PRIVACY PRESERVING ACCESS CONTROL IN E-HEALTHCARE ENVIRONMENT

By

Muneeb Ahmed Sahi

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences & Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security

June 2018

THESIS ACCEPTANCE CERTIFICATE

Certified that the final copy of MS thesis written by **Muneeb Ahmed Sahi**, Registration No. **NUST201463793MMCS25214F**, of **Military College of Signals** has been vetted by the undersigned; is found complete in all respect as per NUST Statutes / Regulations; is free of plagiarism, errors & mistakes; and is accepted as partial, fulfilment for award of MS Degree. It is further certified that necessary amendments, as pointed out by GEC members of the student, have been also incorporated in the said thesis.

Signatures: ____________________________

Supervisor: **Brig Imran Rashid, PhD**

Date: ______________________ 2018

Signatures (HoD): ____________________________

Date: ______________________ 2018

Signatures (Dean): ____________________________

Date: ______________________ 2018

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Muneeb Ahmed Sahi

DEDICATION

I dedicate this thesis to my family, who are everything to me. To my parents, who have always taught me to be honest and respectful. To my brothers and sister, who have always encouraged me to be at by best and have stood by me through everything. I thank all of them for their endless support and love.

ABSTRACT

e-Healthcare promises to be the next big thing in healthcare. It offers all the advantages and benefits that can be imagined as possible by the patient as well as user: it allows for enhanced simplicity, efficiency, accuracy, access and transparency. However, current e-Healthcare systems are far from developed and mature, thus lack the required degree of confidentiality, integrity, privacy and user trust in order for them to be globally implemented. As with most information systems in their early stages of development and deployment, they lack the required degree of sophistication and completeness to be adopted as a replacement for existing, in place and practiced technologies and services.

Two primary aspects of any operational healthcare enterprise are quality of healthcare service and patient and user trust over healthcare enterprise. Use of modern technology and ICT means that quality of e-healthcare is better than current, traditional healthcare services around the globe. E-Healthcare addresses all performance issues of the legacy healthcare approach. Apart from enhanced overall speed, it also allows for better diagnosis, treatment and record keeping and sharing. Other less defined but equally important aspect of a successful healthcare enterprise is trust. This is the grey area for modern e-healthcare as it fails to dedicate sufficient resources, effort and attention to this. Trust is intertwined with handling of issues like confidentiality, integrity, accountability, authenticity, identity and data management to name a few. Trust, by the patient as well as the user has to be a part of e-healthcare's every aspect in order for it to acceptable and implementable.

Privacy remains one of the biggest obstacles to be overcome in e-healthcare in order to ensure its success in winning patient trust as it indirectly covers most of security concerns. Privacy has become of more and more importance to people due to recent events (data breaches, unauthorized information sharing and usage) and it is taken as an integral part of all things technological and using one's personal information. Addressing privacy concerns imply addressing security issues like access control, authentication, non-repudiation, accountability etc. because end to end privacy cannot be ensured without these. Achieving privacy from sensors end (WSN) incorporating IoT to communication link to data storage and access is a huge undertaking and requires extensive work. Privacy requirement is further compounded by the fact that data being handled in this enterprise is of extreme personal and private nature and its

mismanagement either intentionally or unintentionally could seriously hurt a patient along with future prospects of e-Healthcare enterprise.

To top it all off, legal and compliance requirements vary from place to place, and most of the time are mandatory for e-healthcare providers to comply with in order to handle personal healthcare/identifiable information. These legal and compliance requirements are meant to streamline, standardize e-healthcare industry along with ensuring that sensitive information possessed by these service providers is properly secured, processed, stored, transmitted and shared. This is a huge undertaking for any service provider to be compliant but being in line with these requirements boast patient and user trust which in the end is amongst the most important things for e-healthcare enterprise. Research carried out in order to address privacy concerns is not of truly homogenous nature. It focuses on certain parts of e-Healthcare enterprise failing to fully address all aspects of privacy. There is surprisingly low amount of research seeing into the effectiveness of controls and requirements put forward in legal and compliance requirements (HIPAA, HITECH etc.). In the middle of this ongoing research and implementation, a gradual shift has been seen in shifting of e-Healthcare enterprise controls from organization controlled towards patient controlled. This is intended at giving patient more control and authority over decision making regarding his/her PHI/EHR. A lot of work and effort needs to be put in order to better assess this change and its feasibility in the e-Healthcare enterprise. Research carried out can be divided based on technique being used for ensuring privacy of personal information. These include data anonymization/ pseudonymizing and access control mechanisms primarily for stored data privacy among other techniques. This however results in certain privacy requirements being given a back seat (accountability, integrity, non-repudiation, identity management).

This paper reviews research carried out in this regard. It explores whether this research offers any viable solutions to patient privacy requirements for e-Healthcare and how all privacy concerns of its user (technical as well as psychological) can be addressed. Reviewing research carried out in this regard, an access control model is being presented that aims to provide with the suitable solution to privacy concerns that have been identified in currently presented privacy preservation models.

ACKNOWLEDGMENTS

I thank Allah Almighty for His endless blessings and guidance in leading me to the completion of this work. I am grateful to Brigadier Dr. Imran Rashid, Assistant Professor Mian Muhammad Waseem Iqbal and Lecturer Waleed Bin Shahid for their support through putting their trust in me and generously taking me along. I would like to specially thank Dr. Haider for his continuous support and input throughout the span of this thesis. I thank my all other teachers who have enabled me to pursue studies at this level. I finally thank my parents for their love and support through all ups and downs in life and study.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

PHR	Protected Health Record
EHR	Electronic Health Record
PHI	Patient Health Information
PII	Personally Identifiable Information
HIPAA	Health Information Portability and Accountability Act
GDPR	General Data Protection Regulation
HITECH	Health Information Technology for Economic and Clinical Health Act
ABAC	Attribute Based Access Control
IoT	Internet of Things
WSN	Wireless Sensor Network
BAN	Body Area Network
PDA	Personal Digital Assistant
RBAC	Role Based Access Control
DAC	Discretionary Access Control
MAC	Mandatory Access Control
PCI-DSS	Payment Card Industry- Data Security Standard
PSN	Pseudonym
MULTICS	Multiplexed Information and Computing Service
ICT	Information and Communication Technology
TCSEC	Trusted Computer Security Evaluation Criteria
DoD	Department of Defence

Chapter 1

1 INTRODUCTION

1.1 Overview

e-Healthcare is a relatively new concept in healthcare and medical sciences dating back to the start of 21st century [1]. It envisions an ideal healthcare system which incorporates ICT (information and communication technology) in order to improve healthcare services by addressing the shortcomings of traditional healthcare approach meanwhile enhancing efficiency [2, 3]. It allows for remote patient assessment and views of his/her medical record at any given time and place. It, while making efficient use of ICT allows for complete patient privacy as he/she has the authority to allow or deny anyone access to his records. It dreams a healthcare enterprise that takes into account modern developments in technology as well as social limitations i.e. greying population, need for 24/7 patient monitoring, lack of healthcare personnel and increasing cost of healthcare/treatment. Recent advancements in ICT have made it a possibility that can soon become a reality. However, there are certain issues that are still there to be addressed [4, 5]. Information security's preconditions must be met in these systems as information in these systems is of extreme private nature for patients. Conditions of confidentiality, integrity, availability, accountability, non-repudiation etc. must be met in these systems as total privacy (end to end) cannot be ensured without meeting all these. Strong security measures and control mechanisms need to be set in place in order to gain patient trust. Use of wireless sensor networks (WSN) for patient monitoring creating a body area network (BAN) is a relatively new phenomenon being 1st mentioned at the start of 21st century and has not been thoroughly addressed [6]. Contradictory requirements of low processing and high efficiency against high security needs detailed addressing and a careful balance needs to be struck between these [7]. There is a huge gap in research carried out in e-Healthcare that looks into all aspects of the enterprise. Studies usually focus upon their respective areas rarely looking into other research areas. This results into a solution being proposed that although addresses that particular problem/concern but fail to work overall as a part of the broader enterprise. Arrival of smart phones using a more open operating (OS) system although enhance trust in these systems but they also present new threats and vulnerabilities associated with OS' due to their open nature. Smart phones, socializing applications are becoming an important part of e-Healthcare and adoption of e-Healthcare monitoring and remote healthcare services have become a measure of individual’s prestige and social standing in the society [67]. Legislative regulations, personal risk benefit analysis along with social norms play an important role in one’s perception towards adopting e-Healthcare. Introduction of cloud has brought along its advantages and disadvantages in e-Healthcare as well [8]. According to Forbes, 83% of e-Healthcare service providers are using cloud in some capacity and if this trend continues; in the near future, almost all of the e-Healthcare businesses will employ clouds (Public, private and Hybrid) as a core part of their enterprise. It is imperative to address security concerns originating from incorporation of cloud in e-Healthcare as it already is a core component of e-Healthcare architecture. However, research and regulatory information regarding incorporation of cloud in e-healthcare is lacking. Like many new enterprises, personnel training is lacking along with users and patients limited understanding about their rights and responsibilities in context of privacy, confidentiality, integrity and availability of their healthcare information (PHI/EHR) [73, 74]. Identity theft accounts for nearly half (46%) of all attacks targeting e-Healthcare enterprises [9]. Medical records and healthcare data now has more worth than credit card numbers in black market going around 40-50 USD averagely per record [10]. e-Healthcare enterprises have been a frequent target for cyber-attacks in the recent past for high value of information they possess. Several attacks affecting more than a million users each have occurred in the past five years. Biggest attack on e-Healthcare enterprise caused data theft of around 78 million people [11]. Of all medical data stolen in 2015, 72% was stolen from healthcare enterprises and over 90% of industries have seen a patient healthcare information (PHI) breach [12]. High value of information compounded with relatively weak security in place has resulted in e-Healthcare enterprises facing increasing attacks every year. These attacks and data breaches despite all attempts at preventing them shows that existing policies and frameworks need to be re-evaluated. This has resulted in poor trust on part of its users as despite all measures installed; these enterprises have failed to ensure privacy and security of patients. Such incidents have seriously hindered the growth of e-Healthcare enterprises, not only because of security breach but also because lack of accountability and corporations’ inability to apprehend the culprits. Gradual shift towards patient-controlled healthcare information access and rights coupled with enhanced use of smart phones and devices mean that most of this interaction will be taking place through a mobile (android, IOS) application. How these applications are designed, accessed and secured is another area of concern for e-Healthcare domain [72]. A comprehensive study needs to be undertaken in order to assess unique environment of e-Healthcare enterprise, its threats and security requirements. There exist research articles that explain and highlight security and privacy requirements and reviewing and analysing current research; but there seems to be a gap in flow as there are not enough research articles judging and reviewing research on the basis of given e-Healthcare security and privacy requirements. This study aims at reviewing current research addressing privacy concerns and to assess whether these are of sufficient nature to handle unique privacy and security environment of e-Healthcare environment. In this way, it aims towards fulfilling the gap between e-Healthcare security and privacy requirements at one end and measuring and comparing existing e-Healthcare enterprises and ongoing research to these requirements on the other end. Finally, this study hopes to help various stakeholders and participants in e-Healthcare enterprise development in understanding e-Healthcare issues looking through enterprise prism rather than focusing on individual sections. It is need of the hour for all these parties and stakeholders to come together in order to address these issues and design an e-Healthcare enterprise that is secure, efficient and trusted by its users.

1.2 Motivation and Problem Statement

Advancement of modern technology & its accessibility around most of the world has made it possible remote provision for healthcare services. Existing communication infrastructure can be used along with new generation sensors to remotely assess a patient’s healthcare information & transmit it to the physician. Physicians can also use their cell phones to access the protected health information (PHI) of the patients and prescribe medicine. Tele medical system has provided the leverage of movement to both, patients and physicians. Patients can login to the system to check their medical records, get test results and history of prescribed medicines. As communication between handheld device (PDA, smart phone) and Tele medical information system takes place on the public internet, this makes e-Healthcare system inherently vulnerable to any & all attacks associated with the internet. Since information in such system is extremely confidential & potentially dangerous in the wrong hands, Security/confidentiality and privacy are the main hurdles in making the system acceptable to people. From its emergence several protocols have been proposed to authenticate users like patients and doctors in e-Healthcare system. These protocols are designed to provide certain properties such as anonymity, non-traceability & secure access etc. They also aim to come up with a protocol which provides security against some attacks such as: identity theft or PHI's unauthorized access or any other attacks aimed at compromising its privacy. Research will be helpful in proposing a framework for e-Healthcare system which can resist against above said attacks and contain effective CIA+ security+ privacy.

1.3 Objectives

Following are the objectives defined for this research project.

- Provide a state of the art review of the data privacy techniques for Healthcare environment.
- Analyze the customized environment of e-Healthcare and identify the related privacy preservation techniques; their pros and cons.
- Propose data privacy preservation technique related to patient's health records; physician's knowledgebase and metadata.

1.4 Thesis Contribution

This research comprises of multiple contributions as follows:

- e-Healthcare provides an alternative & effective solution to healthcare needs in our society with limited resources.
- Research will help health industry to introduce e-Healthcare, so the health services can be provided to rural and remote locations of the country.
- Analysis will help other related R& D organization understanding the challenges faced by the e-Healthcare industry.
- It will provide health providers a platform to initiate e-Healthcare services to provide user mobility.
- It will help trust building efforts to make the system global.

1.5 Thesis Organization

This thesis is structured in to six chapters as follows.

- Chapter 1 has covered introduction, overview of research, motivation and problem statement and thesis contribution.
- Chapter 2 contains the overview of e-Healthcare, its architecture, sections and components. It provides a generic overview of what constitutes e-Healthcare enterprise and how it works. It describes data and information flow within the e-

Healthcare enterprise as well as its transmission outside the trusted network. 2nd section of this chapter identifies concerns and issues that are there in the e-Healthcare enterprise which limit its adoptability and widespread use, and which need to be addressed.

- Chapter 3 provides brief description of access control. From earliest models for access management in enterprise to complex, adaptive and comprehensive access control models of today are explained here for building a narrative prior to literature review and solution design and discussion. These include access control models from Bell-Lapadula to RBAC and ABAC.
- Chapter 4 reviews global industrial and governmental laws, regulations and standards that revolve around the issue of privacy, security and confidentiality of information (confidential/crucial user information). Standards discussed include apart from obvious HIPAA, GDPR, PCI-DSS and ISO-27001:2013. It also provides a comparison among them and then concludes what features and guidelines from other standards can be used for healthcare data protection.
- Chapter 5 contains literature review that is carried out to review and assess the current state of research in addressing privacy and security concerns in e-Healthcare enterprise. Literature review has been centred around two crucial aspects of e-Healthcare privacy and security. These are records pseudonymization for ensuring anonymity, and access control for organizing access to these records and preventing any and all unauthorized access to these records.
- Chapter 6 describes in detail e-Healthcare framework that is designed keeping in view existing issues, current state of research, literature review carried out and compliance and regulatory requirements pertaining to e-Healthcare. Framework designed is intended to overcome the limitations and flaws of existing e-Healthcare frameworks that are reviewed during our research and literature review, all the while being efficient and secure.
- Chapter 7 is conclusion of research reviewed, carried out here and framework designed for e-Healthcare privacy and security. It also talks about future work to carry out in order to improve framework designed.

Chapter 2

2 e-HEALTHCARE ARCHITECTURE AND ISSUES

2.1 e-Healthcare Architecture Overview

In order to better understand the e-Healthcare enterprise and its security considerations, architectural understanding of e-Healthcare system is necessary. Currently, there exist a number of e-Healthcare enterprises which are operational. However, there is not a single standard or architectural design that has been followed. Major difference is in handling of patient EHR which in some operational enterprises is patient controlled while other enterprises have dedicated healthcare monitors for managing EHR [25]. From this research’s point of view, a broad architectural understanding of the e-Healthcare enterprise is needed excluding finer details. For this purpose, an e-Healthcare system is presented in figure 3.1 that encompasses all its major components and can be taken as the generic picture, which is applicable to all e-Healthcare systems. Major sections (tiers) of any e-Healthcare system are [13]:

- Core network containing all the information and servers.
- Body area network (BAN) containing sensors providing information about patient healthcare parameters.
- Users of e-Healthcare system those are located at a remote position w.r.t. system’s core network (physician, pharmacist, health insurance providers etc.).
- Communication link that connect all these to form a single uniform system.

In some literature these sections are defined w.r.t. data i.e. PHI/EHR (patient health information/ electronic health record) in order to better understand and address security and privacy concerns w.r.t. data. These are defined as: user sphere (patient and his BAN), joint sphere (cloud service provider and communication link) and recipient sphere (physician, pharmacist, nurse etc.) [14]. Both these defining approaches are addressing the same architecture and privacy concerns but from a different perspective.

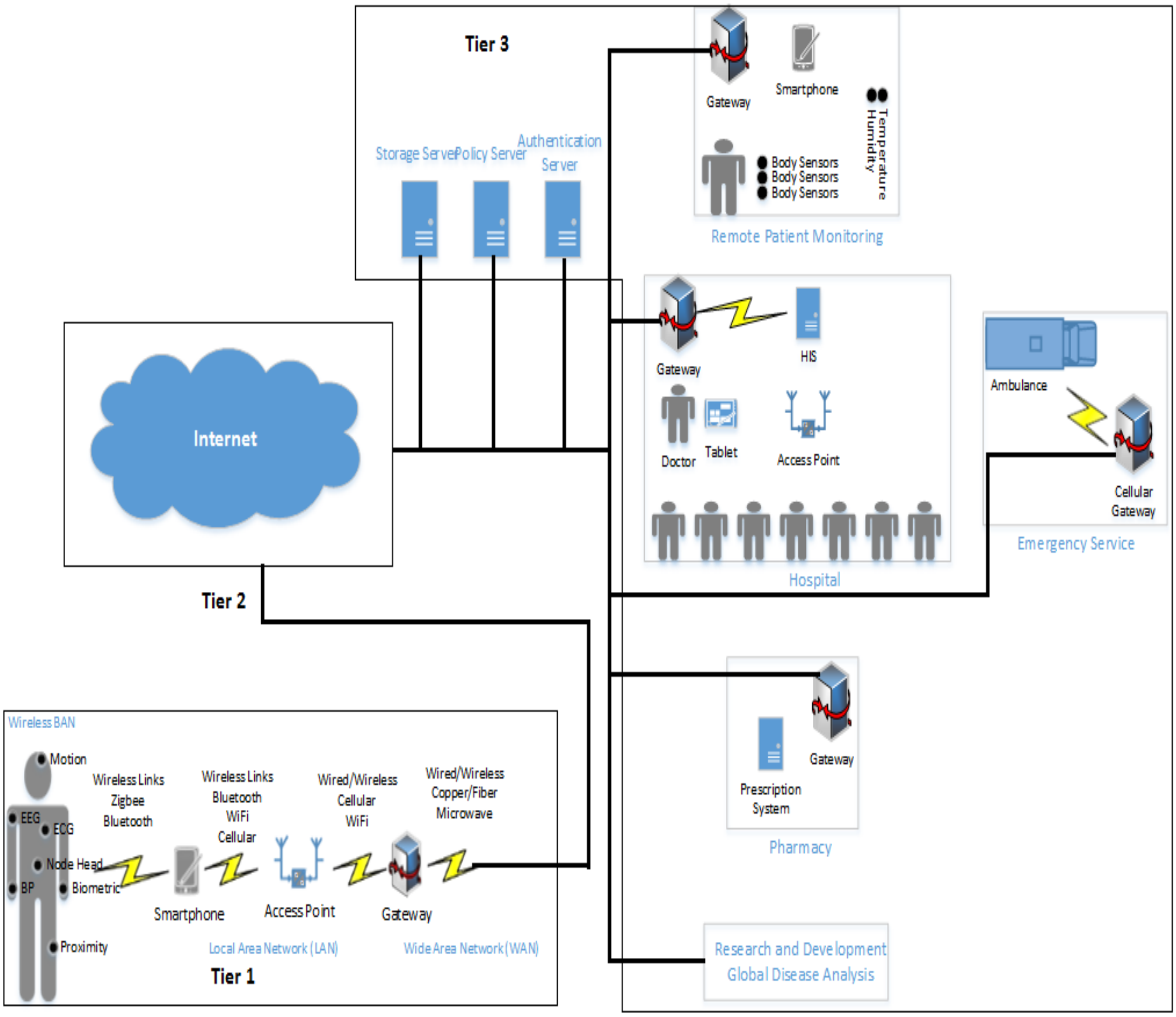


Figure 1: e-Healthcare Enterprise Architecture

Security requirements for all these sections are already defined in detail which encompass both general healthcare as well as technical security requirements. Applying a single security mechanism over the entire enterprise is not feasible as these sections are very different from each other, thus need separate handling [15]. e-Healthcare system needs to be protected from threats at every point from sensors employing IoT to its core network and in between. BAN and its communication link to mobile device have its own threat environment and security measures, which are unique to this section of the enterprise. Mobile device that is responsible for collecting all sensor data and pre-processing and transmitting it to e-Healthcare core network has its own threats and vulnerabilities [16]. These are also compounded by the fact that mobile device is a shared resource which is also used by the patient for his daily activities [17]. Research shows that use of smart phones along with dedicated applications is on the rise and will soon become an essential part of e-Healthcare system. [63] This is along with current popular social media applications being introduced for e-Healthcare social networking. [69] Communication link that transfers all this data from mobile device to the core network and connects all remote users to it employs security measures best suited to it (encryption). Once data securely arrives at the core network safely and securely, its protection, privacy preservation, processing and proper distribution comes into play. Prior to this stage, data confidentiality and privacy are somewhat similar as no one is supposed to see the data. Now however, access control, user anonymity and other privacy preservation requirements are needed to be met. Now a distinction is to be made between those allowed access to health records and those who are not. And more importantly, who is allowed to see patient centric information (name, ID no. etc.) and who is allowed to see his healthcare centric information (PHI). e-Healthcare is already being deployed in various regions in the world. With certain notable exceptions, these enterprises have vulnerabilities and flaws that have been exploited in the past compromising not only patient information but also putting mistrust among their users. Few successful e-Healthcare enterprises, however do not address privacy and security concerns in an end to end fashion but focus more upon access control of stored data. They do not look into accurate, timely collection and correct, efficient transmission of data to the healthcare database [73].

2.2 e-Healthcare Issues

There are a number of challenges that arise due to introduction of ICT, IoT and cloud in the e-Healthcare environment. Including legal requirements (HIPAA) that are to be met in any successful e-Healthcare enterprise, a long list of issues comes up. Crucial among those are [19, 71, 77]:

- Architecture Security.
- Device management (PDA or smart phone handling BAN).
- Sensor security.
- Data Protection (Confidentiality and Integrity).
- Incident Response.
- Identity management and Access control (Privacy Preservation).
- Identity proofing (Authentication).
- Legal and compliance issues.
- Auditability of the enterprise.

- Privacy for entities other than patients in e-Healthcare enterprise.

Although e-Healthcare systems are intended at improving healthcare quality while reducing its cost, it also brings into light new issues concerning patients with it. Issues that to be addressed are of IoT, communication link, cloud storage and access control; both individually as well as when combined together to form the e-Healthcare enterprise. Patient data of extreme confidential and private nature can be compromised at any point from sensors to cloud storage which requires a vigilant security mechanism to protect it from all threats [20]. Security threats to e-Healthcare system can originate at any level. These can be of varying nature: architectural (sensors, PDA, communication, cloud), managerial (weak policies and access control) or software (application). Each and every layer, component of the e-Healthcare system needs to be secured. 1st challenge in this regard is designing the hardware i.e. wireless sensor network (WSN) and communication link from patient to the hospital. Ensuring secure and efficient transfer of data from sensor's body area network (BAN) to the core of e-Healthcare system is crucial. Securing end to end communication from BAN to the core network has its own security threats and vulnerabilities. Although their security objectives are similar as any other part of e-Healthcare system (confidentiality, integrity, availability etc.), but threat perception and mitigation is IoT (internet of things) centric thus needs specific understanding and handling [21]. There is a serious lack of research being carried out on managerial and compliance aspects of WSN and IoT. Lack of standardization regarding this end of e-Healthcare enterprise means serious interoperability issues for e-Healthcare service providers. Data protection while being transmitted or stored at server is another very important security concern. Strong data encryption techniques along with rigorous authentication mechanisms need to be integrated in e-Healthcare system. It is observed that most of the patients will want to use their existing mobile devices as a link between BAN and core e-Healthcare network instead of using a dedicated mobile device (which is security wise feasible). Use of shared resources (smart phone, internet) makes the system inherently prone to threats and vulnerabilities of these resources (applications, operating system, protocols) [22, 23]. Data storage, sharing and access at server is often less focused upon area of e-Healthcare. Existing security measures already in place at various operational enterprises and servers were deemed sufficient for providing security, confidentiality and other functions when deployed in e-healthcare. This statement even though true for the most part still needs modifications to address unique operational and compliance requirements of e-Healthcare enterprise. This requirement is further compounded by adoption of cloud at back end which introduces issues pertaining to cloud into already troubled e-Healthcare enterprise [70].

Privacy is perhaps the single largest hurdle facing e-Healthcare service providers from implementing it in large capacity and gaining patient trust. This is because for an ordinary patient this is the only thing that makes a sense to him and concerns him directly, although this may not be the case in reality. This trust deficit between the system and its users can be overcome by giving patient control over rights to view and share his health records with others. Another factor highlighting privacy is that legislation concerning healthcare in general and e-Healthcare in particular puts more emphasis over patient's privacy. Among existing e-Healthcare enterprises [24], most widely used approaches regarding handling of Patient healthcare information (PHI) are user oriented where patient controls and manages his PHR while on the other hand, in clinic centred approach, a caregiver is designated to manage PHR. Most desirable scenario in this regard is a patient having control over access to his medical information because it is control rather than ownership or possession over data that defines privacy [25]. A rigorous privacy preserving mechanism is needed in order to ensure patient's privacy; his identity, medical record, financial record w.r.t. ongoing diagnosis and treatment. Inability of service providers to come up with a resource efficient and effective privacy preserving approach in order to ensure patient's complete anonymity is the single biggest reason for patients not being comfortable with it as they do not trust the service provider's security and privacy mechanisms installed to protect their privacy. HIPPA and HITECH are certain requirements defined by US government that e-Healthcare service providers need to meet. These are meant to ensure that sufficient measures are placed by service providers to meet security criteria deemed significant for patient's information security [26, 27]. Definition and criteria set for privacy in healthcare are more of legal sort to which a technical answer is needed. Following definition explains privacy precisely:

"Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" [28].

Privacy in e-Healthcare is a more challenging issue to address as compared to others because: [64, 74]

- Duration for which data is collected may span over days, weeks which results in patient everyday routine being learned by e-Healthcare system.
- Data collected is not of purely physiological nature but also of habitual nature i.e. patient diet or daily activities.
- Data collected is often shared among various sections i.e. health insurance and research.
- Perception, preference, and requirements regarding privacy vary among individual users, genders, ethnic and cultural groups.

It has been noted that research regarding e-Healthcare in the recent past (2010-15) has focused more on access control and data confidentiality while ignoring many critical aspects like privacy, anonymity, auditability etc. [66]. recent research has also pointed out the need for addressing security concerns for the smart phone/ PDA interface for patients and users. This call for platform security and development concept of security by design which incorporates security in planning and development phase [62, 66,78]. Recent studies have shown that lack of standardized security and privacy policy implementations has resulted in disruptions in e-Healthcare enterprise. Extended focus on theoretical requirements and implementations has resulted in unintended unavailability of information, workflow disruptions and operational feasibility issues [68]. This coupled with limited or no collaboration among various stakeholders and poor focus on overall picture of e-Healthcare enterprise has resulted in very limited progress towards an efficient, if not ideal e-Healthcare enterprise [72, 80]. It must be noted that an emergency healthcare provision mechanism is needed as well for any e-Healthcare system to be viable. Emergency mechanism in e-Healthcare will allow for bypassing of rigorous security mechanisms in place in order to provide emergency healthcare. This also opens a potential window for exploitation where emergency mechanism is triggered by the attacker to bypass security. So, a careful balance is needed to be struck which provides security to emergency mechanism to prevent is misuse while allowing for its invocation when needed [29].

2.3 Summary and Conclusion

e-Healthcare being an emerging domain has a lot of issues in its operability and security. Introduction of IT in healthcare brings challenges that are unique to healthcare environment. Information security is crucial for e-Healthcare environment since nature of information being processed and stored is private and personal. Technology in healthcare aims at improving the overall healthcare experience for patients and doctors alike. It is essential to ensure safety and security of such an enterprise to enhance its usage. Meanwhile, privacy awareness has been increasing among individuals which has led to several national and international regulations and laws being enacted and enforced. Any new mechanism for e-Healthcare being proposed has to take into account these legal requirements as well to be practical and adopted.

Chapter 3

3 ACCESS CONTROL: UNDERSTANDING AND USAGE IN e-HEALTHCARE

3.1 Introduction

Access control is at heart of modern information systems. It is now the central part in information world ranging from an individual system to complex enterprise wide systems comprising of thousands of systems, users and millions of files. It is the centre piece that allows upholding of core principles of confidentiality, integrity and availability (C, I, A) along with other critical factors like non-repudiation, security and authenticity. By providing and defining only useful access to read and write, it ensures confidentiality and integrity. Availability is ensured by allowing access to authorized personnel only and thus preventing unauthorized, malicious people from damaging the system. Access control is the result of understanding on part of the world that security (identification and authentication) alone cannot ensure a successful, easy to use and manage, and acceptable to the world system. Even it could be done, underlying risk originating from the threat that security system could fail is too huge to accept or more accurately ignore. It is a bad practice to put all your eggs in one basket, or in case of security, to rely on a single security mechanism for entire enterprise. This is where access control comes in which not only provides another level of security but also adds accuracy, efficiency and easiness.

An information system consists of three primary tiers: People (subject), process (operation) and data (object). Access control is the security policy which determines if any subject is allowed to perform an operation on any object. This access to perform actions based on security policy is called ‘permission’. For each of these are three factors regarding system usage: Read, Write and Execute. Another dimension in this regard is creation/deletion of data and its sharing with others. Access control is the matrix that connects these dimensions to give a three dimensional, compact and complete rule set defining access rights based on factors for all users, processes and files which are often in thousands. Thus, Access control can be defined as:

“Process of determining an object’s permission to perform operations on objects based on a defined security policy”.

Access control is core on which protection systems in today's world are built. State of all processes, users is defined, and it is written down as to what processes can access what resources and execute what programs. However, it needs to be remembered that even though, access control is the corner stone of today's security structure, it alone cannot be the guarantee for protection of information system from three dimensional threats it faces. It is always combination and synchronized operation of multiple security features and tools that result in a secure and efficient information system.

Access control works on multiple levels in a system. Multiple layers of access control allow for a degree of isolation between them but still remain connected to form access control system. Level of complexity and details is different for each access control level.

- Highest and closest to a user are application control mechanisms which directly interact with the user. These are very complicated and represent a complex and in-depth security policy. Taking a financial institute using internet i.e. a bank: Application could allow for a user to be assigned a role from dozens of available roles. Each role will have a certain profile which means that it will have a defined set of rules, access to certain data, ability to execute certain programs, write certain fields of data, and perform certain transactions. This role will have a defined picture that will be central to security and all actions from a user in this role will be within the confines of this role. There could be a case where identification+ authentication as well as verification/approval from some third party might be needed. This third party can be different role within the system or can be someone in another system.
- Applications usually are written on top of a middleware which has certain rules and regulations defined within it, at backend of the application. These are the protection mechanisms of the system. These rules are inherent part of the application running on the top most layer. These are often the actions that are performed after certain activity in the application, without users prompting them. In case of our example of online banking system, banking application will be running on top of some sort of data management system. This data management system will have certain rules which will transform in the application running on top of it. If there is a transaction in debit ledger of the

bank application, data management system could define the rule to credit that transaction amount in another ledger for enhanced security.

- Middle ware which lies between application and operating system (OS) relies on OS to provide necessary facilities needed for the application to function. It requisitions applications required resources like communication port for internet access, files and memory (RAM, ROM) for reading writing of data and execution of functions. It is its responsibility to manage and control access for resources it has acquired from OS for application.
- Operating system is at the edge, between application and middleware above and Kernel and hardware underneath. Access control for an OS relies on hardware features and the memory management hardware associated with it. These define at the most basic level access for application i.e. memory address access for various processes being initiated by the application.

It is clear from this example that access control's complexity increases as we move away from OS towards application. Controls will be more complex at application level when compared to control on OS level. Complexity in control results in lack of full understanding on part of security practitioner about all aspects of these controls. This makes them less reliable and more prone to abuse. One of most occurring failure of access control functions is due to their complexity and underlying ambiguity. People being managed through these complex access control rules find some features which can be exploited to break free from access controls to perform actions or access information otherwise off limits to them. This does not mean that complex access control rules offer a disadvantage w.r.t. security and are unable to perform well. Need is to fully understand these controls and ensure that all possible situations are being covered.

Given how complex are today's information systems, it is not possible to understand a system from security, operational or any other perspective while looking at any one part. Like building blocks of an elaborate structure, it makes good sense only when it is being seen, used and studied in context of the entire enterprise system. Like other security related aspects in the IT world, access control and security policies were not an implicit part of early DOS, 95/98 systems. Even though, there were explicit, clearly defined security needs of system users, these were not defined in the OS of those early days.

3.2 Access Control Principles

Access control was first developed and introduced by US DoD in 1960's when they developed and started using distributed systems. It allowed having a methodology in place to control and manage access of shared resources among various users within the DoD. All the basic principles and initial models were developed in this regard and were focused on particular circumstances, rules and structure of the environment these were to be implemented in. This led to development of multilevel access control where access to resources was defined based on confidentiality level of resources. Rules were also defined and put in place to manage access levels and controls for resources that were being shared or moved among users with different levels of access. We explain these principles of access control before going towards recent, advanced access control techniques.

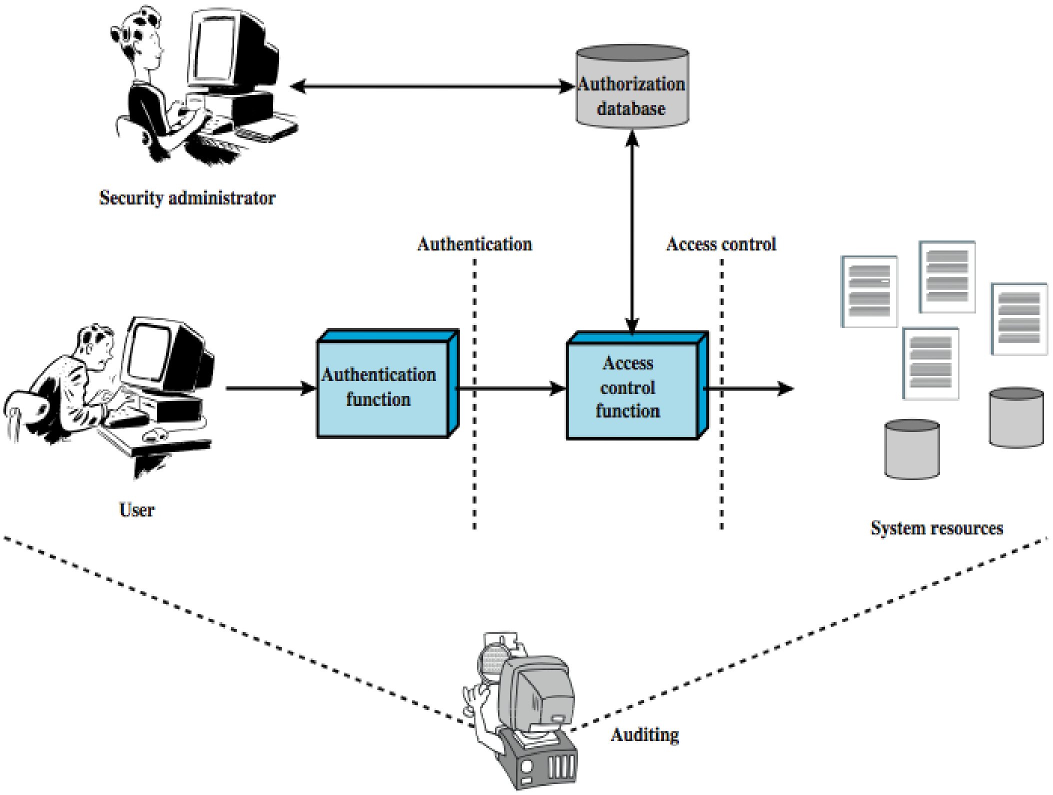


Figure 2: Access Control

3.3 Bell-Lapadula Model

Bell LaPadula model was one of the 1st models that dealt with the notion of selective access to perform operations, objects for subjects based on their state (attribute or level). It was proposed more than three decades ago and has been the source from which inspiration and knowledge has been gained by models that have followed. It allowed for security states and policies of an information system to be formally (mathematically) defined which allowed for full understanding of their operations and abilities. Mathematical representation meant that their limitations could also be brought to light without having to implement them.

Before understanding and explaining the Bell LaPadula model, basic concepts are needed to be understood. Bell LaPadula is designed on basis of state transition model for multilevel security model in place in US DoD, where system state is transitioned based on input and idea is that in case of an accurate system starting from a secure state, it will remain in secure state for all possible inputs to it.

- State: A time based representation of any system at any time.
- State Transition: Change in system state due to any external or internal input.
- Principle of any secure, feasible system is that: if a system started in a secure state, any and all changes to it due to input will lead to a secure (stable) state.

Being an early model for access control in a relatively complex and newer environment, Bell LaPadula model does not distinguish between notions of security and protection whose definitions have become clearer over time. Protection is the mechanism for securely operating the system while security is the policy enforced in/by the system for it to work as desired. One of its major flaws that is also apparent in many older models as well is the fact that these do not take into consideration three dimensional requirements of information security namely confidentiality, integrity and availability commonly dubbed as CIA triad. Bell LaPadula model focuses on data’s confidentiality and to a lesser extent, its integrity but does not cover the entire CIA triad.

Essence of the Bell LaPadula model is various levels defined w.r.t. security clearance or level of trust and access to the system for the users. These levels in any direction represent gradual change in access/trust levels. As Bell LaPadula model was being researched and ultimately used by the US military, access levels were defined using terminologies familiar to them: Top secret, secret, classified, not confidential. These security clearance levels define access for users. Permissions to perform various actions (read, write) are defined for individuals in any one direction. For Bell LaPadula model, due to its access directions is also known as write up- read down model.

3.3.1 Read Down/ No Read Up

To prevent user from accessing/being able to see data beyond/above his security clearance.

1st goal of bell LaPadula model was to preserve system's confidentiality by maintaining system's security clearance levels and access accordingly. In other words, any user who has a certain security clearance level cannot read any data that is marked at a security level higher than his.

- User having 'Top Secret' clearance can read all data in the system as he has the highest security clearance.
- A user having the lowest clearance level (Not confidential) cannot read anything other than that marked as 'Not confidential'.
- User having 'Secret' level security clearance will have access to all data except that marked as 'Top secret' since it is above his security clearance.

'Read Down/No Read Up' aspect of Bell LaPadula model was termed as simple security policy by the writers as in essence, it alone could suffice confidentiality requirement of system, but it was very easy to bypass and exploit this. System for which Bell LaPadula model was designed was dubbed as MULTICS. In it for each file, an access control matrix was defined that defined its security clearance level w.r.t. each user in the system. So, whenever a user tried to read/write or otherwise access a file, system will check for that user's security clearance level and compare it with file's security clearance level for that user that has been defined in the access control matrix of that file. If user's security clearance level is equal or higher to that defined for the user in the file's access control matrix, he/she will be allowed access to perform system's acceptable actions on that file. If this is not the case, user will be denied access to the file.

3.3.2 Write Up/ No Write Down

To allow user to communicate/being able to send data below/underneath his security clearance.

Implementing simple security policy alone cannot ensure confidentiality of the information marked as having higher levels of security clearance requirement. A hypothetical scenario in this regard can be a user with malicious intent having top secret clearance reading content of a file requiring top secret clearance and then, creating a file with not confidential security clearance, and finally copy data from top secret file. In this way, a user can bypass the simple security policy and put the system and its files at risk. 2nd Bell LaPadula principle prevents this from happening.

- A user having security clearance of ‘top secret’ cannot write to anyone other than a user having similar security clearance i.e. Top secret.
- A user having the lowest security clearance (Not confidential) can write to every user as they are either on security level equal to him or higher.
- A user with security clearance level ‘Secret’ can only write to users with ‘Secret’ or ’Top Secret’ clearance and cannot write to users with clearance levels ‘Classified’ and ‘Not confidential’.

3.3.3 Trusted Write Down

To allow certain TRUSTED users to write information down towards lower security levels.

By relying on two core principles of bell LaPadula: Read Down and Write up, all information flow is upwards and is centered there which will not be dispersed, shared with users at lower security levels. This is a flaw as in some exceptional cases, information needs to be written down. To address this issue, Bell LaPadula introduced the notion of trusted user. It is a user that is allowed to write down in order to convey that critical information that has to be passed down the security levels.

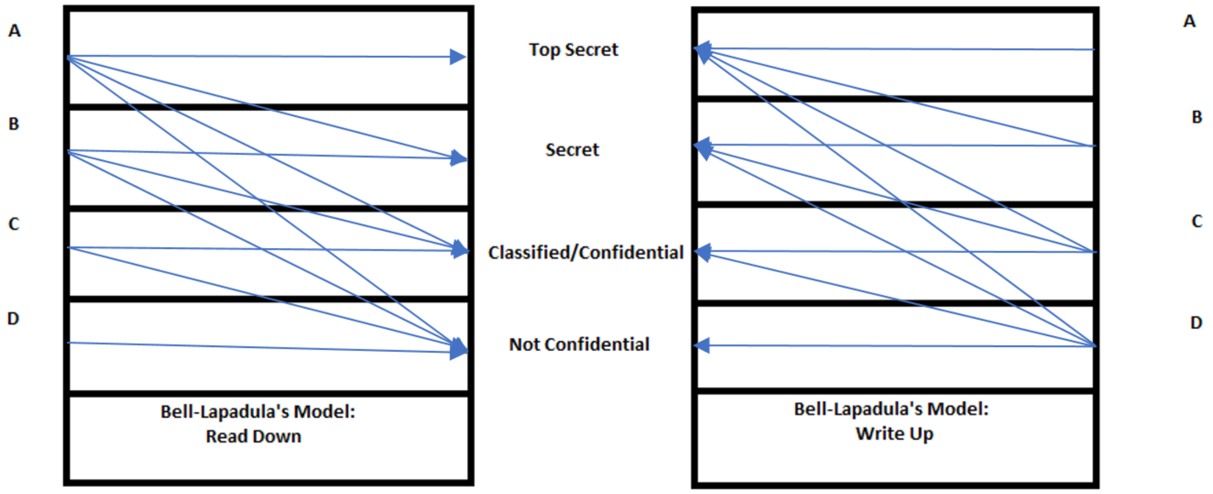


Figure 3: Bell Lapadula Model

3.3.4 Mandatory Access Control (MAC) Attributes

Mandatory access control is still a part of access control systems in today’s world. It has certain features that make it unique, and these features are still applicable to different parts of today’s systems.

Following are the main factors of Mandatory Access Control (MAC) that differentiate it from other access control models.

- Data Owners do not have the authority to define or change an individual user's security clearance level. Administrator, person who is responsible for managing the system and has the highest authority in performing various tasks is the only person who is allowed by Mandatory Access Control (MAC) to manage individual user's security clearance.
- All data in the system is assigned a security level that reflects its relevant security and confidentiality value. This in turn, is detrimental in system user's access to this data.
- Users are allowed to read data that has a security classification lower than them.
- User is only allowed to write data that has a higher security classification than them.
- Read as well as write access for users is limited to their own security clearance level.

3.4 Biba Model (Read up, Write down)

Biba's model or more commonly referred to as Biba's integrity model was system security model that focused on data's integrity preservation as the name implies. Data's integrity is ensured by limiting and controlling the number of people who are allowed to access data to modify it in any way. Unlike Bell LaPadula model that defined access rules on the principles of 'Write up, Read down', Biba's integrity model is characterized by the phrase 'Read up, Write Down'.

To take as an example for use of Biba's integrity model, example of an application code can be used. It needs to be visible to all users from high end application architects to low end developers. However, only senior resources (application architects) can be allowed to edit any code it has. Allowing low end users (developers) to modify application code can not only jeopardize code's integrity but may also result in errors resulting in application's failure to perform its intended functions.

3.4.1 Read Up/ No Read Down

- An application being used or developed, must be visible to every developer and user within its domain. For this to occur under Biba's model, application source code is placed at highest security level which means that everyone within that domain can read it.

- A user with security clearance level of ‘secret’ will have access to read data placed on levels ‘secret’ and ’Top secret’.
- A user at the lowest security clearance level ‘Not confidential’ will be able to read all data in the system.
- It will be more accurate and understandable to see and describe read, write access to users with regards to data instead of users. This will make Biba’s model more realistic dealing with integrity of data while ensuring sufficient access to users who need it.
- Data or code that needs to be accessed by developers and testers for their work on the application will be placed at a clearance level that is equal or above developers and testers clearance. In this way, they will have the access to the code but people with clearance level above it like managers will not have access to read the code.

3.4.2 Write Down/ No Read Up

- In the similar scenario, users with higher level of clearance will need to have the ability to pass down instructions, requirements and suggestions on ongoing work.
- To cater for this, user with higher security clearance i.e. manager is given the authority to write down wards to the people at lower clearance level.
- This allows people at higher levels to pass down client requirements and instructions to lower end users like developers and testers that define the requirements and expectations of clients and management.

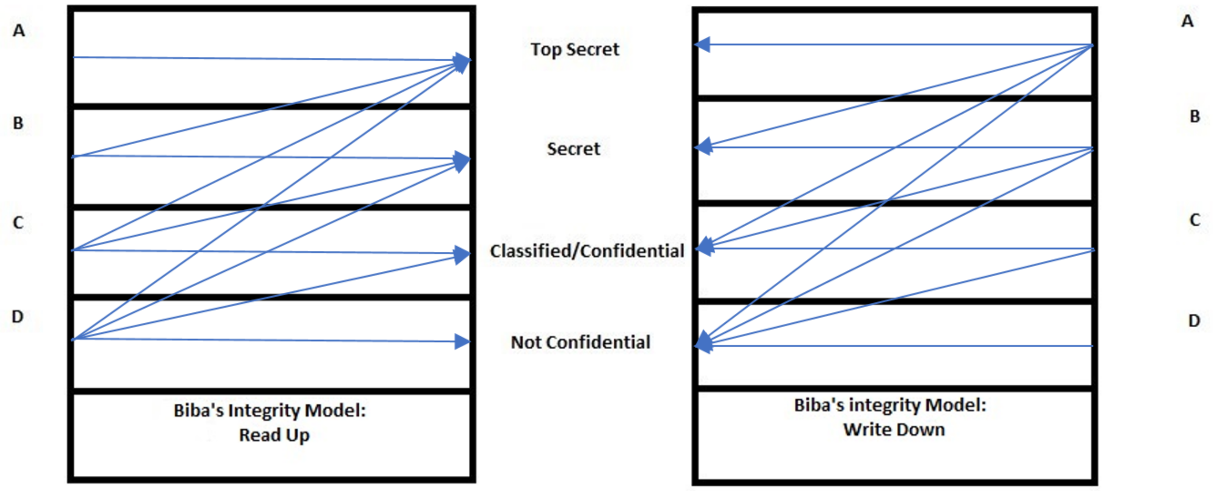

A
B
C
D
Top Secret
Secret
Classified/Confidential
Not Confidential
Biba's Integrity Model: Read Up
Biba's integrity Model: Write Down
A
B
C
D

Figure 4: Biba Model

3.5 Clark Wilson Model and Chinese Wall Policy

Clark and Wilson's model was an access control model introduced to manage operations especially transactions in a financial institution effectively and securely. Like all initial access control models, its primary flaw was similar to that of those in the same timeline; as it did not address all aspects of information's security i.e. confidentiality, integrity, availability more commonly known as CIA triad. Its focus was on in single direction of ensuring accuracy and integrity in financial operations in institutions. Two core principles that Clark Wilson revolved around and were the corner stones of the access control model were: "Separation of Duties" and "Well-formed Transactions". Separation of duties is now taken as an implicit function of all security and access control systems these days.

Similarly, Chinese Wall policy was focused on financial transactions and introduced another critical rule for security and operations. "Conflict of Interest" in operations and transactions occurring in financial institutes was identified and highlighted by authors of Chinese wall policy.

3.6 Limitations of Classical Access Control Models

As with all things in IT and technology world, initially they were developed with individual goals in site and focused on them. They did not offer three dimensional solutions to problems and were not advanced or complex enough to handle other than ordinary situations that were to arise. Initially, development, research and future projections were not mature enough to put out a product strong enough to be sufficient to needs that it was being designed to handle. Major issues that were in these classical access control systems that resulted in their failure were:

- These access control mechanisms were usually designed with focus on individual aspects of systems and their requirements, thus were limited in applicability to those particular systems.
- Central requirements around which information security revolves (confidentiality, integrity and availability) were not addressed. Each access control model focused on individual security requirements instead of focusing on all of them. Systems that were excellent at ensuring information's confidentiality were proportionally poor in managing other aspects of information's security (integrity and availability).
- These access control models were not flexible, and their rugged nature meant that they could not evolve with emerging technologies, hence were outdated and discarded.

3.7 Operating System (OS) Access Control

Access control is always invoked after a user has authenticated him/her self to the system. Passwords or Kerberos are the commonly applied authentication mechanisms in an OS. Once user has been authenticated, access control is invoked to determine as to what resources, processes, files can be used/called upon by the user. Every action of user is within the confines of access control rule set, whether it is access to some data, or calling upon a program or requesting a communication port for access to internet.

User	Operating system	Accounts program	Accounting data	Audit trail
Alice	RWX	RWX	RW	R
Bob	X	X	RW	-
Sam	RX	R	R	R

Figure 5: Basic Access Control List (ACL)

In case of above access control matrix, three users Alice, Bob and Sam are defined. Four processes in this matrix are OS, accounts program, accounting data and audit trail. Access control matrix defines rights for each user w.r.t. all these processes. By correlating columns and rows, access rights of a user for a particular program can be determined. In this matrix, Alice is the system administrator and has access to read and write everything except audit trail. Audit trail is always “read only”, no one is allowed write access to the trail. Audit trail is meant to log all activities within the system to ensure non-repudiation, analysis and track and identify any unauthorized access or activities by users. By allowing “write” access to audit trail would defeat its purpose of allowing for recording of system and user activities as any user could overwrite log of their malicious activities. Note that apart from Alice who is the system administrator, only Sam is allowed to read audit logs which is necessary for him to perform his job of being an auditor. Bob being not a special user is not allowed to review audit logs. Bob is the manager who needs to execute the accounts program and read, write its data but within the defined specifications of the program. This is why he is not allowed to read, write anything in the OS or the program. Since it is not Bob’s responsibility to review logs, he is not allowed access to them in any way.

Above table is for understanding the basic concept of access control matrix only and is not totally realistic. In an access control matrix that is based on real world scenario, book keeping program that was given as an example at the start of this chapter, program also needs access to certain functions, tables to keep transactions balanced and up to date. As mentioned above, in case accounts program is intended to credit all transactions into a separate ledger in case of all transactions in debit ledger by the user, or in this case, Bob the manager. This will be done by adding an additional row highlighting access for accounts program in the access control matrix. Note that accounts program is allowed to write audit logs. This will allow for all activities performed through accounts program to be logged which will be reviewed by Alice (system administrator) and Bob (Auditor).

In a real-life system, there will be multiple programs along with thousands of users and hundreds of processes. Access rights will be defined for each and every one of them: all users as well as all programs w.r.t. all processes within the system. For purpose of creating audit trails to review activities within the programs and system, these programs are the only ones that are allowed access to right into audit trails. Blank, no value from r,w,x in any field in the access control matrix means that, that particular user or program is not allowed any kind of access to the particular program/process.

User	Operating system	Accounts program	Accounting data	Audit trail
Alice	RWX	RWX	RW	R
Bob	X	X	RW	-
Accounts Program	RX	R	RW	W
Sam	RX	R	R	R

Figure 6: Advanced ACL

Another way to designate access in any system is use of user triples comprising of user, program and data/file. However, our focus is towards understanding and identifying a successful access control mechanism rather than drifting towards various methodologies to display this access control.

Now that access control matrix has been understood, it needs to be understood that it is not a practical and feasible approach towards managing access in a large or even medium sized enterprise. For example, in a system consisting of 500 employees and 20 programs/processes will be need a total of 10,000 entries to complete its access control matrix. A figure which is huge and jumps to 10,00,000 in case of a large organization comprising of 5000 employees and 200 programs/processes. Such a large access control matrix is problematic as it is not only processing intensive but also prone to mistakes on part of the system administrator. What we need is a more realistic, compact, efficient, quick and easy to manage way to store all access control parameters. Most used access control methods for this has been either role/group based, or ticket/certificate based which are explained in detail below. Most widely used and effective access control methodology over the years has been Role based Access Control (RBAC). Here, different roles or groups are defined, and access is granted based on roles. Each user is member of at least one role. Access rules are defined for individual roles instead of individual users. Since number of roles in any information system is far less than individuals, it is easy to manage, define and operate.

3.8 Role Based Access Control (RBAC)

Access control, information systems and multilevel security were all result of research by US DoD. They used mandatory access control (MAC) for managing access within defence department where confidentiality of data was of utmost importance.

Discretionary access control (DAC) on the other hand was more commonly used in civilian side and gave a bit of authority to individual users to define access rights for files and processes they owned. However, information systems had come a long way from their early and simpler structure in 1970's. In early 1990's it was felt that MAC and DAC were no longer able to manage access in ever increasingly complex information systems and environment. New type of access control was needed to manage these systems. Role based access control (RBAC) was introduced in 1992 with notion that MAC/DAC are no longer effective or manageable. RBAC was the 1st access control mechanism that was truly global in its information access and security aspects. Before RBAC, standards and research focused on US DoD's needs and were driven in that direction. This meant in negligence of non-military needs and narrowed down the work. These standards focused and addressed concerns raised by the military, were designed and more suited to such environments, but they could not efficiently work in other non-military environments.

RBAC was the 1st standard that focused on giving a global access control platform that could address concerns of all stakeholders and was flexible enough to be used in all sorts of information environments. It was the 1st wide adopted access control mechanism that handled security in all three dimensions: confidentiality, integrity and availability. Role based access control has been the choice for managing access in information systems for more than two decades now. It has come a long way from its initial form in 1992 and has evolved over time. Today, most of information systems and access control methods are based on role-based access control. Very recently, it has been felt that RBAC is lagging w.r.t. new innovations in technological world. Introduction of IoT and Cloud has raised problems for which RBAC does not seem to have an answer. Newer access control mechanism has been proposed (attribute-based access control) but it will take a long time for it to mature and further some time to be implemented and be a replacement for role-based access control.

3.8.1 Weakness in DAC and MAC of TCSEC

Trusted Computer Security Evaluation Criteria (TCSEC) was the security standard for managing access in US DoD's information environment. It was introduced in 1983, was combination of Discretionary and Mandatory access control (DAC, MAC) and is still among the well-known standards originating from military. Problem with TCSEC is rooted in its objectives set out during its designing. Goal of TCSEC being for the military was the need to protect information from unauthorized access to read/write.

This was from the fact that in nature of military affairs, information is of utmost importance and is often confidential. Sole object is ensuring information’s confidentiality which means access to see information is restricted and is being strictly controlled. TCSEC works very well in ensuring information’s confidentiality in such environment however, environments that do not operate in such strict environment and do not process information of such confidential nature cannot be managed by TCSEC. This means most of the public bodies utilizing such access control systems cannot manage access appropriately. So TCSEC security policies and protocols are in the dark when it comes to managing information that is not confidential but still needs to be managed among users in a system. TCSEC consists of MAC and DAC. Two access control mechanisms offered were suitable for multilevel military environment and civilian environment respectively for over a decade. But these did not offer the versatility needed to work in ever complex information environments.

3.8.2 Understanding ‘Role’

“A role is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role”.

As described earlier, maintaining access control lists or matrices is not feasible in case of large organizations with numerous users, functions, resources and job responsibilities. However, number of roles: types or categories of users, functions and responsibilities is always limited. Role is the job function that fits for a specified group of people within the organization. Assigning individuals into combined groups based on their ‘roles’ within the organization addresses the issue of managing access control profiles for too many users. Reason behind extensive use of RBAC and its success in handling most of the responsibilities in small, medium enterprises as well as large organizations with thousands of employees, is the fact that it did not most of the design flaws that were there in classical access control systems. It allowed easy management of the large organizations, allowed use of MAC and DAC for certain aspects of access control where they were suited, it considered entire CIA triad for information security in access control systems, addressed principles of ‘conflict of interest’ and ‘segregation of duties’ as part of RBAC.

Role based access control is unique in its assigning of access rights as it does not assign rights to individual users but to the roles that they have been assigned. This offers a number of advantages over older approach of assigning access rights to individuals:

- Individual can be assigned multiple roles based on needs of individuals.
- Individual can switch between roles to perform tasks as needed.
- Inability to combine privileges of multiple roles assigned to an individual makes access control more manageable and ensures non-repudiation in case of audit logging as user's switching among roles is logged.
- Allowing multiple roles to an individual and structuring RBAC in a way that user has to switch between roles based on needs to his tasks, eliminate the threat of privilege escalation.
- Instead of defining and writing access control permissions in access control matrices and lists for any new user, function or resource, RBAC allows for defining it within the specific role that needs access to these files or services. Same goes for changing access control permissions within the system.
- Option for defining new roles and assigning it to users makes RBAC flexible and versatile as indefinite roles can be defined based on system requirements as they arise.

3.8.3 Understanding RBAC Working

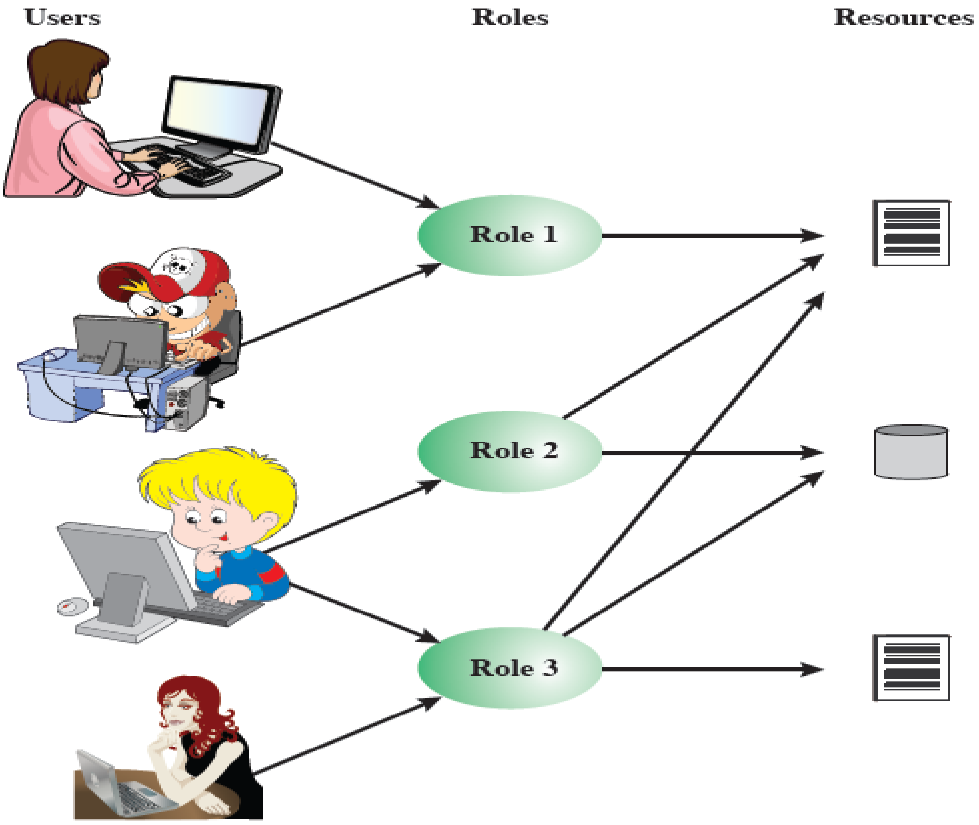


Figure 7: Role Based Access Control (RBAC)

As described earlier, and evident from above figure depicting role-based access control scenario (RBAC), RBAC's operation and access management is built upon 'role', job function of sorts for people within an organization. Roles define job functions in an organization, and their assigning to individuals is an indication of how things work there. RBAC has been almost universally adopted throughout the world and is perhaps most popular and widely used access control mechanism now in the world. National institute of standards and technology (NIST), premier US body responsible for standardization of various industrial and commercial technologies and tools has published its standard on cryptographic modules FIPS 140-3, that requires support for RBAC for administrative and access management activities.

Unlike DAC and MAC where relationships between user (subject) and resources (objects) defined the access control parameters, RBAC is three tiered: role is the middle tier between users (subjects) and resources (objects). Relationship between user and role, and relationship between role and resources are the decisioning factors in access control management. Unlike DAC and MAC, where ACL or AC matrix was the single entity for deciding and defining access control; access control in RBAC is result of two: combination of users and their assigned roles, and roles and their assigned resources. To allow for more flexibility and ease of management, RBAC allows for one to many relationships between users and roles: a user can have more than one role based on their job need. Added advantage of this is the fact that number of roles needed to be defined for access management is reduced greatly, which otherwise would require too many roles to manage thus affecting its reliability and efficiency.

In RBAC, there are two matrices that express the access control within the RBAC managed organization/system.

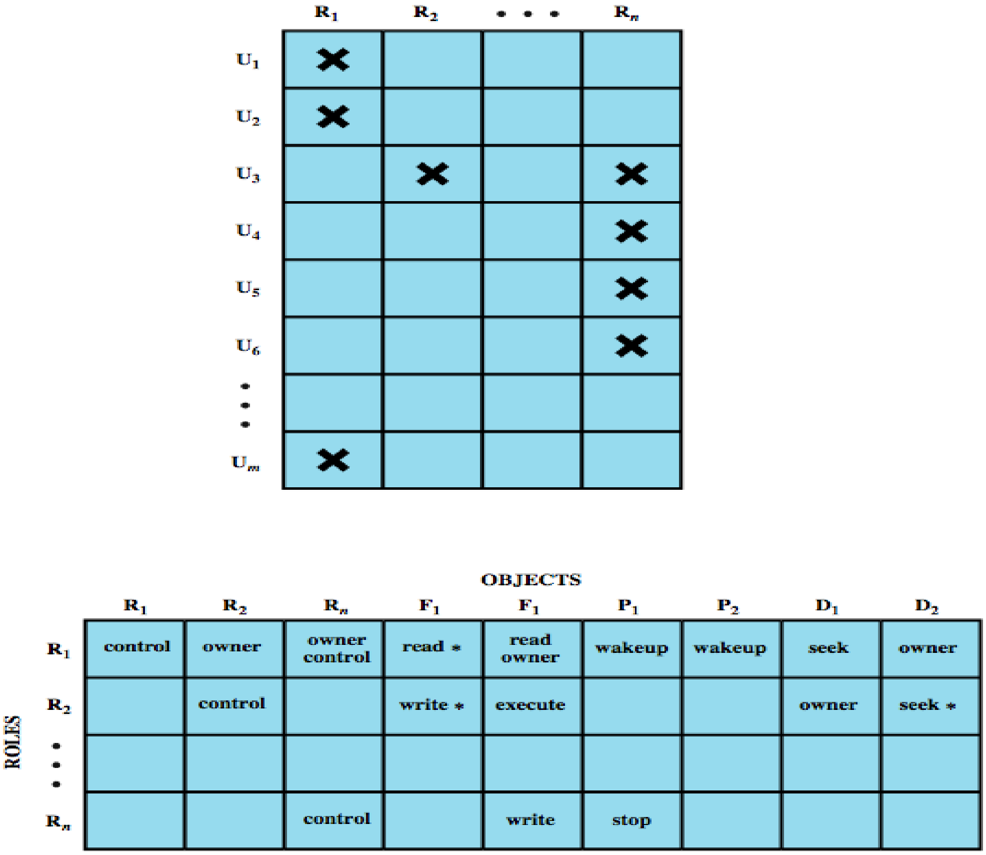
- Matrix one will have relationships between individual users and roles that they can choose from. This highlight, for each user, a selection of roles to choose from to perform their actions based on access rights in that role.
- Matrix two will define for each role, resources, functions that are accessible to these roles. Each role will have a unique set of accessibility to perform actions, access to certain files, programs that differentiate it from other roles and is needed for certain job functions in the organization.
- RBAC follows minimum access necessity principle. Roles are defined and assigned in such a way that user is given minimum access provisions that are needed for him/her to perform their job function. This minimizes any chances of privilege escalation and removes inside as well as outside threats to the system.
- Apart from basic components of subject, object, role and permission in RBAC, a new term of reference called ‘session’ is also introduced. Session is the designation of an individual users activates carried out with a certain role invoked. When a user switches from existing role to a different one, a new session will be initiated. Defining separate sessions not only reinforces purpose of separate roles but also ensures accountability and non-repudiation in an access control system.
- Very often in an organization, role’s access permissions will be a subset of a higher role within that department. A project coordinator’s access permissions will be a subset of project manager’s permissions. In other words, project manager will have all access permissions of project coordinator but will have

some additional permissions according to his higher reporting and managing role in the department. ‘hierarchy’ is some RBAC models incorporates inheritance for users. Having defined hierarchy in a department, role at the highest level will automatically inherit all roles and their permissions that are beneath him. This can be useful in certain scenarios, thus is optional.

- Constraints are another useful feature in RBAC. It allows for defining certain conditions that limit assigning of roles if certain conditions are met or not met. These include among other conditions mutually exclusive roles, cardinality and prerequisite roles. These are the features/ options that make RBAC versatile and suitable for a wide range of access control requirements. This in turn, has led to long lasting usage of RBAC spanning over two decades in fast changing IT environment.
    - Mutually Exclusive Roles: Grouping together of roles in a such a way that a user is allowed only one role from that group.
    - Cardinality: Defining maximum number of users who can be assigned a particular role.
    - Prerequisite role: Conditioning role assignment of user for certain roles to his/her previous assignment to certain role/roles.

Adding the third tier in access management between subject and object (user and role) brings along a number of advantages that make it a successful model for access management in large and rather complex environments.

- Placing ‘role’ between users and resources eliminates any relationship between subjects and objects that they are trying to access. This removes undue interlinking and dependency among subject and object that affect access control management.
- By removing any direct relationship/dependency between subject and object allows for better management. Addition or deletion of individual users and objects does not impact the system in any way. Similarly, addition of users and resources can be easily managed by simply adding them in ‘role’, or if need be, create a separate role and assign users to it.



	R_1	R_2	• • •	R_n
U_1	✕			
U_2	✕			
U_3		✕		✕
U_4				✕
U_5				✕
U_6				✕
⋮				
U_m	✕			

OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
⋮									
R_n			control		write	stop			

Figure 8: RBAC ACL

3.9 Attribute Based Access Control (ABAC)

Attribute based access control (ABAC) is the newest member of access control family having seen some looking into and implementation. As its name implies, ABAC uses attributes associated with its subjects and objects as criteria for managing access. Attributes are various parameters that provide information about their source. For example, in case a file, its attributes can be its type, size, owner, path, creation/modification date etc. Each attribute works as a filter for refined and accurate access control. Access control management based on so many attributes is a processing intensive task but for modern information systems, processing is a cost that is payable for better access management.

Three elements of attribute-based access control (ABAC) model are attributes, policy model and architecture model. These are explained in detail below for better understanding.

3.9.1 Attributes

Attributes are the characteristics that define various aspects of subjects, objects, environment as well as functions/programs/data. Attributes provide the information on basis of which access control rules and provisions are enforced. Attributes are like sensors that provide vital information about various aspects of system objects, environment and system as a whole. Attributes are the classes that are invoked for information, and this information is returned by the system for various system objects and subjects.

There are three types/classes of attributes that are defined in the ABAC:

3.9.1.1 Subject Attribute:

Attributes of the subject: active entity in the access control environment that is initiating the access/execution request, it can be a user, program or resource that when executed would result in change in system state or flowing of information among objects. Subject's attributes are the characteristics that are defining the subject's identity, behaviour and access. A subject's attributes may include its name, organization, job title and sometimes role as well.

3.9.1.2 Object Attribute:

Passive entity in information system access request's context. Object is the entity that is being called for by the subject. It's usually a file, program or domain. Objects too have attributes like subjects that can help in access control decisioning. Object attributes can vary for different objects. For files, it can be its name, path, size and type while for a program, it can be services, functions being called upon. Attributes in objects offer far more detail about themselves thus allowing for a fine grained and well-tailored access control mechanism.

3.9.1.3 Environment Attribute:

Environmental attributes were 1st introduced and used for access control in ABAC as most models before it did not take into account these attributes while making access decisions. Environmental attributes explain the overall context of the system, subject, object and situation in which access call is being made. These attributes are often at the system/global level and are independent of subjects and objects. Examples of environmental attributes can include time, date, overall security level and all other such attributes that are not associated with any subject or object but are rather associated with overall access control system. This relation with system make them an important factor in access control decisioning.

3.9.2 Access Policy

In every access control system, there are often several rules that are global in nature, apply to the entire system and are independent of any subject, object or environmental attributes. These define overall go’s and no-goes for the system and identify rules that underlie in all access decisioning, thus define acceptable behaviour in the organization. These rules along with attributes are the core factors that are considered for access control decisioning in ABAC.

3.9.3 ABAC Decisioning and Logical Architecture

Attribute based access control (ABAC) is a logical access control model which is far more complex in its access control decisioning and for each access request evaluates access decisioning parameters. This enables it to assess each subject’s request to access objects, evaluate subject and object attributes and review overall system conditions and environmental attributes before deciding upon granting or refusing access. ABAC’s ability to fine grain access management lies in its ability to take far more factors/attributes as input to its access decisioning mechanism. ABAC allows implementation of DAC, MAC as well as RBAC which also enhances its operability for systems with widely differing access requirements and environments.

Following figure explain working in ABAC in case of a subject requesting access to an object. Step by step process that is followed is as follows:

- Subject will put forward its request for accessing an object to the ABAC system.
- ABAC will call for and review following parameters.
    - Subject attributes.
    - Object attributes.
    - Environmental attributes.
    - System’s predefined global access control rules.
- Based on all these inputs, ABAC will then decide whether to grant or refuse subject’s request for accessing an object.

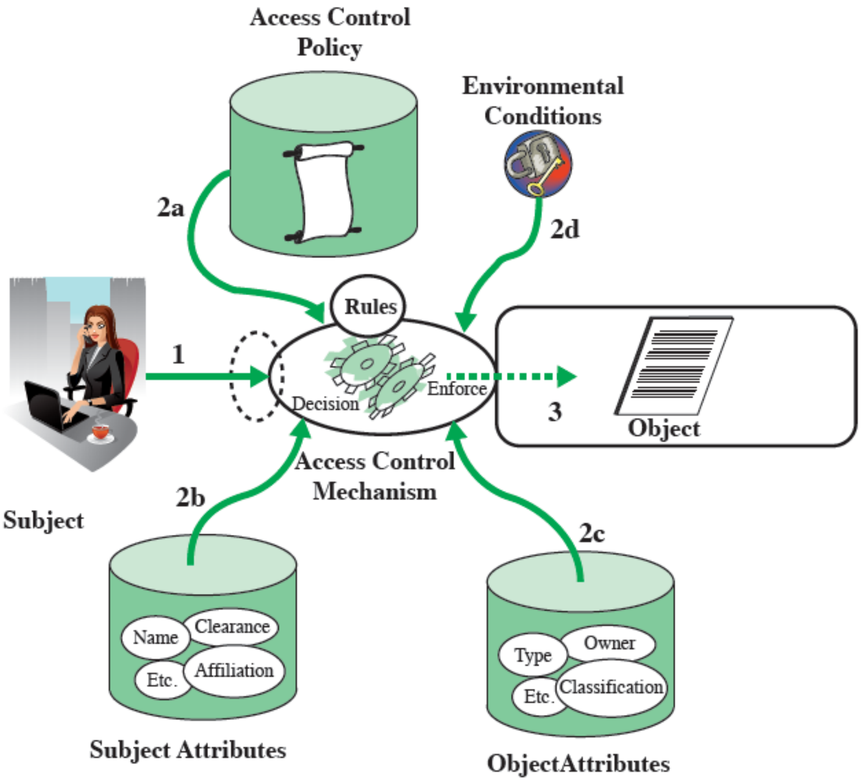


Figure 9: Attribute Based Access Control (ABAC)

3.9.4 Aspects of Attribute Based Access Control (ABAC)

As with all evolving technologies, ABAC also tries to address flaws and limitations of its predecessors. It resolves various issues that had hampered previous access control models. Following are some of the ABAC's prominent features.

- Introduction of subject and object attributes as a factor in access control decisioning.
- Taking environmental attributes into consideration while managing access.
- Infinite possible factors for access decisioning, and consequently infinite access control options.
- Fine grained access control.
- Ability to manage access for each individual as well as subjects altogether.
- Ability to implement older access control methods like DAC, MAC and RBAC.

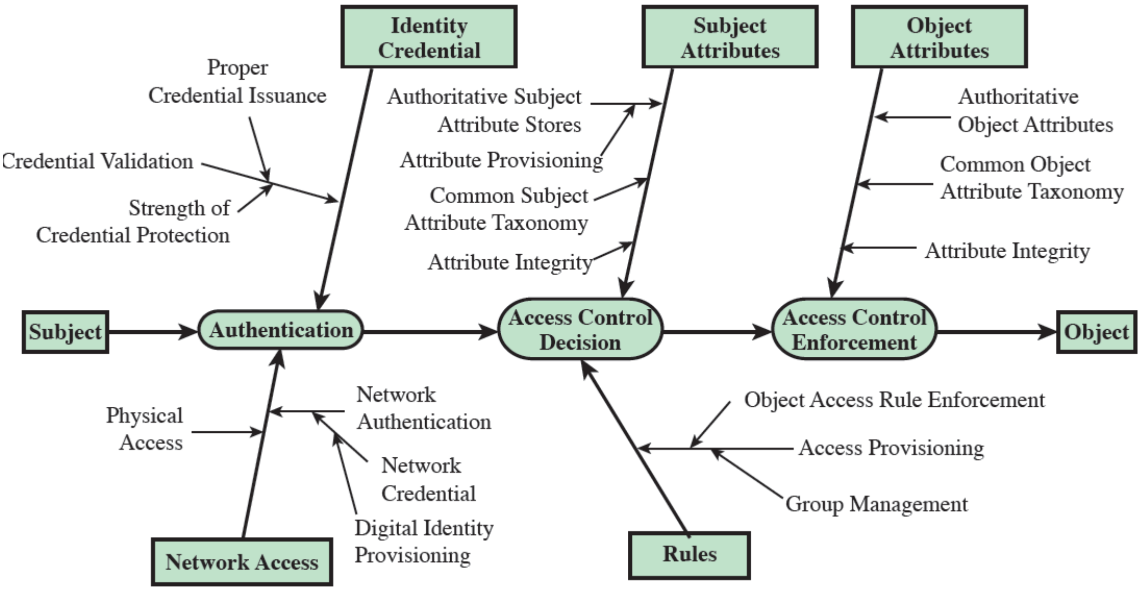


Figure 10: ABAC Attributes and Decision Making

Despite its so many advantages, it fails when it comes to implementing it in real life conditions. Considering all these attributes as decisioning factors requires lots of processing which ultimately makes ABAC slower even for systems with abundant processing capacity. Extensive processing requirement make ABAC infeasible for systems with processing constraints.

3.10 Summary and Conclusion

Access control is the primary measure by which access is managed in today's information systems. After identification and authentication, access control is what defines and decides how access to various resources, functions are managed for various users with varying degree of access and needs.

Access control systems have come a long way forward from their early days; from simpler, mediocre state to advanced and complex as they are today. They have been evolving continuously along with information systems, access requirements and ever complicating security management requirements. Unique aspect of access control has been continuous use of access control principles from their earlier days. Despite having changed greatly in the past three decades, there are many aspects of these access control systems that are still widely used. Mandatory and Discretionary access control (DAC, MAC) are still used in today's OS for access control albeit on a limited level than from their early days.

Role based access control (RBAC) and more recently attribute based access control (ABAC) are being used as the new standards for access and security management in information systems around the globe. However, we do not see access management by any single access control system, no matter how advanced it is, in information systems in operation around the globe. Attribute based access control (ABAC) is new and has not been deployed that widely for access management. Role based access control (RBAC) on the other hand has been used in almost every other access management system. But even it has not been used all alone, DAC and MAC have been a part of access control although RBAC has been central part of the access control system.

Attribute based access control is well ahead of other contemporary access control models in many ways. It allows for use of any aspect of subject, object or system environment as an attribute for access decisioning. This is different in a way that it allows for tailoring access management in a way most suitable to the overall requirements. However, such fine-grained access management does not come without its disadvantages. Biggest among them is the higher processing requirements for such an advanced system. Access decisioning involving so many attributes, in a large organization is bound to be very processing intensive. ABAC uses this complex decisioning technique even in scenarios that are rather straight forward in their access requirements and do not need involvement of so many attributes. This negates advantages that are to be gained from such an effective access control system as it is not implementable in many environments. One solution to this problem is to reduce processing requirements to a point where it becomes feasible for implementation in everyday access management systems. It can be achieved either through reduction in number of attributes in the system, or by limiting the attribute based decisioning to the parts only where it necessary and using other less cumbersome access management systems like RBAC, DAC and MAC for other, simpler access control decisioning. Use of more than one access control system in an overall access control environment is called ‘hybrid access control’ as it is using features of more than one access control system for access management. ‘Hybrid access control’ based on overall structure of ABAC will allow for bringing ABAC down to being used for access control in ordinary information systems.

4 PRIVACY AND DATA SECURITY IN e-HEALTHCARE: INDUSTRY STANDARDS AND BEST PRACTICES

4.1 Introduction

Ultimate goal of all research and development in e-Healthcare and its various aspects is to propose a solution that not only addresses all technical and theoretical concerns regarding privacy, confidentiality, integrity and availability of patient information, but at the same time is efficient, smart and cost effective to the point of utilization and adoptability in healthcare industry around the world. Nature of all things in today's digital world in interlinked. Same is the case with e-Healthcare. E-Healthcare is linked with payment industry, mobile and internet communication industry, financial and insurance industry and research component of healthcare industry to name a few prominent ones.

When it comes to implementation within the industry, primary focus is not always on the effectiveness of the solution but rather on compliance with the industry and governmental standards. On the other hand, research is most of the time focused on solving the underlying issues while ignoring standard and compliance requirements. This present a conundrum when it comes to combining the two unsynchronized items: implementing industry standards and compliance requirements in ongoing research, and implementing solutions found from ongoing research into industry while considering standards and compliance requirements.

Fortunately, or unfortunately, depending on one's views; regulations and industry standards are not that stringent in access control. This, on the one hand allows research to be focused upon solving the issues rather than being limited by compliance and standard requirements. On the other hand, lack of standardization means that research and upcoming solutions will be very diverse in their assumptions and solutions hence may not be suitable to environments currently in the industry.

We'll be looking into privacy, confidentiality, integrity, security and availability requirements of HIPAA, HITECH PCI-DSS and ISO-27001:2013 when it comes to individual's personal information.

4.2 HIPAA requirements on Protecting individual’s information

Health Insurance Portability and Accountability Act (HIPAA) is the primary regulation in the United States that deal with information protection (confidentiality, integrity, availability and privacy) focusing on healthcare information of individuals. Its stated goal is to improve: “the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information”. In the following sections, HIPAA requirements w.r.t. privacy as well as security are explained.

4.2.1 HIPAA requirements for Privacy Protection:

HIPAA provisions regarding privacy protection of PHI are collectively known as ‘administrative simplification provisions’. These provisions include in scope various aspects of healthcare and areas with goal of protecting individual’s privacy w.r.t. its PHI. Unlike HIPAA which was enacted in 1996, its privacy provisions were not finalized until 2002. These administrative provisions along with privacy rule comprise the entire scope of requirements that address privacy. Defined scope of these provisions cover health plans, healthcare providers and healthcare clearinghouses. Protected Health Information (PHI) which is the primary term for individual’s information that is covered under HIPAA’s scope covers any information that include: individual’s past, present or future physical or mental health or condition, the provision of healthcare to the individual, and past, present or future payment for provision of healthcare to the individual. It also defines that any information that can be used to identify an individual will be covered under protective provisions of HIPAA.

Following are the provisions regarding privacy i.e. individual’s PHI sharing, disclosure or access for covered entities.

- PHI can only be disclosed either to individual requesting his/her PHI, or to healthcare regulatory body when they are undertaking compliance review.
- Other than this, covered entity may disclose PHI if it is needed:
    - For healthcare services provisions (payment, treatment or operations).
    - For individual to accept, object to such disclosure with clear and concise options to the individuals.
    - In case of emergency where it might be crucial to individual’s health.

- Information can be shared outside these permitted sections but with the underlying condition that such information was shared after adopting appropriate security measures and only necessary minimum information was shared.
- Use and disclosure other than above mentioned requirements for PHI is permitted for predefined 12 cases which are for improving healthcare access, provisioning and management at federal levels like health oversight, legal, judicial, regulatory and research.
- For research into healthcare in order to improve overall healthcare provisioning, a subset of PHI is defined. This omits certain personal details of an individual and can be shared with outside parties after individual's concent. Requirements such as minimum necessary disclosure, prior concent are necessary to such information sharing.
- Individual who is directly provisioning healthcare services from a covered entity is entitled to privacy notice from the entity. This notice shall clearly define rights to the user as well as circumstances where hi/her PHI might be used, shared with others. Covered entities are required to have explicit consent from individual regarding such PHI accessing and sharing.
- Individuals handling PHI must be trained to handle such information in compliance with local and legal laws.
- Data security should be ensured for PHI during its storage, processing and transmission.

4.2.2 HIPAA requirements for PHI Security:

Unlike privacy and administrative provisions of HIPAA which focus on individual's rights and covered entities responsibilities w.r.t. PHI sharing and accessing, security provisions focus more on technical aspects of PHI's security (confidentiality, integrity, availability). Following are the security provisions of HIPAA w.r.t. PHI security.

- Covered entity must ensure confidentiality, integrity and availability of all electronic healthcare information it creates, receives, maintains or transmits.
- Covered entity must protect PHI against known and potential threats and hazard that can compromise PHI's confidentiality, integrity and availability.

- Covered entity must protect PHI against unauthorized or unintentional disclosure by its users by implementing user access control. In implementing access control, entity must take into account:
    - Complexity, size and capability of the entity.
    - Cost of such security measures.
    - Technical, hardware and software capabilities of the entity.
    - Risk's probability and impact to PHI.
- Covered entity must perform risk assessment, analysis and management for risks identified to PHI.
- Covered entity must regularly review activities on the information system containing, processing or transmitting PHI.
- Covered entity must implement user access management controls like access invocation and revocation as well as employee screening prior to hiring.
- Covered entity must carry out security awareness training for its employees regularly to keep them up to date w.r.t. PHI handling.
- Data backup plan must be in place for an entity handling PHI.
- Physical security measures like CCTV, guards, barriers, RFID etc. shall be in place to protect covered entity from physical threats.
- Passwords shall be strong, long and complex.
- Passwords shall be changed regularly.
- Each user shall be assigned a unique user identity.

4.3 PCI-DSS requirements on protecting individual's information

Payment Card Industry- Data Security Standard (PCI-DSS) is the standard developed by the financial industry, primarily cards (Debit, Credit and prepaid) industry leaders VISA and Master Card for protecting individual's information which in context of PCI-DSS is of financial nature. However, degree of popularity and penetration that plastic money has in the developed and developing world means any monetary transaction will most probably involve plastic money and hence under scope of PCI-DSS. E-Healthcare envisions a health industry that is smart, technologically advanced and more efficient and quick in its operations that involve financial as well as healthcare information. This means that data security requirements for individual's personal information which is dubbed as cardholder data (CHD) in PCI-DSS' context.

Following are some of requirements from a total of twelve major requirements of PCI-DSS.

4.3.1 Requirement 03: Protect stored cardholder data.

Data is of utmost importance in e-Healthcare environment and it is needed 24/7/365 for access, analysis and updating as part of the system. Protection of this data hence becomes crucial for overall security of e-healthcare enterprise. Controlling access to PHI/EHR for only people with a business need and preventing any unauthorized access, disclosure of data is of paramount importance. Confidentiality and privacy of patient's personal, private and confidential information depends very much on protecting his/her data being stored in the enterprise. Security of the system also requires data protection. Requirements defined for securing stored data defined in PCI-DSS are, although not strictly for PHI but for individual's financial information however; purpose of these requirements is similar that is to protect this data from unauthorized disclosure, breach of security and confidentiality and maintaining user's trust. So, these guidelines and requirements can be taken as a source in ensuring confidentiality of user (patient) data present for longer terms in e-healthcare enterprise.

Following are some of some of the technical points of this requirement:

- Only store data is absolutely critical and is needed.
- Use data retention and disposal policies for keeping data current and removing old, unneeded and unnecessary data.
- Sensitive information that is used for authenticating individual and is privy to the individual only must not be stored in the system and removed/flushed as soon as user has been authenticated.
- If sensitive user information is being stored, store it using some sort of technique for obscuring it: encryption like AES-256, 3DES or hashing (SHA), truncation.
- Whenever user information has to be displayed, display it in masked form that does not display complete information to the viewer. Techniques for masked information display include tokenization and partial masking as industry employed practices.
- No matter how strong, encryption algorithm and its corresponding key is, this key has a limited number of sessions, amount of data (packets) that it will

encrypt uniquely and after that it'll repeat that. Number of unique encryptions is called key life and to protect encrypted data and encrypted algorithm from being broken, key has to be changed at its end of life.

- Security of all data stored, being partially displayed is dependent on cryptographic controls being used, which in turn are dependent on keys for their protection. Protection of these cryptographic keys is of ultimate importance. For protecting these keys, standard practice is to store them in encrypted form using another key called 'key encrypting key'. This key encrypting key or often called master key is the single point where all confidentiality and security of encrypted, hashed and masked data collides. For its protection, this must be limited to only few trusted people in the enterprise and key should be handed over to these personnel in chunks so that no one key person has hold of the whole key that is to be used anywhere in the system for encrypting other encryption keys.

4.3.2 Requirement 04: Encrypt transmission of cardholder data across public, open networks.

Cloud is now taken as the new default for larger, geographically decentralized e-healthcare systems. It offers many advantages major among which are availability all around the globe, access over the internet, cost benefits and easier management. However, communication and access among all these geographically dispersed locations is being done using internet which is a public domain, hence open to unauthorized interception and various attacks. This does not mean that costly solutions like designated lines, fiber optics should be deployed, but to use existing security protocols to protect data being transmitted over the internet.

Following are the PCI-DSS' requirements in order to securely transmit sensitive, confidential data over the internet.

- It is better to avoid using wireless media for data transmission, however if it must be done, protocols that offer strong cryptographic protection must be used.
- Common communication media like IM, email should not be used for sending confidential data.
- Data being sent over the internet should be sent in protected form: using VPN or HTTPS (TLS 1.1 & 1.2).

4.3.3 Requirement 06 (Partial): Develop and maintain secure systems and applications.

This requirement is from a development, software perspective and focuses on development security issues. It asks for using security in all aspects of system development lifecycle (SDLC). It asks for taking into account common security vulnerabilities, coding flaws and threats; and address them in the development cycle. Its requirements include established principles like segregation of duties, change management process and backup processes.

4.3.4 Requirement 07: Restrict access to cardholder data by business need to know.

For ensuring privacy and confidentiality of individual data, be it financial, healthcare or personal; it is necessary to limit and control access to this information. Apart from security and access control measures, it needs to be limited to personnel, that absolutely need access to this information for their job duties. By strictly controlling access to people that need, user’s privacy and confidentiality will be ensured. Limiting access to only for people who need it, removes any threat to information as no unnecessary individual is allowed access to such confidential information. In order to ensure better access management, multi factor authentication allows for better authentication and control to manage access to information.

4.3.5 Requirement 08: Identify and authenticate access to system components.

Proper identification and authentication is the mechanism that distinguishes between authorized and unauthorized people for access to sensitive information. Using stronger authentication methods will limit any chances of unauthorized personnel accessing/bypassing security procedure. No matter how strong, an authentication mechanism has been put in place, it cannot hope to prevent unauthorized access unless it is implemented under some rules. PCI-DSS defines such rules that are applicable to all systems using authentication techniques prior to inducing access control. Following are some of these requirements:

- Unique user ID’s for all users, and no generic/group/shared user ID’s.
- Control over addition, modification or deletion of user ID’s.
- Revoking of access rights for any user ID immediately after termination.
- Stronger authentication techniques: multi-factor authentication, stronger passwords, limited number of failed login attempts etc.

- Storing authentication credential s using strong cryptography.

4.3.6 Requirement 10 (Partial): Track and monitor all access to network resources and cardholder data environment.

Monitoring and logging all access on user data will help in identifying any unauthorized access to user data, in real time. This will allow for post incident analysis, in allowing for identifying any flaws in the system by having logs of all such access.

4.4 General Data Protection Regulation (GDPR)

Latest addition to list of regulations by national and international entities seeking privacy preservation for personally identifiable information (PII) is General Data Protection Regulation (GDPR), coming into effect in May 2018. It is the EU initiative to ensure that PII of EU citizens must be protected if it is moved outside EU for storage, analysis or processing.

- GDPR requires specification of data items that are to be collected, reason for their collection, their usage, storage and explicit consent from data subject for all this. (Article 5).
- Processing of PII is to be limited to only what individual has given consent for and it must comply with legal requirements and regulations. (Article 6).
- Consent shall be given by the individual for specific usage of his/her PII, entity using PII has to explain its working around PII clearly and concisely to individual prior to obtaining their consent. Individual has the right to withdraw their consent anytime they want (Article 7).
- Critical information if collected by processing entity requires explicit consent from individual for its usage. This includes among others, health information (Article 9).
- Individual has the right to access his/her PII that is in possession of processor/controller. Individual is entitled to all personal information attributes, their purpose, usage and other such information (Article 15).
- GDPR gives individual right to correct any information that is stored incorrectly with the controller. And to have his/her information removed (Article 16, 17).
- GDPR gives individual right to make decisions on his/her PII. (Article 22).

4.5 ISO-27001:2013 requirements on protecting individual’s information

ISO-IEC-27001:2013 information technology- Security Techniques- Information Security Management Systems, commonly known as ISMS is the international standard for maintaining and managing information technology systems w.r.t. their security perspective. As stated by ISMS: goal of ISMS is to: ‘provide requirements for establishing, implementing, maintaining and continuously improving an information security management system’. Its goal is to identify, assess and then manage all risks that an organization may face to its asset’s confidentiality, integrity and availability. It defines list of controls and their respective objectives that must be addressed to meet ISMS requirements.

Following are some of the controls/requirements of ISO-27001 that are relevant to information’s confidentiality, integrity and availability which can be of use in protecting individual’s PII/PHI/EHR in an e-Healthcare enterprise.

4.5.1 A.6: Organization of Information Security

4.5.1.1 A 6.1: Internal Organization

- Information Security Roles & Responsibilities: All information security responsibilities shall be defined and allocated.
- Segregation of Duties: Conflicting duties and areas of responsibilities shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of organization’s assets.
- Contact with Authorities: Appropriate contacts with relevant authorities shall be maintained.
- Contact with special interest groups: Appropriate contacts with special interest groups or other special security forums and professional associations shall be maintained.
- Information Security in Project Management: Information Security shall be addressed in project management, regardless of the type of project.

4.5.2 A.8: Asset Management

4.5.2.1 A 8.2: Information Classification

- Classification of Information: information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

- Labelling of Information: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
- Handling of Assets: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

4.5.3 A.9: Access Control

4.5.3.1 A 9.1: Business Requirements of Access Control

- Access Control Policy: An Access control policy shall be established, documented and reviewed based on business and information security requirements.
- Access to Network and Network Services: User shall only be provided access to network and network services that they have been authorized to use.

4.5.3.2 A 9.2: User Access Management

- User Registration and de-registration: A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
- User Access Provisioning: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
- Management of Privileged Access Rights: The allocation and usage of privileged access rights shall be restricted and controlled.
- Management of Secret Authentication Information of Users: The allocation of secret authentication information shall be controlled through a formal management process.
- Review of User Access Rights: Asset owners shall review users’ access rights at regular intervals.
- Removal or adjustments of Access Rights: The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

4.5.3.3 A 9.3: User Responsibilities

- Use of Secret Authentication Information: Users shall be required to follow the organization’s practices in the use of secret authentication information.

4.5.3.4 A 9.4: System and Application Access Controls

- Information Access Restriction: Access to information and application system functions shall be restricted in accordance with the access control policy.
- Secure logon Procedures: Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
- Password management system: Password management systems shall be interactive and shall ensure quality passwords.
- Use of Privileged Utility Programs: The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

4.5.4 A.12: operations Security

4.5.4.1 A 12.1Operational Procedures and Responsibilities

- Change Management: Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

4.5.4.2 A 12.3: Backup

- Information Backup: Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

4.5.4.3 A 12.4: Logging and Monitoring

- Event Logging: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
- Protection of Log information: Logging facilities and log information shall be protected against tampering and unauthorized access.
- Administrator and Operator Logs: System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed.

4.5.5 A.13: Communication Security

4.5.5.1 A 13.1: Network Security Management

- Network Controls: Networks shall be managed and controlled to protect information in systems and applications.
- Segregation in Networks: Groups of information services, users and information systems shall be segregated on networks.

4.5.5.2 A 13.2: Information Transfer

- Agreements on Information Transfers: Agreements shall address the secure transfer of business information between the organization and external parties.

4.5.6 A.18: Compliance

4.5.6.1 A 18.1: Compliance with Legal and Contractual Requirements

- Privacy and protection of personally identifiable information: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

4.5.6.2 A 18.2: Information Security Reviews

- Compliance with Security Policies and Standards: Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
- Technical Compliance Review: Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

4.6 Summary and Conclusion

Legislation, laws and regulations vary from country to country, depending on the requirements of the state. HIPAA is the 1st among global healthcare standards that focus on information technology perspectives of healthcare provisioning. Modern healthcare has IT as its enabling element and very often, risks arising from introduction of IT in healthcare are not identified and addressed. HIPAA is taken worldwide as a source for further research and improvement in e-healthcare. Other industry and regulatory standards that focus on information security and privacy can be invoked to further improve and align privacy requirements needed in e-healthcare.

Standards such as PCI-DSS and ISO-27001:2013 are of global nature and are accepted worldwide for their applicability. This means that these can be studied for their requirements and statues in context of protecting and managing individual’s personal information, be it healthcare or financial. This comparison has made an attempt to address the constant lack of study and understanding of industrial requirements for addressing concerns in information management in real life. As can be seen from requirements that are put forward by these multiple standards in order to secure, manage and process personal (financial, healthcare) information that these requirements are implementable and adjustable in experimental access control systems without much effort since these standards and requirements are made keeping in view implementation and application cost.

Chapter 5

5 PRIVACY PRESERVATION IN e-HEALTHCARE ENVIRONMENT: REVIEW

5.1 Introduction

Over the years since the patient requirement for his/her information's management in e-Healthcare environment has become increasingly crucial, several protocols have been proposed to address this issue. These include Pseudonymizing of patient's identity, encrypting patient data and information, creation of public and private clouds to handle sensitive data along with sanitized data, Privacy preserving data publishing, privacy centred access control and data outsourcing and dynamic reconstruction of data etc. [30-33]. It has been recognized that any technique single handily cannot obtain desired levels of privacy and security needed for a healthcare enterprise. Hybrid protocols having been proposed recently are meant to address all dimensions of privacy and security concerns. Hybrid protocols proposed are of several types based on what different approaches they mix together. These include access control (hybrid access control), data and identity anonymization (de-identification plus statistical restructuring) and combination of access control and anonymization techniques to name a few [30]. Hybrid protocols work by incorporating two or more previously proposed techniques in such a way that they reinforce each other with their strong points and their flaws are remedied by implementing them together. Many most recent papers see this approach being discussed, analysed and new such protocols being proposed [14, 49, 51, 55].

Overall privacy preservation in any functional e-Healthcare enterprise requires access control, stored data security as well as anonymization mechanism of some sort when data is shared with others for medical research and insurance outside the enterprise. It is generally assumed that stored data's security will be provided by storing it either behind some access control/authentication or by anonymization. Following is a review of all the research immediately relevant to our requirement of Privacy Preservation of patient's information (Identity as well as healthcare information) having been carried out in the past few years. It considers privacy requirements deemed crucial for its preservation and reviews articles relevant in this regard. Initial research in this regard mainly focused on patient identity management through various techniques [34, 38-40]. Whereas recent research has seen and addressed the need for patient data management to ensure total privacy as seen in figure 1 [14, 30].

5.2 Pseudonymization

One of the earliest propositions with regards to user privacy preservation (personal and healthcare data) was data anonymization. Idea was to modify data in such a way to remove all its information regarding patient. This sanitization of patient information will allow for patient trust in e-Healthcare enterprise while allowing for healthcare record sharing for research without compromising privacy. Pseudonymization was one of the earlier approaches to address privacy issues related to a user's identity. For Privacy preservation, US and EU demand strict measures to be installed for such healthcare systems to be used. Simply speaking; instead of using one's real identity for various tasks in e-Healthcare system, a pseudo identity is derived to be used instead of user's real identity and other attributes unique to him. This identity is used to perform all tasks of the user i.e. sharing EHR with physician, nurse and obtaining medicine from pharmaceutical. This identity cannot be traced back to the user unless all the information along with a secret is available [34, 35]. Security of this algorithm lies in protocol's ability to deny any linking between real and pseudo identities, and system's ability to secure storage containing tabled entries of these identities. A very crucial aspect in this approach is to categorize patient's data into sets; user (Physician, pharmacist) relevant data and personal to be pseudonymized data. This approach is called de-Personalization. Basic approach in deriving pseudonyms is encryption or hashing. There are certain unique requirements when it comes to pseudonymization of PHI.

Pseudonymization of identities was the only privacy concern during initial stages of e-Healthcare enterprise development as it was deemed sufficient for patient privacy preservation [36]. However, it has been seen that identity anonymization alone is not enough for patient privacy preservation. With certain skill it is possible to identify the patient by analysing his healthcare attributes (PHI/EHR). Certain issues regarding privacy breach have been identified:

- Disclosure of sensitive personal information during transit or storage at cloud.
- Unauthorized access to information due to weak authentication scheme or poor access control.
- Dynamic nature of cloud environment may cause aggregation in services.

- Security and privacy requirements specific to above mentioned privacy concerns have been defined for e-Healthcare's patient identity management server:
- Support for cross system interaction due to various existing ID management systems i.e. interoperation and delegation.
- This system must provide a vast range of security and privacy preserving properties such as one and two factor authentications, Attribute based encryption deployment etc.

Initially pseudonymization was centred on identity hiding. This was due to the fact that information was not shared outside the hospital-a trusted environment. This allowed for a certain degree of trust for a patient towards the hospital. Use of cryptographic hash functions was proposed in this regard [37]. Although, this allowed for privacy preservation of user identity, but it did not provide any measures when this data was shared with others. User data short of his identity was visible to others which constituted a serious privacy breach. Earlier research revolving around the issue of data anonymity was very basic [38]. An important improvement over traditional approach of using cryptography was that encryption and decryption were not needed. And more importantly, data could be readily processed as it is as no decryption was needed. Obvious weakness was the weaker data anonymization techniques used (dividing data into chunks each having incomplete patient information). Another security measure identified was use of blank pseudo identities which increase its security as it greatly decreases the possibility of pseudonyms being correlated to actual identity.

Riedl et. al. [34] propose a comprehensive solution in this regard. It allows patient full control over his information as to who can access it in what capacity. One problem that arises from the prospect of assigning new pseudonym to a patient every time and for its multiple samples is that it becomes very difficult to use his information for improvement of e health system components like medical research, improving and integrating bed and biology [39]. Another problem identified in this approach is encryption of huge patient health information (PHI) sets in the data base. Use of symmetric encryption creates additional processing requirements and causes concerns over its performance in real life scenario. Slow processing overhead in this regard can be overcome with use of newer, more efficient encryption techniques. A possible solution is replacement of symmetric block ciphers (AES, DES) with nonlinear feedback shift registers which have proved to be not only secure but also very processing efficient. Inability of this approach to correlate multiple pseudonyms (PSN) to a single PHI has been pointed out [40]. This denies the option of combining this information for a single patient for better diagnosis and analysis. Riedl et al. proposed a change in this regard [40]. A new component was introduced to the system which allowed correlation of multiple PSN's to a single PHI. In order to allow for correlation of multiple PHR's by researcher, he is also assigned an identity which is then used for multiple PHR correlation.

It is very critical to strike a balance between anonymity of multiple patient records while on the other hand, need for detailed PHI and all relevant information for better health care and research [42]. These, somewhat contradictory requirements make it difficult for an effective solution to be designed as there is no middle ground between these. Lack of correlation among multiple PSNs of any user was a major hurdle for medical research. Pseudonymization was introduced to help with sharing of patient data outside the trusted environment of the healthcare enterprise for research purposes, but inability to correlate multiple PSNs made it infeasible. This was overcome by introduction of multiple PSNs for a single user at different junctions of healthcare enterprise [43]. Further improvement can be assigning of parent PSN derived from user identity adding an additional layer of anonymity. All PSN's are to be derived from this which should be able to track their identity to this parent pseudonym. This two level Pseudonymization will allow for only one set of pseudonyms to be sent around and correlated together to parent PSN which cannot be correlated to PID by no one except Pseudonymization authority. This will allow for correlating multiple PID's of a single patient for better diagnostic and medical research while ensuring his anonymity and privacy. A somewhat similar approach of two pseudonyms was also introduced in other research [40] however this lacked the option of deriving multiple tier 2 PSN's from tier 1 PSN which results in all PHI going to one who requests this information which will violate the requirement of providing requester least resource (information) required. This approach of deriving multiple PSNs from a single EHR of a patient for treatment, however does not fully address patient privacy concerns. Patient must be given control over which PSNs of his EHR can be correlated and which are to be kept private. Also, how can patient control over his EHR/PHI be bypassed in life threatening scenarios [44].

In another early article on pseudonymization by Jensen et. al. [45] proposed, instead of assigning every user a new identity, issuing a group identity. A group identity is to be used by the patient to share his PHI/EHR with healthcare provider. Service provider knows the group's identity and will use it to verify with the group that patient is a valid one. However, it cannot know the individual identity of any of the members in the group. Current privacy requirements don't even allow for cloud's ability to correlate users to a group as by determining the group, one could with some certainty guess the nature of its users EHR's. Their defined approach covers non-interactive scenarios but for interactive scenario where cloud is expected to return an answer, opts for public recipient anonymous approach which has evident flaws as it could with some skill be correlated to its actual user by narrowing down his defining attributes. Current e-Healthcare systems are of isolated nature with differing architectures. This is a hurdle in the way of national healthcare program ambitions. Intermediary step in this regard is the ability to correlate different EHRs of a single patient at national level before their full incorporation into it. Bandar et al. [44] have identified patient consent and authorization as a crucial requirement for EHR linking within their privacy sphere. They have created a set of pseudo identities derived from primary identity to be used as electronic medical records (EMR) for treatment independently from each other. Having been a part of a set of PSNs, these can be correlated. Patient privacy is ensured by giving only him the authority to request correlation of his multiple health records. However, he must identify all his EHRs which is a difficult task for a longer time span. Data anonymization, de-identification and pseudonymization are all needed for an EHR to be shared outside patient's privacy and trust sphere. Use of key identifiers search and replacement has been used for this purpose, but it does not provide desired level of anonymity [46]. Legal and corporate requirements for strong de-identification measures to be installed are meant to exert greater user confidence in e-Healthcare system but current techniques in this regard are not up to mark [47]. It is crucial for patient privacy and his PHI anonymity/de-identification that his healthcare data that is derived from his primary health record is retained for a limited time and is either moved to a storage server not readily accessible or is deleted after use. This is not the case for primary healthcare record (PHR). [65] This is evident from comparing these articles and their propositions as shown in table below.

Table 1: Research Review and Comparison

Research Article	Proposition	Patient Anonymity Level	Correlating PHR for medical research.	Anonymized data searching.
Yang et. al [14]	Vertical data partition and hybrid anonymized data searching.	Strong (identity, data).	No.	Yes.
Riedl et. al [34]	Assigning new pseudonym to a PHI for every session preventing correlation of two pseudonyms originating from single PHI.	Weak (identity).	No.	No.
Wang et. al [37]	Pioneering the idea of data anonymization with data partitioning. Multiple tables with incomplete patient information.	Weak (data).	No.	No.
Riedl et. al [41]	Assigning new pseudonym to a PHI for every session preventing correlation of two pseudonyms originating from single PHI.	Weak (identity).	No.	Partial i.e. researcher is assigned a new PSN to access PHI.
Aamot et. al [39]	Identifies problems associated with pseudonymization approach introduced by Riedl et. al [30]	Weak (identity).	No.	No.
Pommering et. al [40]	2-tiered pseudonymization.	Weak (identity).	Yes.	No.
Agarwal and Johnson [43]	Hippocratic data base for legal and ethical e-Healthcare compliance.	Strong (identity, data).	No.	Yes.
Alhaqbani and Fidge	EHR linking to individual EMRs.	Weak (identity).	Yes.	No.

[44]				

5.3 Privacy preserving Access Control

Use of strict Access Control policies has been long observed as the proper way to control access to one's information. By rigorously controlling the access to privileged information, privacy can be preserved. However, any single access control policy alone cannot help preserving privacy for the entire e-Healthcare enterprise. Hybrid access control i.e. use of two or more access control policies to better create a secure and controlled access mechanism, is the solution in this regard. To ensure privacy, access control is very crucial as it allows user to define who has access to his information and to what extent can he use it. When combined with data anonymization, it in concept solves the issue of privacy by hiding user's identity as well as controlling flow of his information as it has addressed all major concerns of a patient w.r.t. PHI/EHR i.e. preventing unauthorized access to PHI, Storing and handling data in an anonymized manner and sharing data with outside 3rd parties without compromising patient privacy.

HadiGunes et. Al [48] discuss several access control schemes that are used worldwide for controlling access to information and resources by users. Seeing their pros and cons, it becomes clear that no single mechanism alone in its totality is perfect enough for our desired access control. A role identity-based access control scheme has been implemented by the authors. However, it still has some issues that need to be handled. For example, a role defined as 'family' to allow family members to view patient EHR will allow every member same level of access but inner family members need access to financial information of the patient which is not possible in simple role-based access control (RBAC). Younis et. al. also points out many issues in this access control approach [49]. According to them Permissions in Task Based Authorization Control (TBAC) are activated or deactivated according to the current task or process state. As there is no separation between roles and tasks, they use varied factors such as users, information resources, roles, tasks, workflow, and business rules, to solve the separation problem and determine the access control mechanism. The scheme uses the workflow authorization model for synchronizing workflow with authorization flow. They utilized tasks which support active access control and roles which support passive access control.

Lu et. Al [50] propose a novel approach for patient e-Health care monitoring. They propose e-Health system dedicated access control mechanism which addresses the concern of giving patient control over who accesses his PHI. Using ESPAC (enabling security and patient centric access control), patient assigns various categories, access to PHI as he desires. In contract-based e-Health system, where patient signs agreement with medical Centre server (MCS) regarding use of his PHI, this information of assigning multiple access levels to elements of the system (Doctor, Insurance company etc.) regarding accessing PHI. PHI, if delegated to someone not allowed to see must be subject to approval by patient by initiating a session regarding this. (For example, highest level entity, doctor who is allowed to see PHI and pass recommendations will not be allowed to delegate this PHI to anybody until delegatee's level is lowered to allow only viewing and not passing any recommendations). So only doctor can provide treatment but anyone else who was delegated this PHI cannot initiate a treatment except offering opinion to doctor.

Sun et. al [51] in their paper have used a simple role-based access control scheme for their e-healthcare system to provide user with a defined EHR access policy. They have defined various roles based on activities performed by these entities in the system i.e. doctor, nurse, pharmacist etc. However, they themselves have pointed out the limitations of using this approach. For example, not all doctors are supposed to have same access to a patient's EHR. A more detailed access control policy needs to be defined and set in place to comprehensively handle access control in e-healthcare environment as flaws are apparent in traditional access control mechanisms which are not suitable for e-Healthcare enterprise's specific requirements.

Requirements that were deemed to be a necessary part of any successful access control mechanism ensuring privacy have been accurately implemented by Zhou et. al [52] along with a couple of new, interesting innovative techniques. Their approach intends to achieve both authentication and privacy with a single stroke, a great feat in an environment where overheads of security have become very cumbersome. Regarding our concern of privacy, authors have proposed Authorized Accessible Privacy Model (AAPM). It not only efficiently resolves the access control requirements but also resolves the issue of managing physicians for a patient. In AAPM, access controls and privileges are defined by an access tree supporting flexible predicate thresholds. For new patients, it is difficult to find the right physician, so this approach allows patients to encrypt their PHI with access policy.

This allows only physicians meeting the criteria set by the access policy to decrypt that PHI. Despite its visible advantages in terms of being user friendly to the patient, it reduces the control a patient has over his information and access to it. Its automatic profile matching to allot physicians to PHI's matching their profile renders patients incapable to select a physician for them based on their own requirements and preferences. Also, a rogue physician set up in the system could easily be used to create a profile to attract specific PHI's thus compromising privacy.

A more comprehensive access control policy and its defining features, although not being defined here, but a skeleton is given here as to further develop and refine it for implementation. Following are some of the proposed features for a comprehensive hybrid access control policy.

- Roles defined as in role-based access control scheme.
- PHI assigned various privacy levels i.e. for health information considered not so private, a low privacy level while for critical and private health information, a higher clearance level requirement defined.
- Patient profile containing his categorized PHI as well as a list of users in e-healthcare environment who are allowed full access.
- A similar profile for doctor containing list of patients whose full PHI he has access to.

Patient can update his profile either to update his PHI sub levels or to update list of users who have access to his PHI.

Chen et. al [53] introduced a cloud centred role-based access control mechanism named Cloud-based Privacy-aware Role Based Access Control (CPRBAC). This access control mechanism has been further alleviated by introduction of active auditing system dubbed AAS. CPRBAC has certain features improving it over traditional RBAC i.e. Context based access control, information sharing among different cloud servers and authorization delegation [54]. It points out the weaknesses present in traditional RBAC schemes which prompt the need for a tailored RBAC policy for e-Healthcare cloud environment [54]. Four new conditions namely purpose, obligations, conditions, organizations have been defined in order to help easily and effectively define complex access control policies and rules. Active Auditing System (AAS) is placed in such a way between CPRBAC and backend data server that all data and communication have to take place through it, thus acting as an intermediary between the two. Its position allows it to monitor all processes among server and CPRBAC thus allowing for a real-time monitoring service. It keeps a check on all the activities and takes prompt action in case a policy violation is detected. This prevents all attacks trying to access confidential information by bypassing CPRBAC framework. It also generates alerts to notify relevant personnel about any misbehaviour in the system. Their experimental results show that a combination of access control mechanism along with active auditing system helps regulate the flow of information and prevents any unauthorized access either deliberately or accidently against which traditional RBAC approaches fail [56].

Access control policies cannot be defined for all scenarios and there are chances that a situation may arise in such a way that cannot be handled by the access control policy, some sort of fall back or initiation mechanism must be in place for arisen abnormality to be normalized and assimilated in the access control mechanism. It has been noted that in many access control mechanisms being proposed, access control policies do not address data access or role changing if data is delegated to someone with less access to data than the one delegating it. Similarly use of 3rd parties for handling several key and session management issues is again a potential cause for security or privacy violation [79].

Deng et. al [57] have looked at the prospects of e-Healthcare system architecture w.r.t. privacy preservation. They have pointed out the advantages and challenges brought up using modern technology primarily cloud services. Their research focuses on the privacy and confidentiality challenges brought up in a home-based healthcare system by induction of modern technology. It also looks at these challenges in light of US and EU legislation and informs about the ongoing research about trust worthy clouds (Tclouds) [58]. A critical analysis of cloud research methodologies namely business driven, and architecture driven is performed. It has been pointed out that most of the research in this regard has been of random and adhoc nature failing to systematically address and analyse a problem. Coming back to their topic, they point out the challenges unique to home-based healthcare environments. These are semi trusted cloud services, data centric protection, efficiency, patient centric protection, control and transparency. Regarding privacy preservation and patient centric access control, authors have relied upon use of attribute-based encryption (access control) and data encryption (privacy preservation), however it has not been further elaborated.

Chen et. al [59] have proposed a protocol for secure data sharing among medical researchers and institutes without fringing upon privacy and confidentiality concerns of the patients [60]. The need for secure sharing among researchers for improved medical practices and services has been seen for a long time since cloud's introduction in e-Healthcare environment. Their protocol dubbed PRECISE intends to address this issue while ensuring privacy and other relevant concerns originating from this, both legal and technical. They have pointed out the limitations and flaws of the existing techniques that are centred around the issue of secure and anonymized data sharing among multiple healthcare service providers [61]. They have chosen homomorphic encryption and Yao's protocol of garbled circuits for their setup. Homomorphic encryption allows for data processing in encrypted form, thus by performing operations on encrypted data without having to reveal the information ensure confidentiality and privacy of system users. Homomorphic encryption has been prescribed as a solution to privacy concerns in e-Healthcare in other research articles as well, but it is a well-established fact that homomorphic encryption at its current processing speed cannot be deployed in e-Healthcare enterprise which already is constrained by existing processing powers of systems [76]. PRECISE is intended to help healthcare service providers in cooperating and sharing information in order to improve services and benefit from each other's experience. However, they themselves have described that this approach is an experimental one and there needs a lot of work to be done to make it suitable for industrial use. As per the authors, work is being carried out to come up with more systems of such functionality albeit with improved security footprint and efficiency.

5.4 Summary and Conclusion

It is clear from above documented review of current state of research in e-Healthcare that there is no singular, directed and user specific approach to coming up with a e-Healthcare solution. There are number of shortcomings in existing research:

- Research does not connect with realities and limitations on the ground.
- Solutions proposed are very few, and often do not have the capacity to work in the real environment.
- Research carried out usually do not cover all aspects of an e-Healthcare enterprise.
- Lack of established basics means that underlying definitions and rules vary from solution to solution.

Chapter 6

6 DISCUSSION AND ANALYSIS

6.1 Introduction

e-Healthcare offers several advantages over traditional healthcare approaches. However, its security and privacy concerns continue to hold it down from being implemented at global level. Privacy among other issues, remains to be addressed to a level satisfactory to its users. Existing e-Healthcare enterprises have faced a number of attacks compromising patient trust and in turn leading to questions regarding its usage. Review carried out here reviews recent research carried out to address concerns raised about privacy preservation of patient healthcare data during storage and usage. This chapter reviews research on both privacy concerned areas, data handling during storage and transmission along with how to manage access and privacy of this data when in possession of other users, in a way that such access neither compromises patient's privacy nor does it violate any regulations.

Seeing the work done in recent years regarding privacy preservation, it needs to be clarified that Privacy preservation using a single approach is not possible in the entire e-Healthcare enterprise due to multiple reasons.

- Privacy requirements and definitions may vary at different points in e-Healthcare system.
    - For example, anonymization and access control are both portrayed as a solution for Privacy requirements in e-healthcare. They both take care of certain Privacy requirements although both possess certain weaknesses thus are unable to meet Privacy requirements single handedly. Anonymization secures patient's identity against stolen PHI from correlation, but it does not address the access mechanism for this.
    - Similarly, access control although controls the access to PHI/EHR but it does not provide anonymity in case of privilege escalation (access control failure).

Privacy defining, and guiding regulation may vary from country to country, hence require a versatile approach/framework addressing privacy in e-Healthcare.

6.2 Proposed Framework Salient Aspects

Having studied recent research on Privacy preservation in general and for e-Healthcare in particular, a hybrid approach is being suggested here. Pseudonymization will be used to protect data stored and shared outside trusted e-Healthcare environment while access control will be used to control data access and its flow within the trusted environment. Major privacy concerns in healthcare data privacy during storage and usage are: unauthorized access to patient data and patient healthcare information sharing outside e-Healthcare environment without depersonalizing it. Most of the research carried out in this regard focuses on either one of these issues and fail to recognize the need for handling them simultaneously. This proposition intends to address both simultaneously which will ensure total privacy preservation for healthcare data stored at the cloud. It will address two primary concerns regarding Privacy I.e. Patient centric access control and identity/ information hiding from exposure. Following sketch is suggested as a solution for overcoming Privacy preservation challenges in e-Healthcare.

- Use of data anonymization (pseudonymization) during storage and transmission will ensure that patient’s identity and personal information (name, address, social security number, contact info. etc.) are not revealed in case someone intercepts his PHI/EHR. Further analysis and research is needed to define a suitable technique which is both efficient and secure in this regard.
- Patient centric access control will allow patient to exercise control over who can have what level of access to his PHI/EHR. This not only meets privacy requirements but also allows e-Healthcare system to gain patient trust- a vital component for e-Healthcare system’s success.
- PHI in itself should be divided into various sections requiring different degree of access levels in order to be accessed. Lower access levels will only allow for seeing the only relevant data for the user i.e. medicine requirements of a patient for a pharmacist. While physicians will have higher access level allowing them to see both the patient medical condition, his diagnosis as well as the treatment he is getting. This compartmentalization approach will allow for more secure and efficient management of the e-Healthcare system.
- PHI levels are defined based on the user group information requirements. Healthcare insurance providers, government security agencies should not be

concerned with the technical (medical) details of the patient but rather with his financial and general information so a level allowing access to this particular section will be created. Similarly, a level will be there for the hospital staff revolving around the medical information of the patient.

- An alternate to this can be use of multiple tickets for a single patient, each revolving around a certain aspect of patient’s healthcare. Multiple tickets for hospital staff, healthcare insurance service providers, medical researchers etc. could be defined. This will reduce the overall complication of the access control mechanism, but it will require definition of more than one access control mechanism (Figure 2).

As it has been noted that use of traditional role-based access control (RBAC) mechanism for the PHI/EHR management is not feasible [51, 56], it is logical to divide healthcare information into sections based on their usage, type and privacy value. Figure 2 has shown overall PHI divided into various sections based on their usage and type i.e. patient insurance ticket (PIT) for health insurance management, Patient profile (PP) for family/friends, Hospital healthcare data (HHD) for hospital staff usage and finally research data (RD) for sharing outside e-Healthcare environment for medical research. Categorizing healthcare information in this way allow for defining separate policies and rules for categorized information which in turn allows for better and refined management and access control. Although ABAC fulfils above mentioned requirement for a more tailored access-controlled access control mechanism, but its processing constraint limits its usage in a real-world scenario. ABAC’s complexity which is its advantage over RBAC in allowing for defining a more complex access control mechanism is also a weakness in sense that, for large scale enterprise, defining and managing such an access control system is very difficult.

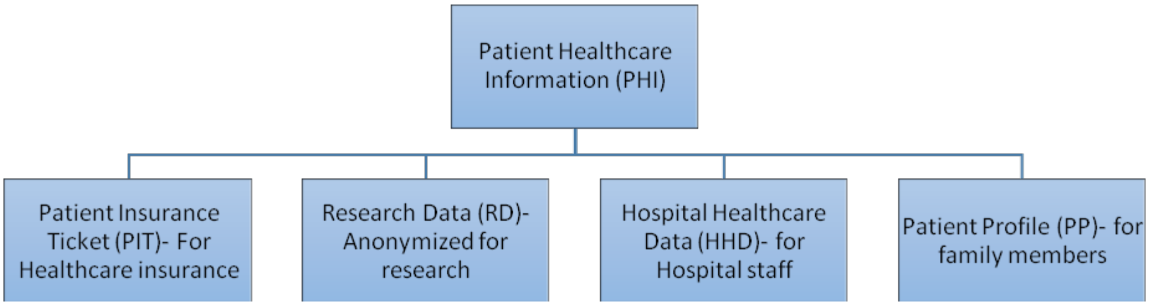

Patient Healthcare Information (PHI)
Patient Insurance Ticket (PIT)- For Healthcare insurance
Research Data (RD)- Anonymized for research
Hospital Healthcare Data (HHD)- for Hospital staff
Patient Profile (PP)- for family members

Figure 11: PHI Compartmentalization for better control and security

- We are proposing a multi-tiered access control scheme somewhat like multi-factor authentication in its essence where both conditions are needed to be true in order to be authenticated. Role based Access control (RBAC) on upper level and identity/attribute based on certain lower levels (roles).
- Physician, Pharmacist, Nurse etc. are certain roles that are defined and possess certain level of access. For example, pharmacist only needs read access while a nurse checking body health parameters only needs write access in most cases. While a physician needs both read and write access (As shown in figure 3). For these common roles that are to be present in all e-healthcare enterprises, traditional RBAC can function effectively without requiring any additional processing, thus negating ABAC's complexity and processing constraint.
- Since not all persons of a certain role are entitled to see PHI, identity/ attribute-based access control comes into play. At this level, usage of more specific access control is a necessity. Multiple access control mechanisms like DAC, MAC and ABAC can be used simultaneously based on which one of these best suite access control requirements.
- For patient's family members, RBAC or identity-based access control can be used. Cases where a fairly substantial number of family members are allowed access to PHI, a role for family can be defined. However, for few closer family members or people taking care of insurance and financial aspects related to healthcare can be entitled to some additional information along with PHI. Information classification suggested above can be employed to handle this.

- Delegation in this is performed using computer security models which enforce read/ write bounds on upper/lower layers. This prevents people with lower level of access and trust from proliferating PHI. This also allows people with write access to PHI (physicians) to look for another opinion on healthcare matters from fellow physicians, but it does not give the consulted person authority to make any changes in PHI. That authority lies only with the authorized person (Physician with write read/access).

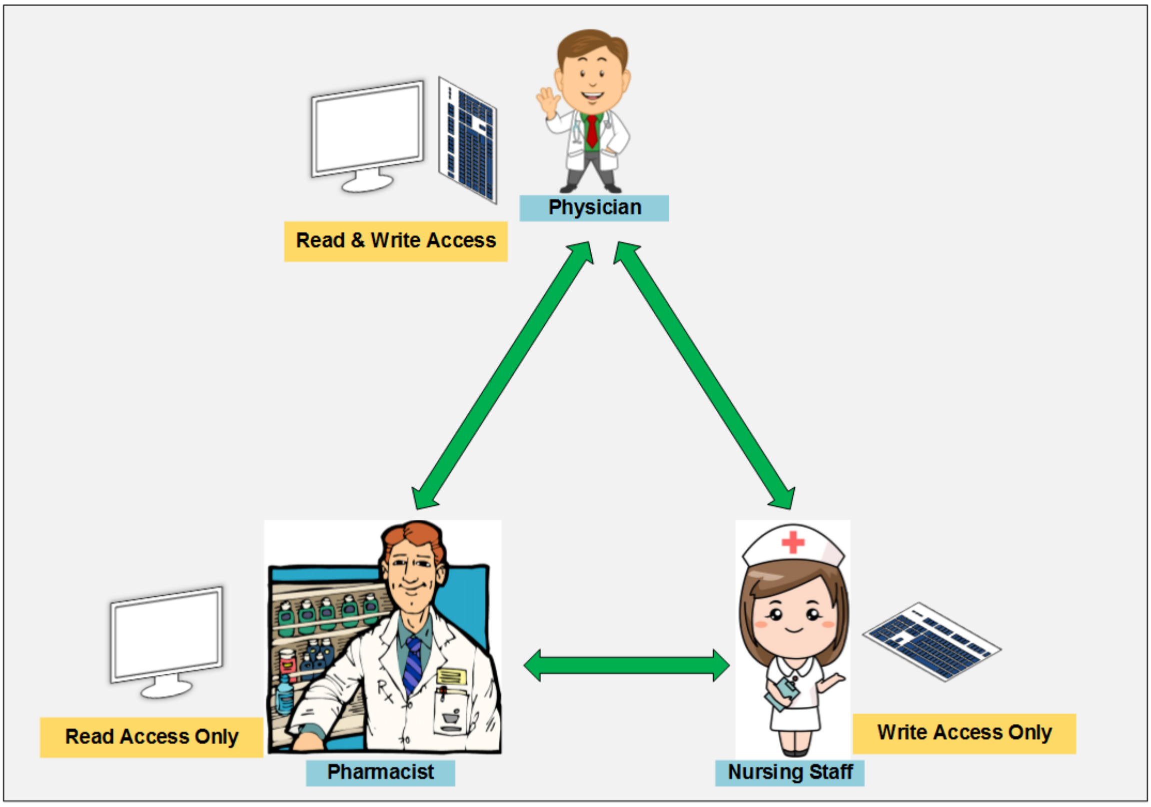


Figure 12: Conceptual HBAC Model of e-Healthcare

On a broader scale, especially in the case of under developed regions like parts of Africa and Asia and Latin America, level and quality of healthcare services being provided are different. Urban healthcare services tend to be more advanced and modern while rural healthcare services centre around more basic healthcare provisions. This heterogeneity can be employed to create a faster healthcare enterprise. Rural section of e-Healthcare enterprise, which is tending to medical needs of a greater section of society is relatively simple while more complex urban healthcare section of enterprise is handling lesser number of patients as compared to its rural counterpart. This allows them to be not only balanced out but also get maximum amount of benefit with relatively limited resources at state’s disposal [81].

Despite all this, it needs to be remembered that all these conditions and policies are not applicable in case of an emergency. Emergency healthcare provision requires immediate healthcare services and often, traditional approach cannot be counted upon in such cases. Authentication and access control mechanism which are patient dependent during normal operation of e-Healthcare are not able to work in case of emergency. So, an alternate emergency response and processing mechanism must be devised and installed to allow for patient treatment without all these restrictions. However, it must not act as a way to exploit the system because if for a certain patient emergency protocols are invoked unlawfully, they will allow for his PHI to be seen by unauthorized personnel thus resulting in Privacy breach.

6.3 e-Healthcare Enterprise Privacy Preservation Framework (eP2F)

Our proposed e-Healthcare privacy preserving framework revolves around the more important concern of access control and information sharing while relying on industrial practices to address other issues such as identity and information anonymization. Tokenization and hashing using hardware security module (HSM) is probably the best option available to address identity anonymization. It is being used for identity anonymization in PCI-DSS which also revolves around protecting and securely handling individual’s financial information which lies in same league as PHI. By relegating identity anonymization to HSM which is considered as secure by financial industry, we can focus on the remaining issues to e-Healthcare enterprise’s privacy: Access control within the enterprise, and information sharing for research outside e-Healthcare enterprise.

Our hybrid approach to access control has been somewhat defined in above section of this chapter. Its underlying and equally crucial part is information classification which is the 1st of two layers of access control decisioning. Classifying information helps in defining a limited set of information groups which result in better definition and management of access in the e-healthcare enterprise. For our e-Healthcare access control framework, we have classified information in following sections.

- Personal Identifiable Information (PII), which is the information or its subsets that can be corelated with an individual. This can include individual’s name, parent’s name, date of birth, religion, ethnic background, gender, age etc. It may be noted that possession of any one PII attribute may not result in revelation of an individual’s identity but corelating multiple attributes can result in identification of an individual even if some of their attributes are not known.

  - To effectively protect an individual, PII can be further grouped into public, restricted and confidential information. In this way, his/her information can be further controlled and prevented from unauthorized access.

- Person's Healthcare Information (PHI), individual's medical information that give an idea about his/her medical history and condition. This may include blood group, any inherited/genetic disease or medical condition, previous medical history, existing or past medication or surgeries, any psychological condition etc. This is the information that is present in e-Healthcare enterprise only and does not exist anywhere else unlike PII or individual's financial information whose custodians may be government or banks. PHI is more crucial than PII or PFI due to two reasons: this information is far more critical and important, and e-Healthcare enterprises are not mature on the levels of state or financial institutions to properly and effectively store and process this information in compliance with laws and patient's expectations.
  - This information can be further divided into public, restricted and confidential information based on risk associated with exposure of this information. For example, information such as an individual's eye sight is not critical or confidential when compared with an individual's rather intimate medical information.
- Person's Financial information, costs associated with healthcare services provisioning and insurance, which are intertwined with healthcare contain information which individuals hold dear and do not want to be public. This may include bank information, account details, insurance provider etc.
- HIPAA defines 18 specific information attributes that are covered under PHI and hence require compliance with HIPAA and its regulations. These include PII, healthcare as well as financial/insurance information.
- In our data classification, anonymized research data is the data that does not contain any of these information attributes. This data does not contain any information that may reveal any individual information or allow for correlation of information with its corresponding individual. It must be noted

that for certain research cases, where healthcare as well as individual information is required which is otherwise omitted from this RD; RD will not be of use. HIPAA allows for sharing healthcare data of an individual that is not anonymized (contains PHI) but after consent from patient and after knowing that entity who is being given access to this information is also HIPAA compliant and thus have necessary controls and processes in place to adequately protect healthcare information.

- For better access control and management, PHI attributes (18 individual healthcare) are further divided into three categories: healthcare, financial and personal. In this way, more refined and appropriate access control mechanism can be put in place.

6.3 Solution Validation

eP2F proposed above has been designed keeping in view limitations and shortcomings of existing research and solutions. It also takes into account existing as well as upcoming industry, technological, security and legal requirements. Its aims are two-fold: Overcome limitations, flaws and shortcomings in existing solutions and frameworks; and address any issue, be it technological or legal that has not been addressed in previous frameworks. Following are some of the salient features of the eP2F:

- Framework is designed keeping security and privacy requirements in view. By keeping these as part of framework design and not treating as an add-on, these requirements become part of the framework equation from the very beginning ensuring a framework that is fully secure and ensures total user privacy.
- Framework uses hybrid access control instead of using any single access control model allows for increased flexibility, efficiency and operability.
    - Most of the existing access control frameworks that have been proposed use RBAC as the fundamental access control model upon which the framework is built. RBACs limitation is in its ‘Role’ based working which means that for every operational responsibility, a role must be defined. This problem exponentially increases with expansion in the system. At enterprise level, there will be hundreds if not thousands of roles that will contain only one person and of limited usage, limiting access control model’s efficiency.

    - In recent research, ABAC has been proposed as the core access control component for building on the framework. Two biggest flaws in ABAC model are its huge processing cost and its relative novelty. Novelty means that many of ABACs features and attributes are still being worked on and discovered. This adds uncertainty to the working of the e-Healthcare access control model. Secondly, access control decision making in the ABAC based models is done on the attributes associated with a subject and object. A comprehensive access control model will consist of thousands of attributes if based on ABAC. This exerts huge processing cost on the enterprise rendering it unfeasible for large, complex and fast paced environments.
- Legal aspects and requirements are a MUST for any e-Healthcare model to enable its implementation and working in the real world. Research carried out in this regard has been severely lacking. HIPAA, HITECH and GDPR are some of the international standards that are currently in place around EU, US and other developed countries. These regulations establish and determine the privacy and security related requirements to ensure that individual’s privacy and security and ensured. eP2F has been designed taking into account legal and regulatory requirements of these standards and coupling them with other industry information security/management standards to come up with a fully compliant standard. Ensuring compliance not only allows its unhindered operability but also addresses security and privacy requirements.
- With ever increasing focus on security and privacy, a gradual shift has been observed in enterprise e-Healthcare access control systems. Earlier systems were centrally controlled and didn’t allow for individuals decision making w.r.t. their PII/PHI. This contradicts new legal requirements that aim to empower PII/PHI owners aka the patient. Newer solutions have tried to give more decision-making authority to individuals. However, leaving all decision-making to patients and requiring their action for all these activities will not only hinder the patients, it will slow down the enterprise as well. eP2F comes up with the solution that while giving patients control over who accesses their information, does not over-burden them with excessive input for access control decision making. Patients are allowed to make all the important

decisions when it comes to having others access their private and confidential information.

- Dividing eP2F into groups based on user requirements, information available and operational needs, compartmentalize the system. This approach is beneficial not only in terms of security but also in terms of management and efficiency. Since groups are formed based on their common, collective needs and requirements; group level rulesets can be created. This additional level for ruleset definition below the enterprise level works as the middle step between individual and enterprise rulesets. Since groups are partially isolated from other groups, this allows for better monitoring of users accessing information and information being transmitted to and from the group. This in turn, allows enhanced security and confidentiality.
- Within groups, inherent access control rights are defined to provide enterprise and users with a guided template for further access control rights allocation and decision making. Each group has a set of roles that pertain to that specific group and are crucial for that group but have no need to exist outside the group. i.e. nursing staff will exist only in 'Hospital' group while spouse/sibling will exist only in 'Family & Friends' group. Access rights can be transferred among individuals within the group, but they cannot be transferred to others outside the group.
- eP2F allows patient full and complete control over his/her PII/PHI. Individual is defined as the 'originator' of the information thus ultimate manager and custodian. User over the span of time, will allocate rights to various persons for various PII/PHI attributes which are grouped based on their similarity and usage. This allocation can be action based, time based, date based or independent of these parameters. User will also define if the person who is being allocated access rights can delegate these rights to another one in the groups.
- In case an individual is allowed access control rights delegation by the 'Originator', rights will be degraded every time they are allocated to the person other than the initial one allocated by the originator. i.e. RW rights will only remain R, and if the rights are already R only, they will either be allowed after PII/PHR anonymization or not allowed. In case, same level of access

rights are required for the person who is accessing PII/PHR after delegation, ‘originator’ will have to be asked for these.

- Any information that is being shared for R&D will have to shared after anonymization as per HIPAA and GDPR requirements. All PII/PHR attributes that are required to be removed/anonymized by HIPAA and GDPR must be anonymized/removed prior to such information being shared with them. For R&D purposes, anonymized information has to be placed and stored separately from the actual information to minimize the chance of any intended or unintended exposure.

6.3.1 Working Model and Components:

Our healthcare framework has following components that are grouped based on their role, rights and responsibilities into groups that allow easier access management.

- Patient Group
    - Patient: individual who has his/her EHR in the system, who is undergoing treatment/diagnosis.
        - Patient being the information owner is the entity who has the authority to allow/deny access to his/her healthcare information.
        - This patient authorized access is not invoked for every instance. Patient is informed of overall access mechanism and his/her consent is taken. For specific cases of access that lie in the grey area, patient is asked; either to decide on access provisioning on case by case basis or define a ruleset on which access is to be decided.
    - Family/Friends: People who are associated with the patient are entitled to his/her health condition and may have access to see/visit patient.
        - Family, friends can be defined as a ‘role’ and granted certain rights. However, for spouse and/or siblings, extensive access can be granted based on individual’s identity. Using ‘’ this can be limited to individuals within the family, friend’s role. This special ‘caretaker’ can also manage insurance and be the point of approval/consent in case of emergency where patient’s consent cannot be obtained.

- 3rd Parties (Insurance, Government): 3rd parties are any such entities that are accessing and/or processing PHI legally but outside patient-hospital combo. These primarily include government officials and departments working on statistical analysis or insurance providers working in their field.
    - Health insurance provider who is taking care of patient's bills and other monetary expenses.
        - Health insurance providers are responsible for taking care of costs associated with patient's treatment. They are often allowed access to healthcare data under certain non-disclosure agreements (NDA) with the patient.
    - Government or independent bodies accessing PHI statistical data for large scale healthcare analysis.
        - Access by such bodies is usually mandated by states and individuals do not have the option to opt out from sharing their data with them. GDPR however, allows individuals option to opt out from sharing their PII/PHI in some cases.
- Hospital Group
    - Physician: Doctor who is treating the patient.
        - Patient's personal physician, one who is treating the patient and main responsible user for assessing and accordingly deciding on course of action to be taken.
        - Physician can refer for guidance/expertise to other doctors. These doctors can add additional information but cannot alter existing one. Also, they can only refer this information back to the original physician and cannot further refer it.
    - Nursing staff: Staff responsible for patient's medication intake and vitals checking. They can only write against specific information sections which is part of healthcare information.
    - Pharmacist: Staff responsible for providing medication that patient is taking. Pharmacist will have access to healthcare information in order to read prescription, but his write access will only be to financial information in order to put bills there for insurance provider.
- Research Group:

- HIPAA compliant research: Research where individual’s health records are shared for research after; patient approval and, knowing that entity is HIPAA compliant.
- Anonymized research: Research data that is being shared after removal of personal identifiers as per HIPAA requirement (18 PHI identifiers) so that this data cannot be traced back to the individual.

Table 2: eP2F comparison with other Access Control Solutions

Solution Title	Access Control Model	HIPAA/GDPR Compliance for PII/PHR anonymization	Patient Controlled Access Control Decisioning	Information/operations Compartmentalization
eP2F [PROPOSED FRAMEWORK]	Hybrid Access Control	Yes: HIPAA PHRs defined separately.	Yes: Patient allowed access control decisioning on his/her PII/PHE	Yes: Groups defined based on security/operational requirements. Users, Hospital and 3rd parties.
ESPAC [50]	Patient Centric Access Control	No.	Yes: Patient allowed access control decisioning on his/her PII/PHE	Partial. Access rights delegation limited to minimize access rights escalation.
AAPM [52]	Threshold based Access Decisioning	No.	Partial. Patient can define attributes for desired physician.	No.
CPRBAC [53]	Role Based Access Control	No.	No.	Yes. Roles defined to identify various groups based on security/operational requirements.

6.4 Conclusion and Future work

Having seen latest research w.r.t. Privacy preserving in e-Healthcare, it is clear that use of any single technique is not sufficient as it does not take care of all privacy concerns. Understanding unique aspects of e-Healthcare is crucial for better measures to ensure privacy. Privacy needs to be defined in such a way that it considers e-Healthcare's unique environment and its patient's situation. Time and again, in surveys conducted in various regions of the world, underlying issues in this regard have been lack of: precise definition and understanding of Privacy, regulation, inter agency cooperation and conflicting goals among partners. Most importantly, it needs to ensure patient that he/she is the one having access control over his/her PHI/EHR. This research not only provides a review of R&D carried out in this regard but also presents a sketch about privacy preserving mechanism that addresses all major privacy concerns. Architecture abstract given here for privacy preservation in e-Healthcare works under the observation that individual protocols cannot ensure sufficient security and privacy for such a large and complicated enterprise. Solution is to divide patient's PHI/EHR into sections based on privacy and access requirements. This compartmentalization allows for better management as different protocols can be adopted for different PHI/EHR sections having divided them on differing privacy and security requirements. Subsections envisioned are: Patient profile (PP) for family members, Patient health record (PHR) for hospital staff and treatment, Patient insurance ticket (PIT) for healthcare insurance and monetary management and finally, research data (RD) - anonymized for healthcare research. In this way, a secure and privacy preserving healthcare enterprise can be designed that allows for using multiple protocols at different sections of PHI/EHR based on information's security and privacy requirements.

AI and automation have been becoming more and more prominent with each passing year. Designing e-Healthcare systems that are smart and self-adopting in such ways that they learn and evolve over time in ways to mimic user behaviour. This will not only reduce user input and delay in decision making but also improve the overall security and efficiency of the system. This will also prevent any misuse due to system vulnerabilities as decisioning criteria will be formed after calibration and learning.

Bibliography

1. Della Mea, Vincenzo. "What is e-health (2): the death of telemedicine?."*Journal of Medical Internet Research* 3.2 (2001): e22.
2. Baker, Chris R., et al. "Wireless sensor networks for home health care."*Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*. Vol. 2. IEEE, 2007.
3. Varshney, Upkar. "Pervasive healthcare and wireless health monitoring."*Mobile Networks and Applications* 12.2-3 (2007): 113-127.
4. Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications."*Journal of medical systems* 36.1 (2012): 93-101.
5. Giannetsos, Thanassis, Tassos Dimitriou, and Neeli R. Prasad. "People centric sensing and assistive healthcare: Pri vacy challenges and directions."*Security and Communication Networks* 4.11 (2011): 1295-1307.
6. Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications."*Journal of medical systems* 36.1 (2012): 93-101.
7. Alemdar, Hande, and Cem Ersoy. "Wireless sensor networks for healthcare: A survey." *Computer Networks* 54.15 (2010): 2688-2710.
8. Putri, Nia Ramadianti. *Enhancing information security in cloud computing services using sla based metrics*. Diss. Blekinge Institute of Technology, 2011.
9. Verizone 2014 data breach investigation report, figure 19; visited at http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf
10. http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=1
11. http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364
12. Verizone 2015 Protected health information data breach report, figure 7; visited at

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

13. Miao, Fen, et al. "Biometrics based novel key distribution solution for body sensor networks." *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*. IEEE, 2009.
14. Yang, Ji-Jiang, Jian-Qiang Li, and Yu Niu. "A hybrid solution for privacy preserving medical data sharing in the cloud environment." *Future Generation Computer Systems* 43 (2015): 74-86.
15. Rouse, William B. "Health care as a complex adaptive system: implications for design and management." *Bridge-Washington-National Academy of Engineering*- 38.1 (2008): 17.
16. Stanford, Vince. "Pervasive health care applications face tough security challenges." *pervasive computing, IEEE* 1.2 (2002): 8-12.
17. Kulkarni, Prajakta, and Yusuf Öztürk. "Requirements and design spaces of mobile medical care." *ACM SIGMOBILE Mobile Computing and Communications Review* 11.3 (2007): 12-30.
18. Avancha, Sasikanth, Amit Baxi, and David Kotz. "Privacy in mobile technology for personal healthcare." *ACM Computing Surveys (CSUR)* 45.1 (2012): 3.
19. Neela, T. Jothi, and N. Saravanan. "Privacy preserving approaches in cloud: a survey." *Indian Journal of Science and Technology* 6.5 (2013): 4531-4535
20. Egbogah, Emeka E., and Abraham O. Fapojuwo. "A survey of system architecture requirements for health care-based wireless sensor networks."*Sensors* 11.5 (2011): 4875-4898.
21. Kumar, Pardeep, and Hoon-Jae Lee. "Security issues in healthcare applications using wireless medical sensor networks: A survey." *Sensors*12.1 (2011): 55-91.
22. Dehling, Tobias, et al. "Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android." *JMIR mHealth and uHealth* 3.1 (2015).
23. He, Dongjing, et al. "Security concerns in Android mHealth apps." *AMIA Annual Symposium Proceedings*. Vol. 2014. American Medical Informatics Association, 2014.

24. MHV 2008, Microsoft. The HealthVault web-based PHR. Online at http://www.healthvault.com.

25. Avancha, Sasikanth, Amit Baxi, and David Kotz. "Privacy in mobile technology for personal healthcare." *ACM Computing Surveys (CSUR)* 45.1 (2012): 3.

26. www.legalarchiver.org/hipaa.htm

27. whatishipaa.org/hitech-act.php

28. Cohn, Simon P. "Privacy and confidentiality in the nationwide health information network." *Online at http://www. ncvhs. hhs. gov/060622lt. htm*(2006).

29. Sun, Jinyuan, Yuguang Fang, and Xiaoyan Zhu. "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks."*Wireless Communications, IEEE* 17.1 (2010): 66-73.

30. Fernández-Alemán, José Luis, et al. "Security and privacy in electronic health records: A systematic literature review." *Journal of biomedical informatics* 46.3 (2013): 541-562.

31. Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and privacy issues in implantable medical devices: A comprehensive survey."*Journal of biomedical informatics* 55 (2015): 272-289.

32. Abbas, Asad, and Samee U. Khan. "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds." *Biomedical and Health Informatics, IEEE Journal of* 18.4 (2014): 1431-1441.

33. Aggarwal, Charu C., and S. Yu Philip. *A general survey of privacy-preserving data mining models and algorithms*. Springer US, 2008.

34. Riedl, Bernhard, et al. "A secure architecture for the pseudonymization of medical data." *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 2007.

35. Pfitzmann, Andreas, and Marit Hansen. "Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology." (2005).

36. Lysyanskaya, Anna, et al. "Pseudonym systems." *Selected Areas in Cryptography*. Springer Berlin Heidelberg, 1999.

37. Wang, Jian, et al. "Providing privacy preserving in cloud computing." *Human System Interactions (HSI), 2010 3rd Conference on*. IEEE, 2010.

38. Jian et al. “providing Privacy preserving in Cloud Computing”, Human System Interactions (HSI), 2010 3rd conference on, IEEE, 2010.
39. Aamot, Harald, et al. "Pseudonymization of patient identifiers for translational research." *BMC medical informatics and decision making* 13.1 (2013): 75.
40. Pommerening, K., et al. "Pseudonymization in medical research-the generic data protection concept of the TMF." *GMS Medizinische Informatik, Biometrie und Epidemiologie* 1.3 (2005): 2005-1.
41. Riedl, Bernhard, et al. "Pseudonymization for improving the privacy in e-health applications." *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008.
42. Bickford, Julia, and Jeff Nisker. "Tensions between anonymity and thick description when “studying up” in genetics research." *Qualitative health research* 25.2 (2015): 276-282.
43. Agrawal, Rakesh, and Christopher Johnson. "Securing electronic health records without impeding the flow of information." *International journal of medical informatics* 76.5 (2007): 471-479.
44. Alhaqbani, Bandar, and Colin Fidge. "Privacy-preserving electronic health record linkage using pseudonym identifiers." *e-health Networking, Applications and Services, 2008. HealthCom 2008. 10th International Conference on*. IEEE, 2008.
45. Jensen, Meiko, Sven Schäge, and Jörg Schwenk. "Towards an anonymous access control and accountability scheme for cloud computing."*Proceedings-2010 Ieee 3rd International Conference on Cloud Computing, Cloud 2010*. 2010.
46. Huang, Lu-Chou, et al. "Privacy preservation and information security protection for patients’ portable electronic health records." *Computers in Biology and Medicine* 39.9 (2009): 743-750.
47. Elger, Bernice S., et al. "Strategies for health data exchange for secondary, cross-institutional clinical research." *Computer methods and programs in biomedicine* 99.3 (2010): 230-251.
48. Narayanan, Hema Andal Jayaprakash, and Mehmet Hadi Güneş. "Ensuring access control in cloud provisioned healthcare systems." *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*. IEEE, 2011.

49. Younis, Younis A., Kashif Kifayat, and Madjid Merabti. "An access control model for cloud computing." *Journal of Information Security and Applications*19.1 (2014): 45-60.
50. Barua, Mrinmoy, et al. "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing." *International Journal of Security and Networks* 6.2-3 (2011): 67-76.
51. Sun, Jinyuan, Yuguang Fang, and Xiaoyan Zhu. "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks."*Wireless Communications, IEEE* 17.1 (2010): 66-73.
52. Zhou, Jun, et al. "PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System." *Parallel and Distributed Systems, IEEE Transactions on* 26.6 (2015): 1693-1703.
53. Chen, Lingfeng, and Doan B. Hoang. "Novel data protection model in healthcare cloud." *High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on*. IEEE, 2011.
54. Sandhu, Ravi S., et al. "Role-based access control models." *Computer* 2 (1996): 38-47.
55. Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." *Infocom, 2010 proceedings IEEE*. Ieee, 2010.
56. Sainan, Liu. "Task-role-based access control model and its implementation."*Education Technology and Computer (ICETC), 2010 2nd International Conference on*. Vol. 3. IEEE, 2010.
57. Deng, Mina, et al. "A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges." *Cloud Computing (CLOUD), 2011 IEEE International Conference on*. IEEE, 2011.
58. Trust worthy clouds (Tclouds), www.tclouds-project.eu
59. Chen, Feng, et al. "PRECISE: PRivacy-preserving cloud-assisted quality improvement service in healthcare." *Systems Biology (ISB), 2014 8th International Conference on*. IEEE, 2014.
60. Dwork, Cynthia, et al. "Calibrating noise to sensitivity in private data analysis." *Theory of cryptography*. Springer Berlin Heidelberg, 2006. 265-284.

61. Naehrig, Michael, Kristin Lauter, and Vinod Vaikuntanathan. "Can homomorphic encryption be practical?." *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*. ACM, 2011.
62. Henze, Martin, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, Bernhard Rumpe, and Klaus Wehrle. "A comprehensive approach to privacy in the cloud-based Internet of Things." *Future Generation Computer Systems*56 (2016): 701-718.
63. Lee, Namyeon, and Ohbyung Kwon. "A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services." *Expert Systems with Applications* 42, no. 5 (2015): 2764-2771.
64. Anwar, Mohd, James Joshi, and Joseph Tan. "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges." *Health Policy and Technology* 4, no. 4 (2015): 299-311.
65. Mounia, Bouhriz, and Chaoui Habiba. "Big Data Privacy in Healthcare Moroccan Context." *Procedia Computer Science* 63 (2015): 575-580.
66. Sajid, Anam, and Haider Abbas. "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges." *Journal of medical systems* 40, no. 6 (2016): 1-16.
67. Li, He, Jing Wu, Yiwen Gao, and Yao Shi. "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective." *International journal of medical informatics* 88 (2016): 8-17.
68. Parks, Rachida, Heng Xu, Chao-Hsien Chu, and Paul Benjamin Lowry. "Examining the Intended and Unintended Consequences of Organisational Privacy Safeguards Enactment in Healthcare: A Grounded Theory Investigation." *European Journal of Information Systems (EJIS)(accepted 07-May-2016)* (2016).
69. Kamel Boulos, Maged N., Dean M. Giustini, and Steve Wheeler. "Instagram and WhatsApp in Health and Healthcare: An Overview." *Future Internet* 8, no. 3 (2016): 37.
70. Wang, Wei, Lei Chen, and Qian Zhang. "Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation." *Computer Networks* 88 (2015): 136-148.

71. Pussewalage, Harsha S. Gardiyawasam, and Vladimir A. Oleshchuk. "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions." *International Journal of Information Management* 36, no. 6 (2016): 1161-1173.
72. Pankomera, Richard, and Darelle van Greunen. "Privacy and security issues for a patient-centric approach in public healthcare in a resource constrained setting." *IST-Africa Week Conference, 2016*. IIMC, 2016.
73. Puppala, Mamta, et al. "Data security and privacy management in healthcare applications and clinical data warehouse environment." *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. IEEE, 2016.
74. Ama-Amadasun, Marvin Mondale. "Patients and Healthcare Providers' Perceptions Towards Privacy Rights of Patients: An Investigation of Listed Swiss Participating Hospitals."
75. imrana Fatima, Syed, and Saad Siddiqui. "HEALTHCARE IN CLOUD USING MULTI-LEVEL PRIVACY-PRESERVING PATIENT SELF-CONTROLLABLE ALGORITHM."
76. Lavanya, P. M., and P. Valarmathie. "Big Data in Healthcare Using Cloud Database with Enhanced Privacy."
77. Mehraeen, Esmaeil, et al. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." *Global Journal of Health Science* 9.3 (2016): 157.
78. Hassan, Noor Hafizah, and Zuraini Ismail. "INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS: A PRELIMINARY INVESTIGATION." *Journal of Theoretical and Applied Information Technology* 88.2 (2016): 202.
79. Shaikh, Nisar Salim, and S. Y. Raut. "INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY PSMPV: PATIENT SELF-CONTROLLABLE AND MULTI-LEVEL PRIVACY-PROTECTING COOPERATIVE VALIDATION IN DISTRIBUTED M-HEALTHCARE CLOUD COMPUTING."
80. Kumar, Vimal. "Tata Elxsi's Solution Suite for Tackling the Challenges for Wireless Technology in Healthcare."

81. Deshmukh, Pradeep. "Design of cloud security in the EHR for Indian healthcare services." *Journal of King Saud University-Computer and Information Sciences* (2016).