiles,” *Int. J. Healthc. Technol. Manag.*, vol. 1, no. 8.0, pp. 1–177, 2008.

[23] dkorolyk, “What Is The Difference Between XDS,XDS.a,XDS.b and XDS-I?,” 2012. [Online]. Available: http://healthcareitsystems.com/2012/05/22/what-is-the-difference-between-xds-xds-a-xds-b-and-xds-i/. [Accessed: 17-Feb-2019].

[24] M. N. Luke, S. J. Lee, Z. Pekarek, and A. Dimitrova, “Blockchain in Electricity: a Critical Review of Progress to Date,” pp. 1–36, 2018.

[25] PwC, “a Catalyst for New Approaches in Insurance.”

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. June, pp. 557–564, 2017.

[27] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview (NISTIR-8202),” *Draft NISTIR*, p. 59, 2018.

[28] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks,” *Mayo Clin.*, no. 1, p. 10, 2016.

[29] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, I. Original, and T. Vieira, “A Case Study for Blockchain in Healthcare: " MedRec " prototype for electronic health records and medical research data,” *IEEE Technol. Soc. Mag.*, pp. 1–13, 2016.

[30] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using Blockchain to Protect Personal Data,” *Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015*, pp. 180–184, 2015.

[31] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, 2018.

[32] “ÐΞVp2p Wire Protocol.” [Online]. Available: https://github.com/ethereum/wiki/wiki/ÐΞVp2p-Wire-Protocol. [Accessed: 26-Apr-2019].

[33] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain,” *CEUR Workshop Proc.*, vol. 2058, pp. 1–11, 2018.

[34] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-Janua, pp. 2567–2572, 2017.

[35] yutelin, “Istanbul Byzantine Fault Tolerance.” [Online]. Available: https://github.com/ethereum/EIPs/issues/650. [Accessed: 09-Apr-2019].

[36] Jim Zhang, “Consensus Algorithms: PoA, IBFT or Raft? - Kaleido - Kaleido,” 2018. [Online]. Available: https://kaleido.io/consensus-algorithms-poa-ibft-or-raft/. [Accessed: 09-Apr-2019].

[37] “Quorum | J.P. Morgan.” [Online]. Available: https://www.jpmorgan.com/global/Quorum. [Accessed: 26-Apr-2019].

[38] nivida, “Web3js Ethereum javascript API.” [Online]. Available: https://github.com/ethereum/web3.js/. [Accessed: 26-Apr-2019].

[39] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, “Ethereum query language,” *2018 IEEE/ACM 1st Int. Work. Emerg. Trends Softw. Eng. Blockchain*, pp. 1–8, 2018.

[40] United States National Institute of Standards and Technology, “NIST Document Sharing Test Facility.” [Online]. Available: http://ihexds.nist.gov/. [Accessed: 27-Apr-2019].