ELICITATION OF SECURITY REQUIREMENTS FOR ERP

A Dissertation submitted in partial fulfilment of the requirement for
the award of degree of

Master of Technology

In

Software Engineering

Submitted by

Kritika Chaudhry

(Roll No. - 2K09/SWE/09)

Under the esteemed guidance of
Dr. Daya Gupta

DEPARTMENT OF COMPUTER ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

BAWANA ROAD, DELHI

2009-20011

CERTIFICATE

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College Of Engineering)
BAWANA ROAD, DELHI – 110042

DATE: _______________

This is to certify that dissertation entitled **"ELICITATION OF SECURITY REQUIREMENTS OF ERP"** has been completed by Ms. Kritika Chaudhry in partial fulfilment of the requirement of Master of Technology in Software Engineering.

This is a record of work carried out by her under my supervision and support during the academic session 2010 -2011. This work will help the security engineers to make the system less vulnerable in the early stages of SDLC thus making system robus

(Dr. DAYA GUPTA)
HOD & PROJECT GUIDE
(Dept. of Computer Engineering)
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI - 110042

ACKNOWLEDGEMENT

It is distinct pleasure to express my deep sense of gratitude and indebtedness to my learned supervisor **Dr. Daya Gupta, HOD, Department of Computer Engineering,** Delhi Technological University, for her invaluable guidance, encouragement and patient reviews. Her continuous inspiration only has made me complete this dissertation. She kept on boosting me time to time for putting an extra ounce of effort to realize this work. She provided the conceptions and theoretical background for this study as well as suggested the rational approach. She remained a pillar of help throughout the project. I would also like to take this opportunity to present my sincere regards to other staff members of Computer engineering Department providing me unconditional and anytime access to the resources and guidance.

Finally, I would like to thank my classmates for their unconditional support and motivation during this work.

(KRITIKA CHAUDHRY)
Master in Technology
(Software Engineering)
Dept. of Computer Engineering
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI – 110042

ABSTRACT

This report addresses the topic of Elicitation of security in Enterprise Resource Planning (ERP) software systems. Specific attention is given in extending a security modelling technique for ERP software packages.

Existing software packages to control business processes are widely accepted and have become the central data repository for most information relating to an enterprise. Each of these systems provides a method by which data may be protected. Access to information may be restricted to authorized users only. To protect the business, access to critical resources must be limited to authorized and authenticated users only.

The aim of this study is to investigate existing security and threats modelling techniques and implement ERP systems in the best available technique for modelling security.

The deliverable of the study is to provide a clear and concise process to provide organizations with a better security requirement elicitation process for ERP. Such an implementation should enable the organization to be aware of problem areas and to be able to address them confidently. Organizations are unsure as to how security requirements are elicitated within their selected product, the methodology proposed by this study should enable such organizations to gain a better understanding of how security could and should be implemented to best effect.

TABLE OF CONTENTS

LISTS OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Introduction

Security is of great concern since last two decades and its importance is growing day by day with the evolution of new techniques and software which needs client interaction, sales, financial information etc to deal with.

ERP is one of such software which deals with the client in many organizations and huge amount of data regarding sales, finance, human resources are stored in it. Since the use of web in every activity of software including ERP increases the inclusion of threats and vulnerabilities while transacting online, thus security is one of the most concerned area for the researchers.

There are already existing techniques and frameworks which deals with the security in software like ERP. These techniques are helpful in elicitating the security features and requirements which are to be embedded in the software.

If there is not a proper security mechanism in the system it can lead to harm, disaster and data loss. Thus security has to be emphasized right from the beginning of software development life cycle(SDLC).

Referring to the security elicitation techniques we can elicitate the security requirements for the ERP.

1.2 General Concepts

Computer security [7] is defined as measures and controls that ensure confidentiality, integrity and availability of the information processed and stored by the computer.

Computer security is a military term which was once used in reference to the security of information stored. But now it can relate either to military or civilian community. It also concerns preventing unauthorized users from gaining entry to a computer system[8].

Computer system may be affected by computer viruses, malicious software, hackers, and Internet frauds. In fact these things have become commonplace in the news. Being consumers, we know the importance of protecting our personal information against the threats. Sometimes we are not even aware that when we logon to our systems whether we are safe or not, or somebody is tracking our system and private data.

Ignoring the computer security is not an option since whole new era heavily relies on web and the software such as ERP which includes client interaction. Software is found in airplanes, chemical factories, hospitals, corporate, military and various other systems and businesses. With the growth of technology the use of software system is increasing with a very good rate. We trust our life, our property and our environment to these software systems. If these systems get attacked by the viruses and intruders, our life, property will be at risk and trust on these systems will be weakened.

Security Requirements can be defined as requirements which provide detail specification of any system that may not be acceptable if the requirements are not implemented properly, For example all child application can only access data for which they are properly authorized and authenticated.

Security engineering is a relatively new and emerging field which deals with following[17,19]-

- *Security requirements specification and management*
- *Implementing security requirements while taking design decisions*
- *Implementing specific algorithms and others mechanism to make system acceptable during the design phase*

Unlike other functional requirements that specify the required capability, security requirement specify what is to be prevented and how to keep the system secure. (For example malicious software, intruders, viruses, attacks due to safety hazards etc.) These requirements also deals with the threats related to the assets. These must be managed in a proper way. Although much research has been done to find out the solution to this aspect of the problem that is, security threats. According to the authors this problem is severe because of the total neglect of sound principles of system design.

1.3 Motivation

Gathering requirements is the first and most mandatory step in developing a computer based system. Requirement engineering [17,18] is a difficult task and any faults or errors in this process can lead to the system which can fail in certain circumstances or which is not up to the expectations. Cost of changing the requirements in the later stages of SDLC is very high. Thus all mandatory requirements should be gathered in the early phase of SDLC using proper steps of requirement engineering so as to build a good quality and reliable system.

Numbers of softwares are developed to incorporate the security mechanism during the design and implementation phase. This is because the security needs are noticed and evaluated once the softwares are implemented. Thus security mechanism applied after the implementation results in the high cost and inefficient system.

Many researchers have proposed the security mechanism that can be incorporated during the requirement phase itself. It seems more fruitful that combining existing approaches together with newly developed approaches will result in development of cost-effective, reliable and efficient system. Therefore we need to have a proper security which should be integrated with requirement engineering process.

An ERP[12] is an information system that provides an automated means of managing a business. The automation and support functions include manufacturing, distribution, personnel, payroll, financials, sales, etc. Thus it contains very critical data.

The integrated and centralized nature[12] of ERP systems should make it clear that security is an important aspect to be considered when implementing an ERP system. As all data is stored in a central repository/database and is potentially open to the entire user population of the organization, a mechanism is required to ensure only authorized users gain access to their relevant information. This is particularly true when human resources data shares the repository with other areas of the organization. To ensure controlled access to all data, most commonly available ERP systems should provide strong mechanisms to protect data from unauthorized access.

If they are attacked by intruders and malicious [10] software then it can lead to disaster and thus making a potential impact on organization and system users. Security requirements are more important for such software since client interaction is an integral part of it. Security feature is incorporated in the softwares like ERP in an adhoc manner. Thus this has to be improved and then developed. We feel that if security requirements along with other functional and non functional requirements are captured for ERP system in its SDLC, can lead to efficient and cost effective system. In other words we wish to apply security engineering to ERP system.

The problem is that to develop a reliable and secure system, requirement engineers needs to find out all such requirements. All the functional and non functional requirements are taken care of by the requirement engineers but they are not trained to deal with security requirements. Most of the requirement teams end up specifying the security design constraints.

Thus from the above facts we can say that we need well defined techniques for discovering security requirements. There are many proposals for elicitating security requirements of information systems.

In our thesis we propose to elicitate the security requirement for software like ERP as to make the software more efficient and robust.

1.4 Related Work

An ERP system controls all the business related information of an organisation as well as information relating to customers and suppliers[10,11]. It is necessary to protect this information from the opposition as well as to ensure that the information within the ERP system is secure. Researchers have been doing a great work for improving the security in ERP since last decade. Following are the work done by researchers to improve the security feature in ERP.

1.4.1 Security moving from Database system to ERP

Riet and janson[14] in 1999 gave the description of how security moved from earlier database system into ERP system. It tells the uses of moving the system from centralized database to the ERP level.

When database systems came along, access control moved to these systems. Security rules were defined in the data model and are centrally maintained. For distributed database systems security rules are also defined centrally and maintained by local database systems. With the coming of so-called ERP systems (ERP standing for Enterprise Resource Planning), security again is moving; now from the database system to the ERP system. [14]

1.4.2 A WFM (work flow management) technique

In ERP then came a technique to define work for employees by means of WFM specification [14]. In this specification the tasks are defined and the order, together with the conditions under which the tasks have to be performed. The tasks concern such things as handling of orders sent in by external clients, treatment of claims in an insurance company or even administering patients in a hospital. Usually, tasks also involve contact with colleagues or superiors for approval or expert advice and dealing with information in the databases. A WFM system is designed to actually direct/aid all employees in their tasks. It uses e-mail facilities and multi-media tools to perform this. It integrates the WFM system with the security procedures in ERP like SAP.

1.4.3 ERPSEC- A framework to enhance security in ERP system

Hertenberger [9]in 2005 presented a method of integrating the concept of information ownership in an Enterprise Resource Planning (ERP) system for enhanced security. In addition to providing enhanced security, the reference framework ERPSEC developed better manageability and eases implementation of security within ERP software packages. The results of this framework indicate that central administration, control and management of security within the ERP systems under investigation weaken security. Central administration of security should be replaced by a model that distributes the responsibility for security to so-called information owners. Such individuals hold the responsibility for processes and profitability within an organization. Thus, they are best suited to decide who has access to their data and how their data may be used. Information ownership, coupled with tight controls can significantly enhance information security within an ERP system.

1.4.4 ERP software requirement elicitation with reference model

Juntao in june 2010 proposed an ERP software requirement elicitation with reference models [15]. It states that ERP systems provide a lot of reusable software packages, which accelerate the implementation process to some extent. However they also put enterprises into a dilemma: whether to adapt as-is business processes or to customize software packages. In order to help the enterprises get out of the dilemma, a holistic methodology is proposed to automatically elicit software requirement using reference models as domain knowledge. The methodology involves three phases: business modelling, gap detection and gap bridging. Firstly, VPML is employed to describe as-is business process, Secondly, semantics computing technology is employed to analyze the gap between enterprise needs and COTS software capacity. At last, Goal Reasoning Technology is employed to encourage enterprise users and software vendors take participate in decision making process together.

But these techniques described do not focus on elicitating security objectives. They are incorporated in adhoc manner.

1.5 Proposed work

The process we will describe here is applying security engineering for ERP system to enhance security features in it. So we are going to incorporate security engineering in ERP to elicitate the security requirements needed in the system which will address all the security issues and then take appropriate design decisions and apply appropriate cryptographic techniques to meet these requirements [40]. This will make system cost effective, efficient and robust.

The different activities performed in the security oriented process are: -

i. **Requirement engineering** – Discover security requirement along with functional and non functional requirements.

ii. **Design Decisions** – With true security requirements specified most appropriate design decisions can be taken along with usual designing quality attributes. This needs selecting appropriate cryptographic techniques [17,40].

iii. **Implementation** – The decisions should finally be implemented.

Viewpoint oriented and Tropos [20,21,17]methodologies are very recent techniques applied to elicitate security requirement, we shall be applying these techniques to elicitate security requirements for ERP system. Our problem is to discover security objectives of ERP using viewpoint and secure tropos.

We have used two methodologies i.e. view point oriented security requirement elicitation process(VOSREP) and secure tropos, firstly for experiment purpose and secondly to ensure that the security objectives are discovered for application.

Also a tool is developed which helps to elicit the security requirements of software like ERP using view point oriented security requirement engineering process and tropos[20,21] process. This tool also contains a GUI to create graphs for secure tropos methodology.

The advantage of using this approach for engineering security requirements of ERP helps in the identification of true security requirements. With true security requirements have been identified, systematically analyzed and specified the architecture team can choose most appropriate security mechanisms to implement them and thus making the ERP more efficient, reliable and secure.

1.6 Thesis statement and outline

The aim of this thesis is to provide security requirement engineering process, which will elicitate the security requirements of ERP along with functional and non functional requirements. The approach used for finding out the security requirements can help to make a system more robust, secure and cost effective.

Chapter 2 will state overview of ERP and frameworks developed in ERP to enhance its security and state of art techniques which can be used to elicitate the security requirements.

Chapter 3 explains view point oriented security requirement process and tropos approach to elicitate security req. Of ERP

Chapter 4 will be a case study implementing these above two methodologies

Chapter 5 provides the details of implementation of the tool for the security elicitation methodologies discussed i.e. viewpoint and tropos.

Chapter 6 concludes the thesis

Chapter 7 list the references I have gone through during my research

Chapter 2

OVERVIEW OF ERP AND SECURITY REQUIREMENT ELICITATION TECHNIQUES

In this chapter we first describe overview of ERP followed by framework proposed by researchers to achieve security in ERP. We then survey the literature for techniques for elicitating security requirements.

2.1 ERP overview

ERP or Enterprise Resource Planning [10,11]refers to a software architecture which is used to manage internal and external resources by the integration of business management practices and modern technology. It attempts to integrate all the department and respective functions of a company into a single computer system that can serve all the different needs of the departments'. ERP is a combination of three important components- Business Management Practices, Information Technology and Specific Business Objectives.

The definition provided by Mario salex and drou [10] states :-

ERP (Enterprise Resource Planning) is an industry term for the broad set of activities supported by multi-module application software that help a manufacturer or other business manage the important parts of its business, including product planning, parts purchasing, maintaining inventories, interacting with suppliers, providing customer service, and tracking orders.

2.1.1 A brief history of ERP

From a historical perspective, companies have always relied on hand-written ledgers to keep track of income and expenditure. The birth of the spreadsheet application allowed accountants to track similar data in more detail. The ability to control larger portions of the organization was possible once custom or tailor-made software programs where created to allow orders, sales details and ledger information to be saved in one or more databases[16].

A particular type of software developed specifically for the manufacturing industry provided the basis for today's ERP systems. The Materials Requirements Planning (MRP) application served as the method for planning and scheduling materials for complex manufactured products.

The MRP application was developed primarily for mainframe computers and provided many companies with a competitive advantage. The term ERP (Enterprise Resource Planning) was first introduced in the early 1990's when MRP-II was extended to cover areas like finance, human resources and project management.

2.1.2 Architecture of an ERP system

Generic ERP system architecture includes the repository and application layer. The end user interacts with the ERP system through a terminal or workstation. Generally, the workstation front-end software for the ERP system is easy to use and provides the user with a pleasant environment. Using the front-end software on his workstation, the user is able to perform all required functions directly from the comfort of his desk. Due to the integrated nature of ERP systems, a manager may be able to view all financial, sales and production data directly from a head office location. This is possible even if the sales and production locations are physically separated from the head office.[14]

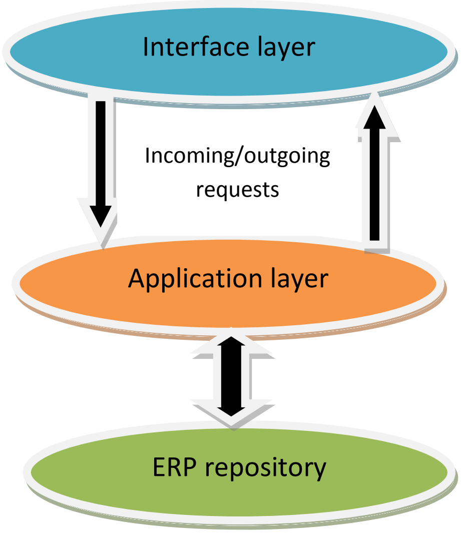


Figure 1: Generic ERP system architecture

2.1.3 Advantages of ERP system

i. Faster inventory turnover by providing increased efficiency and automation of processes such as production planning and procurement

ii. Improved customer service by ensuring that goods in demand by customers are available

iii. Improved accuracy of inventory counts as compared to physical inventory

iv. Timely revenue collection and improved cash flow by providing financial management information that is updated and maintained in real time

v. Higher employee satisfaction by providing powerful functionality at the desktop level.

2.1.4 Security issues in ERP system

The balance between making data available to the users that need it and denying it from those who should not have access is not easy to achieve. To manage this risk your company needs to implement an appropriate access strategy. [13]

Various security issues considered in ERP are –

i. How to get certain that sensitive information is not displayed to unintended user.

ii. To ensure that critical functions only be performed by the right people in your organization.

iii. Ensure that the ERP system used give your users access to all the relevant information, to make the optimum decisions

iv. E-Commerce requirements have a security plan developed

v. Users are not confident that they have appropriate security and control over their data

vi. Network in ERP is not reliable

vii. Issues on how to eliminate the disclosure of confidential information

viii. How to comply with internal and external audit requirements

2.2 Security techniques related to ERP

An ERP system[15] controls all the business related information of an organisation as well as information relating to customers and suppliers. It is necessary to protect this information from the opposition as well as to ensure that the information within the ERP system is secure.

Researchers have been doing a great work for improving the security in ERP since last decade. Following are the work done by researchers to improve the security feature in ERP.

2.2.1 Security moving from Database system to ERP

Riet and janson[14] in 1999 gave the description of how security moved from earlier database system into ERP system. It tells the uses of moving the system from centralized database to the ERP level.

When database systems came along, access control moved to these systems. For distributed database systems security rules are also defined centrally and maintained by local database systems. With the coming of so-called ERP systems (ERP standing for Enterprise Resource Planning), security again is moving; now from the database system to the ERP system. [14]

Following figures shows relation between the traditional database system and ERP system.

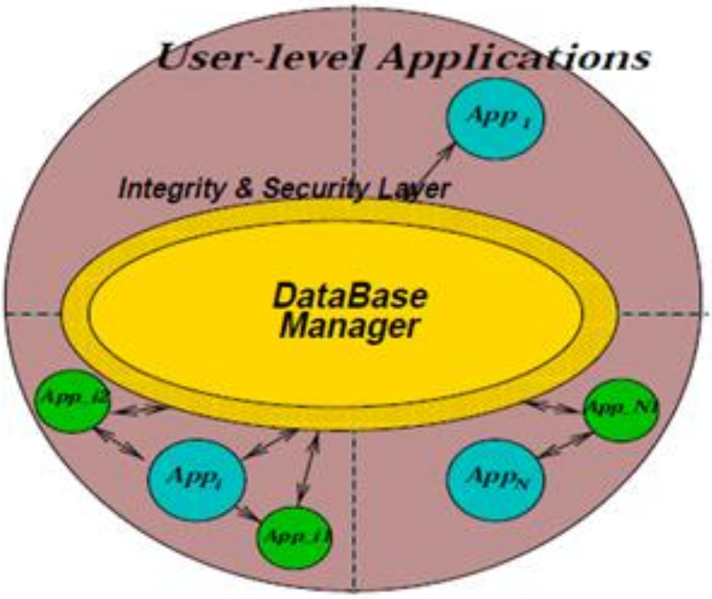


Figure 2: security in traditional database system

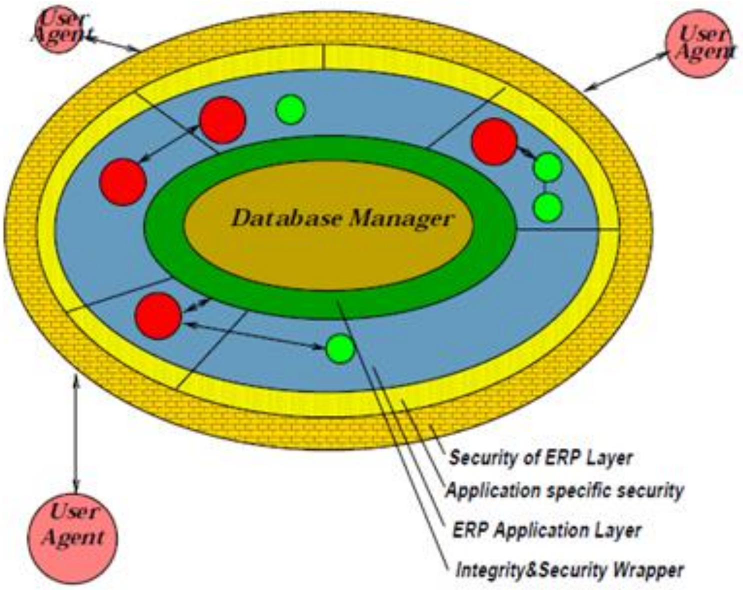


Figure 3: Security in proposed ERP system

Earlier in databases all the application were directly connected to the centralized database. But now there comes application specific security and security ERP layer in between the application and the database.

2.2.2 A WFM (work flow management) technique

In ERP then came a technique to define work for employees by means of WFM specification [14]. In this specification the tasks are defined and the order, together with the conditions, under which the tasks have to be performed. The tasks concern such things as handling of orders sent in by external clients, treatment of claims in an insurance company or even administering patients in a hospital. Usually, tasks also involve contact with colleagues or superiors for approval or expert advice and dealing with information in the databases.

A WFM system is designed to actually direct/aid all employees in their tasks. It uses e-mail facilities and multi-media tools to perform this. It integrates the WFM system with the security procedures in ERP like SAP.

2.2.3 ERPSEC- A framework to enhance security in ERP system

Hertenberger in [9] 2005 presented a method of integrating the concept of information ownership in an Enterprise Resource Planning (ERP) system for enhanced security. In addition to providing enhanced security, the reference framework ERPSEC developed better manageability and eases implementation of security within ERP software packages. The results of this framework indicate that central administration, control and management of security within the ERP systems under investigation weaken security. Central administration of security should be replaced by a model that distributes the responsibility for security to so-called information owners. Such individuals hold the responsibility for processes and profitability within an organization. Thus, they are best suited to decide who has access to their data and how their data may be used. Information ownership, coupled with tight controls can significantly enhance information security within an ERP system.

2.2.4 ERP software requirement elicitation with reference model

Juntao in june[16] 2010 proposed an ERP software requirement elicitation with reference models. It states that ERP systems provide a lot of reusable software packages, which accelerate the implementation process to some extent. However they also put enterprises into a dilemma: whether to adapt as-is business processes or to customize software packages. In order to help the enterprises get out of the dilemma, a holistic methodology is proposed to automatically elicit software requirement using reference models as domain knowledge. The methodology involves three phases: business modelling, gap detection and gap bridging. Firstly, VPML is employed to describe as-is business process, Secondly, semantics computing technology is employed to analyze the gap between enterprise needs and COTS software capacity. At last, Goal Reasoning Technology is employed to encourage enterprise users and software vendors take participate in decision making process together.

But they fail to incorporate security needs of requirement phase. Hence we shall survey literature for dictating security requirements and apply appropriate techniques to do requirement engineering for ERP.

2.3 Requirement Engineering

It is the process of establishing the services that the customer requires from a system and the constraints under which it operates and is developed. The requirements are nothing but are the descriptions of the system services and constraints that are generated during the requirements engineering process.[17,18]

Requirements can be classified as -

- Functional Requirements,
- Non Functional Requirements and
- Domain Requirements.

Functional Requirements

Functional Requirements of a system describe functionality or System services. Functional requirements may vary depending on the type of software, expected users and the type of system where the software is used.

Examples –

- The user should be able to search either all of the initial set of databases or select a subset from it.
- The system should provide viewers for the user to read documents in the store.

Every order shall be allocated a unique identifier (ORDER_ID) which the user shall be able to track the order of the items purchased by them.

Non Functional Requirements

Non Functional Requirements are those that define system properties and constraints for ex reliability, security and response time.

Non-functional requirements may be more important than the functional requirements. If these requirements are not met, then system is useless.

Domain Requirements

Domain requirements can be defined as the requirements which are derived from the application domain and describe system characteristics and features that reflect the domain. Domain requirements be new functional requirements, constraints on existing requirements or define specific computations. Again the problem with domain requirements is if they are not satisfied, the system may be unworkable.

Examples –

The domain requirement for a LIBSYS can be that there shall be a standard user interface to all databases which shall be based on the ISO standard.

One of the process for requirement elicitation is View Point Oriented Requirement Definition (VORD)

The process of eliciting the requirements as according to view points is called as view point oriented requirements definition [17]. Viewpoints now fall into two classes –

a. Direct viewpoints – These correspond directly to clients in that they receive services from the system and send control information and data to the system. Direct viewpoints are either system operators/users or other sub-systems which are interfaced to the system being analyzed.

b. Indirect viewpoints – Indirect viewpoints have an ‘interest’ in some or all of the services which are delivered by the system but do not interact directly with it. Indirect viewpoints generate requirements which constrain the services delivered to direct viewpoints.

There are two steps in the VORD as defined by Sommerville which are as follows –

- View Point Identification.
- And documenting View Points.

View Point Identification

The method of **viewpoint identification** which is proposed by Sommerville involves a number of stages –

- Prune the viewpoint class hierarchy to eliminate viewpoint classes which are not relevant for the system under question.
- Consider the system stakeholders. If the stakeholders fall into classes which are not part of the organizational class hierarchy, add these classes to it.
- Identify sub-system viewpoints, using system architecture. This model may either be derived from existing system models or may have to be developed as part of the Requirement Engineering process.
- System operators are identified who use the system on a regular basis on occasional basis and who request others to use the system for them. All of them are crutial viewpoints.
- Roles for each of the indirect viewpoint are considered.

Documenting View Point

Viewpoints have an associated a set of requirements, sources and constraints. Viewpoint requirements are made up of a set of services (functional requirements), a set of non-functional requirements and control requirements. Control requirements describe the sequence of events involved in the interchange of information between a direct viewpoint and the intended system. Constraints describe how a viewpoint's requirements are affected by non-functional requirements defined by other viewpoints.

2.4 Security elicitation methodologies used in software engineering

Security Requirements can be defined as the requirement that gives detail specification of any online system that may not be acceptable such as all child application can only access data for which they are properly authorized and authenticated.

2.4.1 Different types of security requirements

There are various types of security requirements proposed by firesmith [17,18]

- **Identification Requirement**: Identification requirement specifies the extent to which the system shall identify its users and other applications that actually uses the system.

- **Authentication Requirement:** It is the security requirement that specifies the extent to system should verify the identity of its users which can be human user, system stakeholders or other applications integrated with it The typical objective of this security requirement is to ensure that externals are actually who or what they claim to be. They are not independent of Identification requirements, and many applications will group them together.

- **Authorization Requirement:** This requirement specifies the extent to which authenticated externals can access specific application, capabilities or information. This requires that System administrator will pre decide the privileges, functionalities permitted to external and he shall be allowed to access for which they are explicitly specified.

- **Immunity Requirement:** An immunity requirement is any security requirement that specifies an extent to which application shall protect itself from infection by unauthorized and undesirable programs such as computer viruses, worms, and Trojans.

- **Integrity Requirement:** This security requirement is meant to ensure that system data does not get corrupted intentionally via unauthorized creation, deletion, modification.

- **Intrusion detection Requirements:** This security requirement specifies that if an application has been attacked by intruders then that can be detected and recorded so that the administrator can handle them.

- **Non-repudiation Requirements:** This security requirement specifies the extent to which system shall maintain tamper proof record of all accesses made to it by different users. This may be required to avoid future legal and liability problems that a party should not deny after interacting (e.g. transaction) with all or part of the interaction.

- **Privacy Requirements:** This security requirement specifies the different types of privacy to be maintained by the system so that the application is able to keep its data and communications private from unauthorized individuals and programs. Also its objective is to minimize user’s confidence and bad press comments.

- **Security Auditing Requirements:** A security auditing requirement specifies that a system shall enable security manager to audit the status and use of its security mechanisms. This helps security team to analyze information about various security mechanisms it has implemented and review them.

- **Survivability Requirements:** The security requirement specifies the range to which an application should work possibly in degraded mode even if some intentional destruction loss of data has been there in the application. They are different from robustness requirements which prevent the system from hardware or human error.

- **System Maintenance requirements:** This requirement specifies system maintenance against accidentally modifications of security mechanism deployed by i It means during usage of the system all security mechanism deployed by the system should be maintained and reviewed.

- **Physical Maintenance requirements:** This security requirement specifies the extent to which system shall protect itself from physical damages such as destruction, theft of computer or replacement of its hardware or software due to sabotage or terrorism.

2.4.2 Various methods to elicitate security requirements

i.) **Attack Trees -** Attacks trees[6]are a way to represent the attacks using the most widely used data structure Trees. In this method the attack is represented with the attacker goal as the root node and the different ways of achieving that goal as leaf nodes. Satisfying a tree node represents either satisfying all leaves (AND) or satisfying a single leaf (OR). The value of attack tree analysis is derived from the attributes associated with each of the nodes.

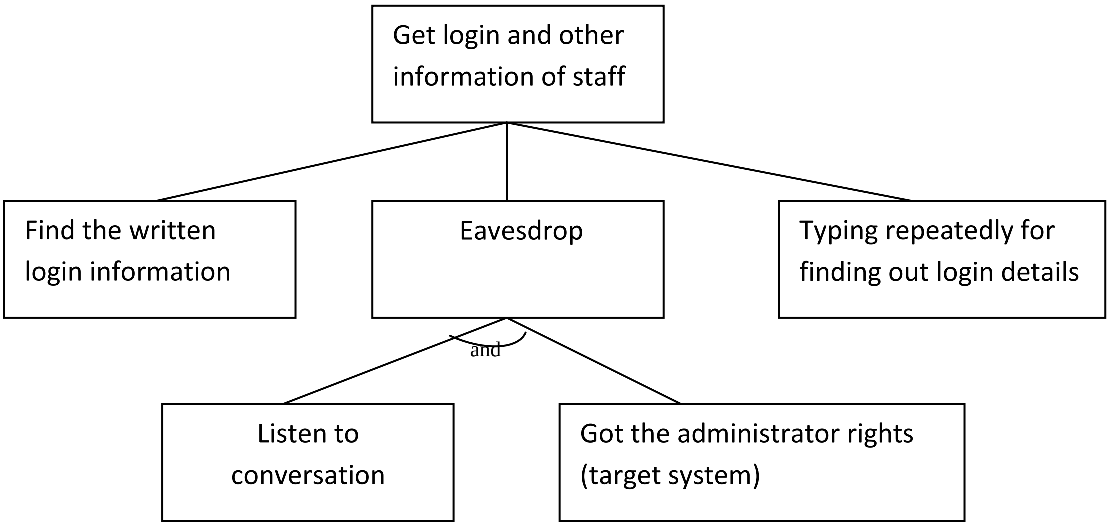

Get login and other information of staff
Find the written login information
Eavesdrop
Typing repeatedly for finding out login details
and
Listen to conversation
Got the administrator rights (target system)

Figure 4: Attack tree for college registration

ii.) **Abuse Cases** – Abuse case [4] is a specification of complete interaction between a system and one or more actors, where the interaction can cause harm. A complete abuse case defines an interaction between an actor and the system that results in harm to a resource associated with one of the actors, one of the stakeholders, or the system itself. A further distinction we make is that an abuse case should describe the abuse of privilege used to complete the abuse case. Clearly, any abuse can be accomplished by gaining total control of the target machine through modification of system software or firmware. Abuse cases can be described using the same strategy as for use cases. We distinguish the two by keeping them separate and labelling the diagrams. Figure 5,6 are showing the concept with the example Railway reservation system.

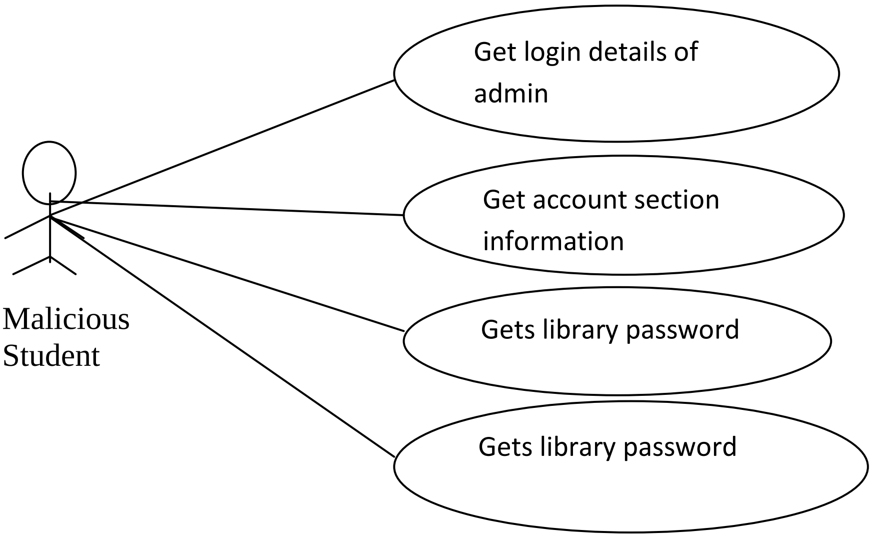


Figure 5: Abuse case for student

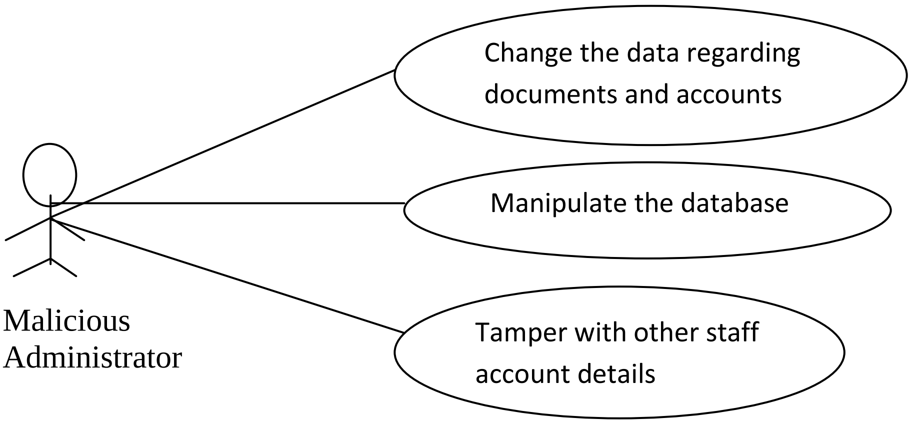

Change the data regarding documents and accounts
Manipulate the database
Tamper with other staff account details
Malicious Administrator

Figure 6: Abuse case for college management

iii.) **Misuse Cases** – This approach described [1, 2] is an extension of use-case diagrams. A use case generally describes behaviour that the system/entity owner wants the system to perform while Misuse cases apply the concept or behaviour that the system's owner does not want to occur. Use case diagrams are driven by goals of the system misuse are driven by threats to the system. For example misuse case for college registration system is shown below.

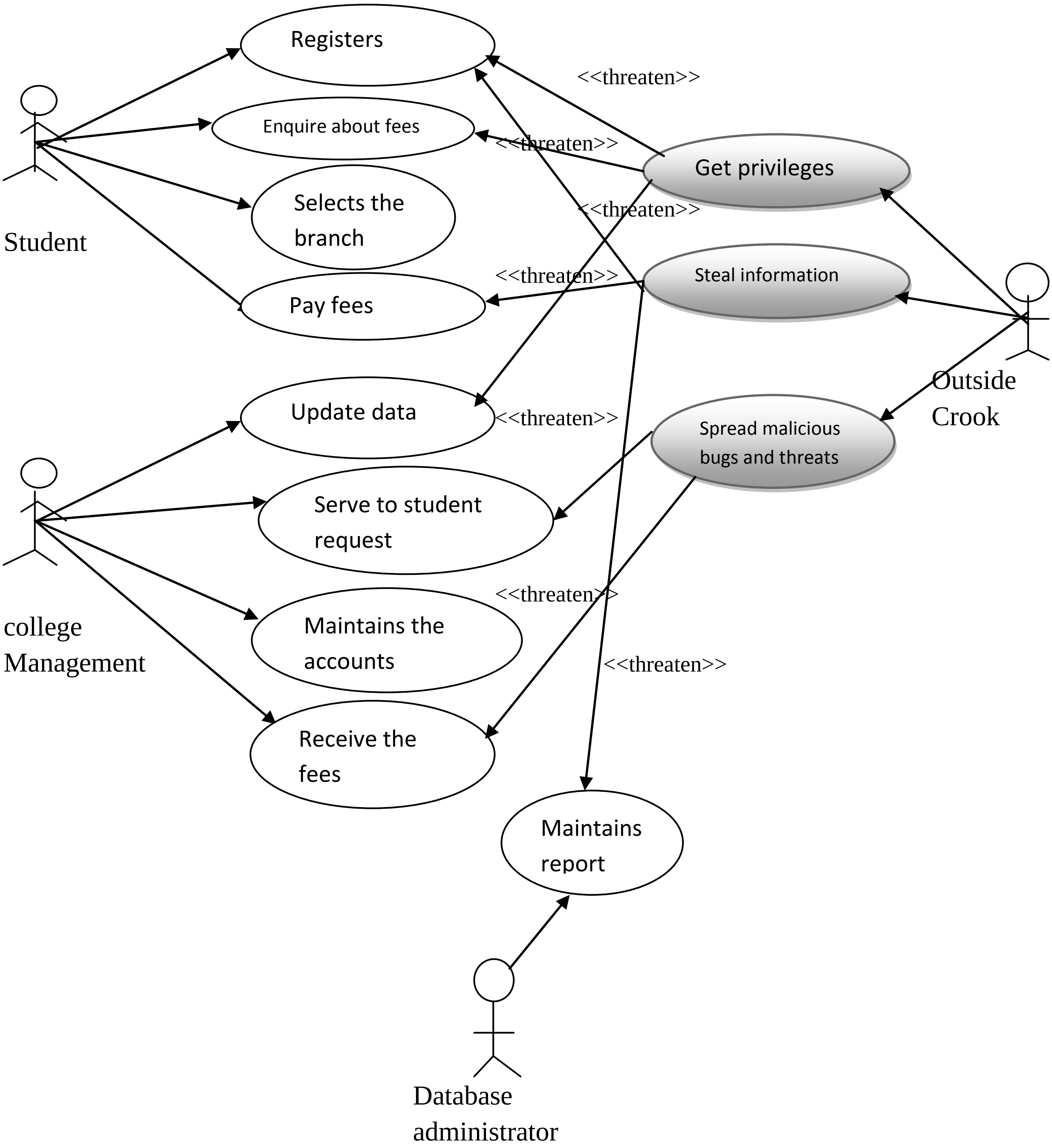


Figure 7: Misuse case example for college registration system

iv.) Security Use Cases - This approach by Firesmith [18] says that misuse cases[2] are highly effective ways of analyzing security threats but are inappropriate for the analysis and specification of security requirements, Because the success criteria for a misuse case is a successful attack against an application while the security use cases specify requirements that the application shall successfully protect itself from its relevant security threats.

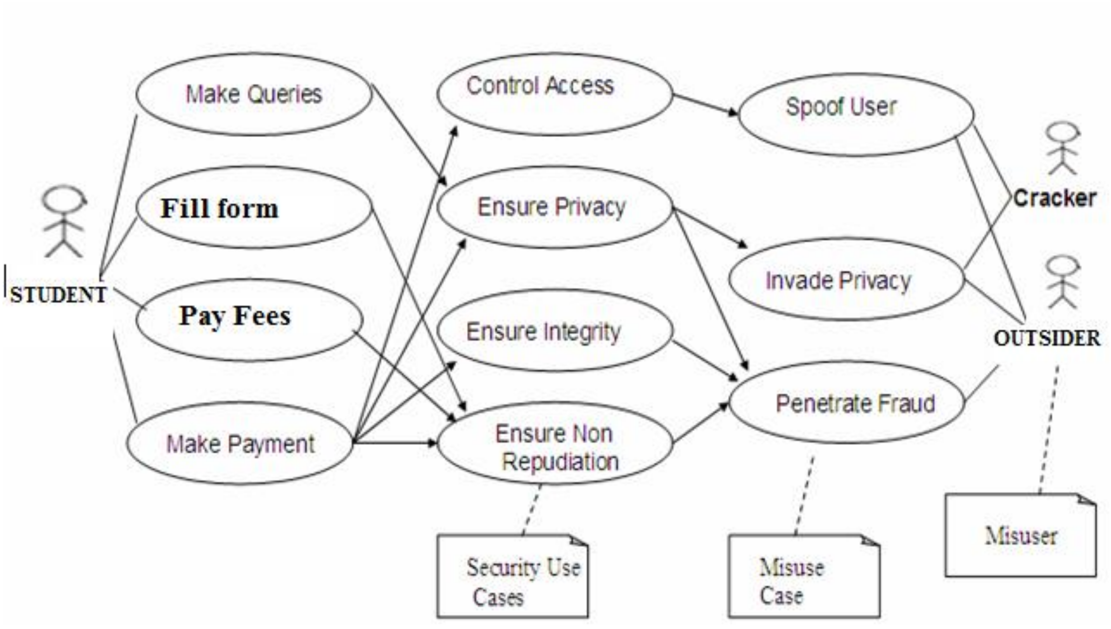


Figure 8: Security use case for college registration system

v.) Trust assumptions – A trust assumption[32] is an acceptance by a requirements engineer that the membership or specification of a domain can depend on certain stated properties, up to some stated level, in order to satisfy a security requirement. The requirements engineer trusts the assumption to be true. These assumed properties or assertions act as domain restrictions; they restrict the dependent domain in some way. A trust assumption is represented by an arc from the dependent domain to an oval describing the properties being depended upon. Adding a trust assumption serves two purposes. The first is to document the ways in which the requirements engineer chooses to trust the behavior of domains that are in the context for some reason. The second, which follows from the first, is to explicitly limit the scope of the analysis to these domains in the context. To illustrate the latter, assume the existence of a requirement stipulating that the computers operate for at least eight hours in the event of a power failure. The requirements engineer can satisfy this requirement by adding backup generators to the system. Appropriate phenomena would be added to detect the power loss, control the generators, detect going beyond eight hours, etc. In most situations, the requirements engineer can trust the manufacturer of the generators to supply equipment without trapdoors that permit an attacker to take control of the generators.

thereby restricting the domain to contain generators without trapdoors. By making this trust assumption, the requirements engineer does not need to include the supply chain of the generators in the analysis.

vi.) Intensional antimodel – Steps in making an intentional anitmodel are[44]:-

- Get initial anti-goals by negating relevant Confidentiality, Privacy, Integrity and Availability goal specification patterns instantiated to sensitive objects from the object model.

- For each such anti-goal, elicit potential attacker agents that might own the anti-goal, from questions such as "WHO can benefit from this anti-goal?" (Application specific specializations of known attacker taxonomies may help answering such questions).

- For each anti-goal and corresponding attacker class(es) identified, elicit the attacker's higher-level anti-goals from questions such as "WHY would instances of this attacker class want to achieve this anti-goal?". Such questions may be asked recursively to elicit more and more abstract anti-goals yielding threat rationales together with other potential threats from alternative refinements of those higher-level anti-goals.

- Elaborate the anti-goal AND/OR graph by AND refining/abstracting anti-goals along alternative branches, with the aim of deriving terminal anti-goals that are realizable either by the identified attacker agents or by attackes software agents. The former are anti-requirements assigned to the attacker whereas the latter are vulnerabilities assigned to the attackers. (This step may be performed informally by asking HOW/WHY questions, or formally by regression through the goal model and the domain theory or by use of refinement patterns and obstruction patterns .)

- Derive the object and agent anti-models from antigoal specifications. The boundary between the antimachine (under the attacker's control) and the anti environment (which includes the software attackee) are thereby derived together with monitoring/ control interfaces.

- AND/OR-operationalize all anti-requirements in terms of potential capabilities of the corresponding attacker agent – the latter may include blind or intelligent searching, eavesdropping, deciphering, spoofing, cookie installation, etc.

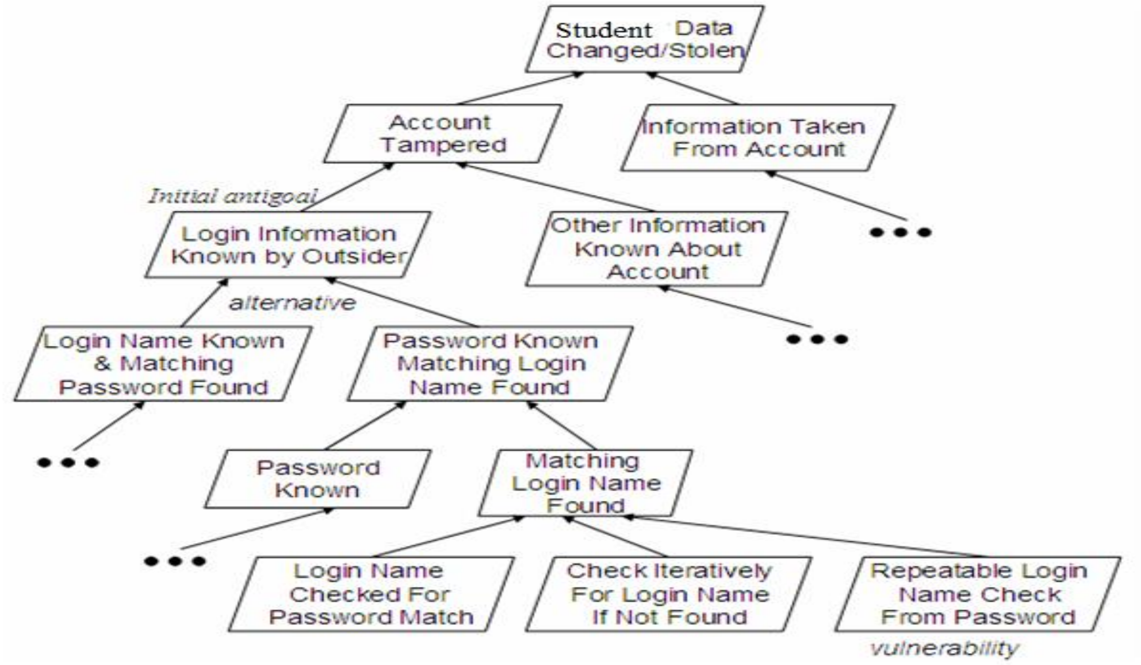

Student Data Changed/Stolen
Account Tampered
Information Taken From Account
Initial antigoal
Login Information Known by Outsider
Other Information Known About Account
alternative
Login Name Known & Matching Password Found
Password Known Matching Login Name Found
Password Known
Matching Login Name Found
Login Name Checked For Password Match
Check Iteratively For Login Name If Not Found
Repeatable Login Name Check From Password
vulnerability

Figure 9: Intentional Anti Model for College registration System

vii.) Common criteria – This approach specifies how standards such as common criteria [3, 41] can be correlated with use case diagrams. The purpose of correlating use case and common criteria is to handle security in IT products during the software engineering process itself. It has following steps -

• For the Purpose of correlating common criteria with use case diagrams the approach makes it mandatory to complete the actor profiles for each actor involved in the use case diagram.

• Actor profile has seven fields consisting of:

• Its name

• Functionality

Type of Actor that may be

a. Human

b. Corporative

c. Autonomous

• Location

a. Local

b. Remote

• Use Case Association

a. Read

b. Write

c. read_write

d. ask

e. answer

f. ask answer

- Whether or not the use case involves exchanging private information
- Whether or not the use case involves secret information exchange.
- After the use case creator completes the actor profiles, these actor profiles are used to maps vulnerable threats to the actor from a predefined set of threat categories. As it has maintained threat repository so we can get threats by completing the threat profile as shown in Table 1. Now these threats are used to find out the security requirements.

Association (read)	**Association (write)**
Impersonate Repudiate_Receive If(Private Exchange = true) Privacy_Violated If(Secret Exchange = true) Data_Theft If(Location = remote) Outsider	Change_Data Repudiate_Receive If(Private Exchange = true) Privacy_Violated If(Secret Exchange = true) Data_Theft If(Location = local) Insider

Table 1: How threats are found when actor type is direc

Viii.) Tropos and Secure Tropos

Tropos is a software development methodology which aims at building agent oriented systems [20,21]. It is based on i* [22] which offers the notions of actor, goal and (actor) dependency. Those notions are used to model early and late requirements, architectural and detailed designs. In this chapter we are thus going to present the concepts of Tropos which will be used to elaborate the security in the softwares like ERP.

We first present the different Tropos phases, followed by the different modelling activities and Tropos diagrams.

Tropos Phases and modelling activities

Tropos is basically composed of 5 phases:

The first phase is the "Early requirements". During this phase, different stakeholders are identified. Stakeholders are generally actors, which are involved in the domain of the software system. An actor can depend on other actors for goals to be achieved and plans to be performed and resources to be supplied.

Actor diagram notations used in Tropos

The second phase i.e. late requirements, the model built during the previous phase is extended with a new actor: the system-to-be. Moreover, the dependencies between this new actor and the ones described in the early requirements phase are added. These dependencies define the functional and non-functional requirements of the system-to-be.

The third phase i.e. Architectural design phase defines the architecture of the system-to-be in terms of subsystems. These subsystems are interconnected through the data and control flows. Subsystems are represented as actors, while the data and control flows are represented as dependencies.

The fourth phase i.e. Detailed design phase, the internal structure of the different agents identified in the previous step is defined and the interactions of those agents are specified.

The final step is Implementation phase. Implementation is made in the development language chosen during the earlier phase. One has to follow the design specifications defined in the detailed design phase.

Modelling Activities in tropos

We will describe the various activities used in secure tropos which helps in building a secure model of the system.

First modelling step is actor modelling step. In this different stake holders are identified and analysed [20].

Second modelling i.e. dependency modelling consists of "identifying actors which depend on one another for goals to be achieved, plans to be performed and resources to be furnished"

Third modelling is goal modelling. It focuses on actors and goals analysis. Three reasoning techniques are used- means-end analysis, contribution analysis and decomposition. Means-end analysis helps in finding the different plans, resources and goals which can achieve a goal. The contribution analysis helps in finding the goals which can contribute, positively or negatively, to a given actor's goal. The and/or decomposition aims at decomposing the original goal into sub-goals.

Fourth modelling technique is the plan modelling. This analysis focuses on plans. This technique is the same as the goal modelling except that the object of the analysis is the plan.
A goal diagram is graphical representation of goal and the plan modelling [20].

The last modelling activity is the capability modelling. During the capability modelling, the capabilities of the sub-systems are delimited. Those capabilities represent "the ability of an actor of defining, choosing and executing a plan for the fulfilment of a goal.

Security in Tropos

Security has been mainly ignored and very little work has been taken place in order for agent oriented software engineering methodologies to support security concerns during the development stages.[21] Following concepts and notations has been included in earlier tropos, to make this agent oriented methodology secure.

Constraints

Constraints are limitations (restrictions) that do not permit specific actions to be taken or prevent certain objectives from being achieved.

Security Modelling Features

Concepts of security diagram, security constraint, secure dependency, and secure goal, task, and resource are introduced in order to felicitate the security in tropos.[22]

Security Diagram

A security diagram is constructed after analysing the security requirements of the system-to-be and its environment and it is similar to the security catalogue first introduced. This process usually involves identification of the security needs of the system and then problems related to the security of the system (such as possible threats and vulnerabilities) and possible solutions to the security problems.

Security mechanisms identify possible protection mechanisms of achieving protection objectives. In order to represent security mechanisms we are employing the concept of a task. A task represents a way of doing something, such as the satisfaction of a goal. However, it must be noticed that tasks (security mechanisms) can contribute positively (+) but also negatively (-) to different protection goals. The following figure shows the above mentioned Concepts and how they are graphically represented in the security diagram.[22]

Secure Entities

The term secure entities involve any secure goals, tasks and resources of the system. A secure entity is introduced to the actor (or the system) in order to help in the achievement of a security constrain [21,22] These terms are included in the tropos modelling to introduce security feature.

For example various security constrains and other secure entities are shown below :-

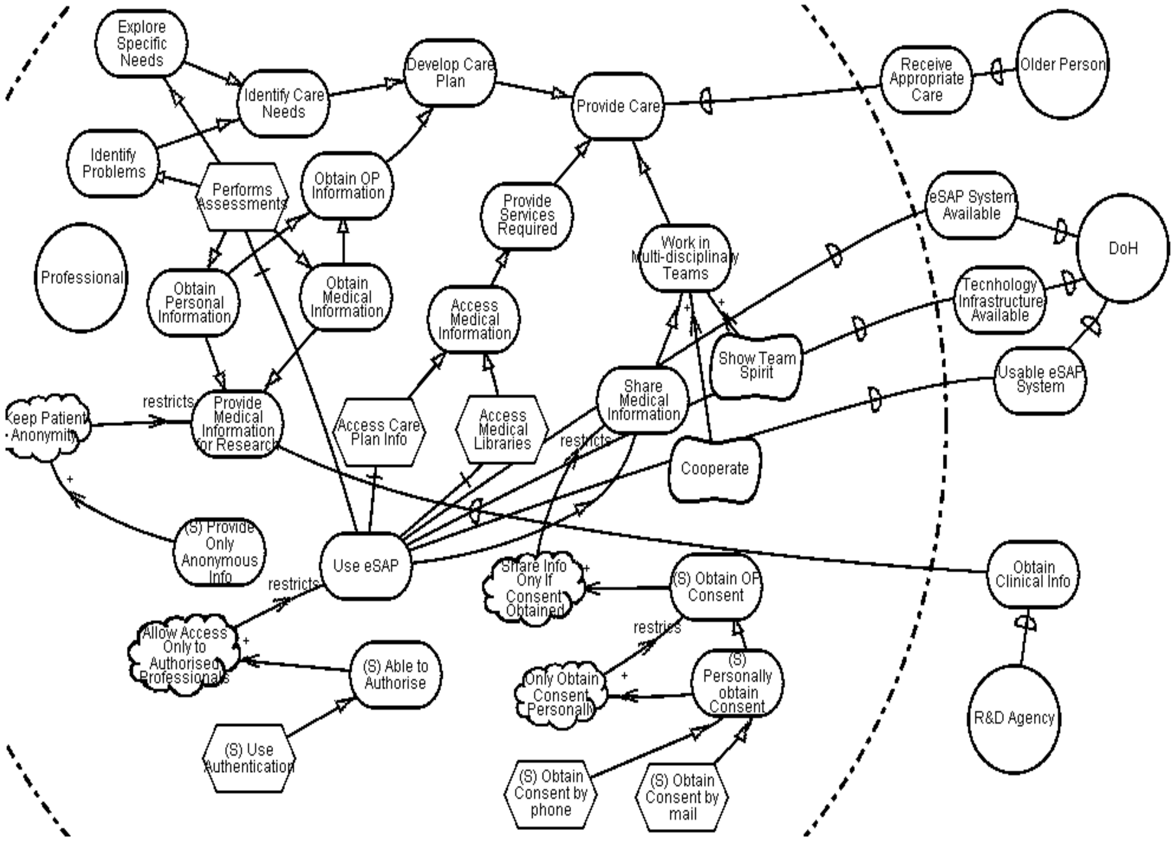

Explore Specific Needs
Identify Care Needs
Develop Care Plan
Provide Care
Receive Appropriate Care
Older Person
Identify Problems
Performs Assessments
Obtain OP Information
Provide Services Required
Work in Multi-disciplinary Teams
eSAP System Available
DoH
Professional
Obtain Personal Information
Obtain Medical Information
Access Medical Information
Tecnhology Infrastructure Available
Show Team Spirit
Usable eSAP System
Keep Patient Anonymity
restricts
Provide Medical Information for Research
Access Care Plan Info
Access Medical Libraries
Share Medical Information
restricts
Cooperate
(S) Provide Only Anonymous Info
Use eSAP
Share Info Only If Consent Obtained
(S) Obtain OP Consent
Obtain Clinical Info
restricts
Allow Access Only to Authorised Professionals
(S) Able to Authorise
restricts
Only Obtain Consent Personally
(S) Personally obtain Consent
R&D Agency
(S) Use Authentication
(S) Obtain Consent by phone
(S) Obtain Consent by mail

Figure 10: Representation of various stake holder and security used in tropos

ix.) View point oriented security requirement elicitation process (VOSREP):

Very recently a software process which is an extension of spiral model presented by Gupta[18,19r,32] consisting phases of requirement engineering, design, implementation. In other words a framework is presented for requirement engineering and design engineering where security requirements are embedded in the earlier phases. Also a framework for requirement engineering is presented.

- Requirement elicitation [32] with functional, non-functional security requirements are also elicitated.
- Based on the security requirements, corresponding design decisions are taken.
- Also in the implementation phase they have stated various techniques like ECC etc.

As our interest is only in discovery of security requirements for ERP, we present overview of requirement discovery techniques in this phase.

Security Requirements Discovery and Definition

It is the first activity of the VOSREP[32] process. Different steps in this process are:-

a. Identify various stakeholders (actors) of the system using view-point analysis

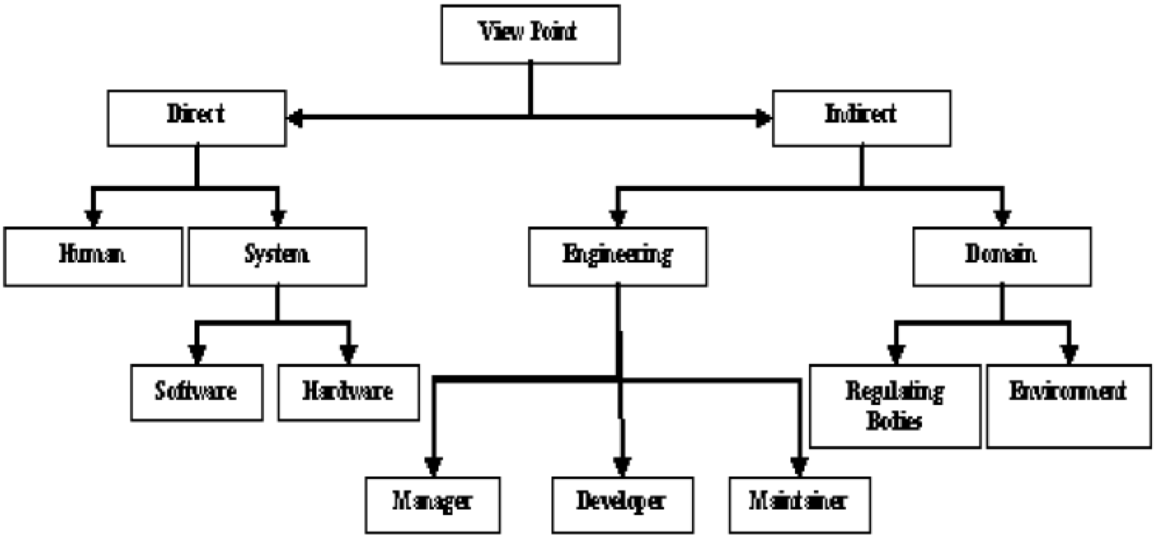


Figure 11: Various stake holders are identified using view point approach.

b. Identify the functionalities of each actor conceptualized in step i. Also determine associated non - functional requirements.

c. Identify the threats associated with each of the functional requirements or data which is used by this functionality using common criteria.

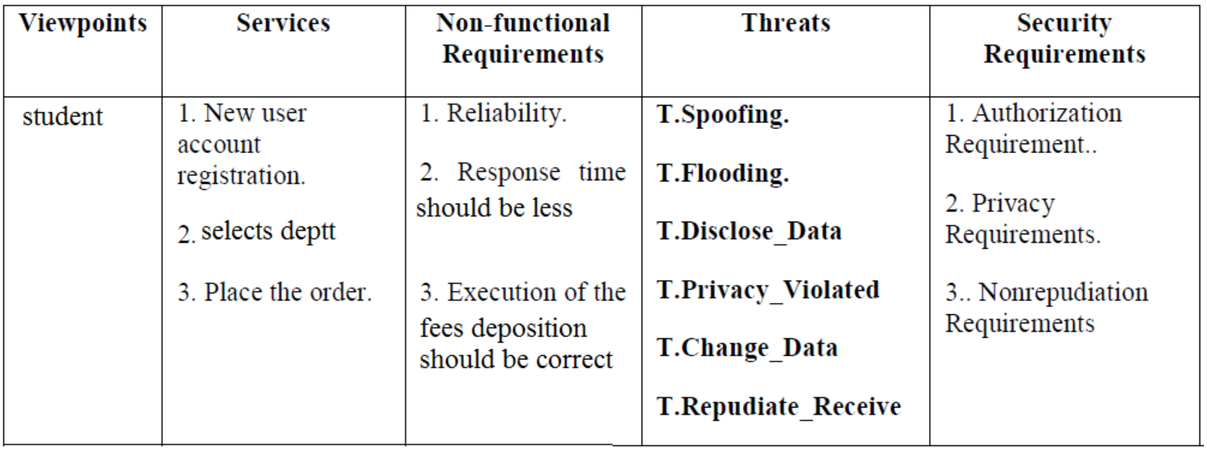
d. Once the threats have been identified it defines security requirements to mitigate these threats.

Analysis and Prioritization of Security Requirement

In this activity analysis of the various security requirements for their completeness, Consistency, Unambiguousness, Feasibility etc is done. Once the security requirements are analyzed the corresponding security requirements are prioritized based on the measure of risk of threat on an asset. For measuring risk there are various techniques such as OCTAVE [42], CORAS [42], CRAMM [43] etc.

Management of Security Requirements

After the security requirements are discovered, analyzed, prioritized management of security requirements is done. Since functional and non – functional requirements tend to change during the course of the project same is the case with security requirements too. They also change and grow up during the entire project. Hence it is very essential that the corresponding security requirements should be managed properly so that in further stages they don't grow up making the system under development a failure.



Viewpoints	Services	Non-functional Requirements	Threats	Security Requirements
student	1. New user account registration. 2. selects deptt 3. Place the order.	1. Reliability. 2. Response time should be less 3. Execution of the fees deposition should be correct	**T.Spoofing.** **T.Flooding.** **T.Disclose_Data** **T.Privacy_Violated** **T.Change_Data** **T.Repudiate_Receive**	1. Authorization Requirement.. 2. Privacy Requirements. 3.. Nonrepudiation Requirements

Table 2: Shows the example of college registration using secure viewpoint

Chapter 3

SECURITY REQUIREMENT ELICITATION PROCESS FOR ERP

After establishing the foundation stone of security engineering, we now present our process for elicitation of security requirements for ERP. Processes defined will be the extension of the earlier methodologies i.e VOSREP and secure tropos into ERP.

Our Security requirements elicitation [17,18,32] process is based on following observation from the above section.

- Implementation of Security mechanisms effectively in ERP to mitigate threats which can be considered as special kind of risk.
- Security requirements are driven from functionalities and data which are accessed by user of the system which may be internal or external to the system.
- Non functional requirements to some extent avoid security threats or cover security requirements.
- Security requirements are related to each other. For ex. - authorization requirements require existence of both identification and authentication requirements.

We will describe two methodologies to elicitate security requirements for ERP

i. Viewpoint oriented security requirement elicitation process
ii. Tropos methodology

We will adapt the viewpoint oriented security requirement elicitation process for ERP system and concentrate on requirement discovery process.

Following the steps of requirement discovery given by VOSREP process, here are the steps for ERP.

3.1 View point oriented security requirement elicitation process for ERP

Here we are extending the technique of VOSREP[32] defined in section 2.4 for ERP

The flow in which the ERP security requirements are found is: -

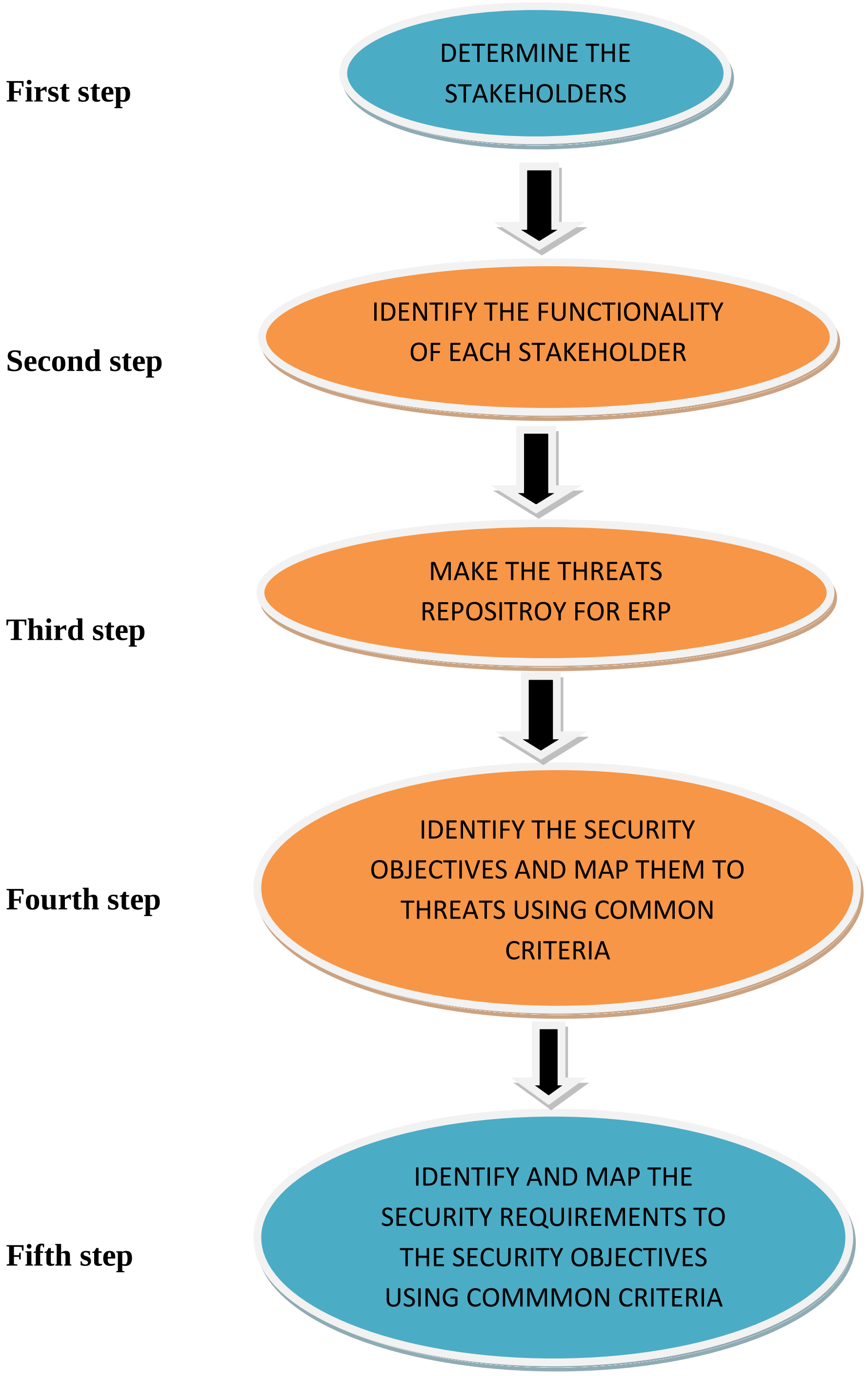

First step
DETERMINE THE STAKEHOLDERS
Second step
IDENTIFY THE FUNCTIONALITY OF EACH STAKEHOLDER
Third step
MAKE THE THREATS REPOSITROY FOR ERP
Fourth step
IDENTIFY THE SECURITY OBJECTIVES AND MAP THEM TO THREATS USING COMMON CRITERIA
Fifth step
IDENTIFY AND MAP THE SECURITY REQUIREMENTS TO THE SECURITY OBJECTIVES USING COMMMON CRITERIA

Figure 12: Process used for elicitating security requirements for ERP

3.1.1 Identify various stakeholders (actors) of ERP system using view point analysis

Actors can be classified as direct and indirect actors[32]. Direct actors are those who directly interact with the system such as human, software system and hardware devices. Indirect actors refer to personals who develop software and people who regulate application domain.

For Example- For ERP to be implemented in college then direct actors can be end users and department people and indirect actors can be the database manager, security administrator, process owners etc.

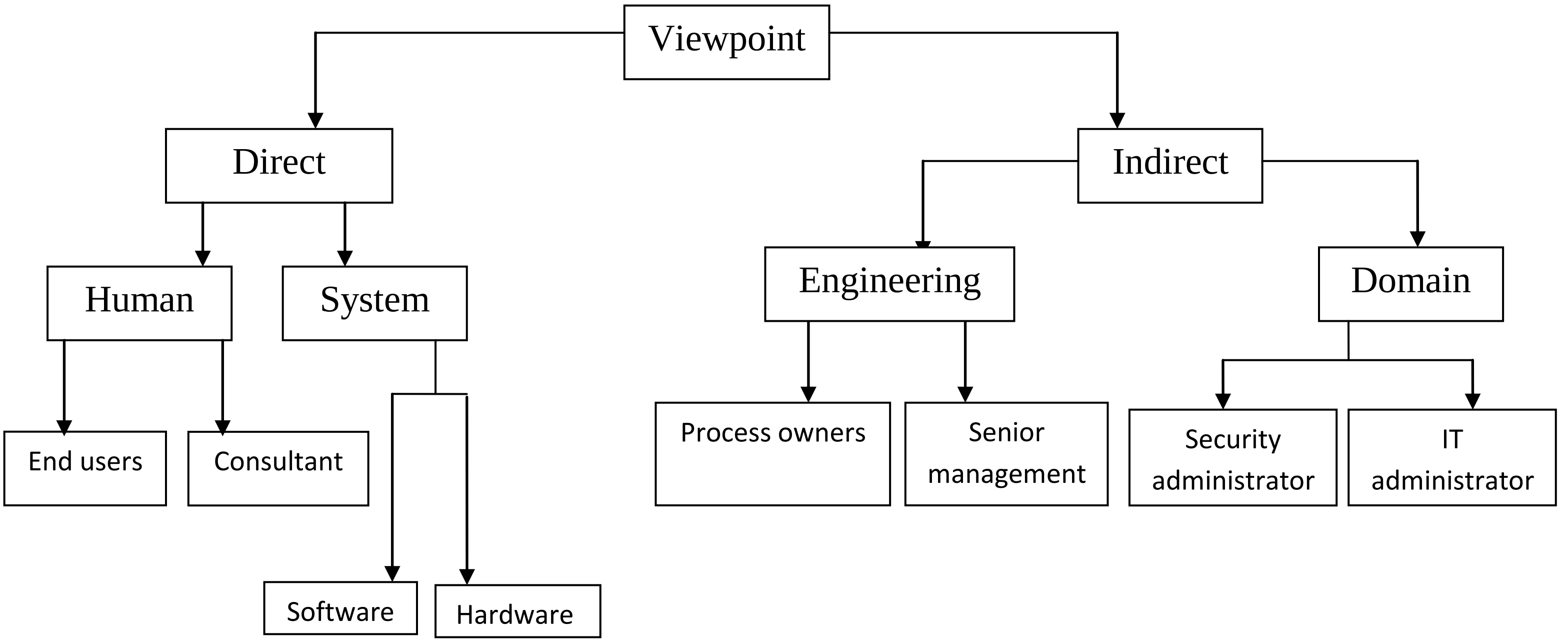


Figure 13: Different types of stake holders in ERP

3.1.2 Identify the functionalities of each actor.

For Example- the functionality of End users i.e. the department persons can be to enter the data, update the records etc. The functionality of process owners is to check whether the processes are understood by the consultants as required and assigning the end users their access rights to the ERP software (i.e. checking the authority provided to the end users)[32].

Actors	Functionality
End Users	1.) Using ERP systems for feeding the data in system 2.) Fetching organization data from the system 3.) Maintains financial accounts 4.) performs the functions on ERP system according the role provided to the End user
Consultants – Functional	1.) Understands the requirement from process owner and implements in organisation in ERP(SAP, BAAN, ORACLE) 2.) Trains the End users for how to use the system.
Consultant – Technical	1.) Build the forms and reports required by the organization/ process owners. 2.) Integrate different modules and checks for its correctness. 3.) Responsible for customizing the ERP for sending Emails through.
Managers - Process owners	1.) Describes the process to the consultants so as to implement ERP in organization. 2.) Define the roles to be assigned to the employee 3.) Checks the process is customized in ERP as required by organization.
Security administrator	1.) Updates the system with all the anti viruses and firewalls 2.) Checks for update of the ERP software and system.
IT administrator	1.) Checks and provides authentication and authorization for all the users of ERP system. 2.) Maintains and updates the record of all the data of ERP in database.
Auditor	1.) Maintains the audits and log details

Table 3: Mapping actors and their functionalities

3.1.3 Identify the threats associated with each of the functional requirements or data which is used by this functionality.

A predefined repository of threats which can affect ERP system is used[11,32]. ERP Actors will be classified as mentioned in view point analysis. Also threats will be classified, based on functionality and the actor kind predefined threats can be retrieved from the repository according to the profile of the actor. Define Security requirements which will mitigate these threats. We will make a repository of threats to identify the existing threats in ERP for each stakeholder we will make a stakeholders profile that helps in the automatic generation of threats from the repository made by us. The profile of the stakeholder will be based on seven fields.

Actor Name – Ex- End users like, professors, administrative department People.
Use Case – Ex- Check Results. Display Books
Type - Ex – Direct, Indirect etc.
Location – Local Or Remote
Private Exchange – Yes or No
Secret Exchange – Yes or No
Association – read, write, ask, answer, retrieve, store, send, display, update etc.

Security requirement elicitation using view point approach identifies threat by mapping common criteria (CC) with use case diagrams method for generation of threat based on stake holders profile as describe above.

Now we describe the category of threats which can be found in ERP system.[11,13]

S.No	Threat Name	Description
1.	Change_Data	If some authorized person changes data intentionally
2.	Data_Theft	Data is stolen and send via mail or pendrive
3.	Scavenging	Acquisition of data from residue
4	Covert_ communication_ channel	Captures electromagnetic radiations from computer screen to hack data
5.	Denial_of_service	Application and network not favourable for use

6.	Sabotage	Destruction of the equipment deliberately
7.	Natural_disaster	Can be earth quakes or other natural calamities
8.	Unauthorized_access	External body accessing data without authorization
9.	Disclose_data	Information disclosed to unauthorized person while storing or processing
10.	Impersonate	Obtaining unauthorized access by impersonating an authorized user.
11.	Insider	An authorized user may gain unauthorized access.
12.	Outsider	An individual who is not an authorized user of the system may gain access to the TOE.
13.	Privacy_voilated	Unauthorized access to privacy data of system users may occur without detection.
14.	Repudiate_Receive	An entity may deny that it has received business or commitment data.
15.	Repudiate_send	An entity may deny that it has send business or commitment data.
16.	Spoofing	An entity may cheat for money
17.	Social_Engineer	Tricking someone into giving you his or her password for a system than to spend the effort to hack in.

Table 4: Threat category and description in ERP

Once the threats are identified and are stored in repository, they are mapped to the functionality of the actors as described in the table below

Actors	Functionality	Threats
End Users	1.) Using ERP systems for feeding the data in system 2.) Fetching organization data from the system 3.) Maintains financial accounts	Change data Data theft Sabotage Disclosure of data Impersonate data Insider Spoofing Data theft

	4.) performs the functions on ERP system according the role provided to the End user	Unauthorized access Insider Covert communication channel scavenging
Consultants – Functional	1.) Understands the requirement from process owner and implements in organisation in ERP(SAP, BAAN, ORACLE) 2.) Trains the End users for how to use the system.	Change data Disclose data Impersonate Privacy violated Spoofing Social engineer Disclose data Change data
Consultant – Technical	1.) Build the forms and reports required by the organization/ process owners. 2.) Integrate different modules and checks for its correctness. 3.) Responsible for customizing the ERP for sending Emails through.	Data theft Change data Sabotage Unauthorized access Disclose data Outsider Repudiate send Social engineer Denial_of_service Unauthorized access Repudiate send n receive Privacy violated Change data Impersonate Repudiate send and receive
Managers - Process owners	1.) Describes the process to the consultants so as to implement ERP in organization. 2. Define the roles to be assigned to the employee 3.) Checks the process is customized in ERP as required by organization.	Disclose data Privacy violated Change data Unauthorized access Social engineer Impersonate Insider Change data

Security administrator	1.) Updates the system with all the anti viruses and firewalls 2.) Checks for update of the ERP software and system.	Outsider Unauthorized access Denial of service Change data
IT administrator	1.) Checks and provides authentication and authorization for all the users of ERP system. 2.) Maintains and updates the record of all the data of ERP in database.	Social engineer Impersonate Privacy violated Repudiate send Privacy violated Social engineer Data theft
Auditors	1.) Maintains the audits and log details	Change data Data theft

Table 5: Mapping of threats with functionality of the stake holders

3.1.4 Determining the security objectives

After identifying the threats in the above section, we define the security requirements to make these threats less severe. The threats identified are mapped to security objectives for ERP as shown in the table – 2 below.

Security objectives[41] are goals and constraints that affect the confidentiality, integrity, and availability of data and application.

Identification of security objectives is the first, best step you can take to help ensure the security of application like ERP. The objectives, once created, can be used to direct all the subsequent security requirement activities that you perform.

Security objectives can be classified as[3,41]:-

- **Identification & Authentication**: Identify an unknown user using various attributes such as username. Authentication is to prove somebody that whom he claims to be, by verifying the security attributes, such as password. It is the most basic and important security objective.

- **Confidentiality:** It protects information from unauthorized disclosure. Confidentiality contains several aspects, or sub-objectives such as: access control, information flow control, encryption, and residual data protection etc. It is important to not confuse access control with authorization [17]. Authorization is to make sure if a subject has the proper permission to perform actions (e.g., read, modify, delete) on an object, and it is often required that the subject is authenticated. While access control helps controls the access/operations on an object based on more general rules, such as system time.

- **Integrity:** Integrity protects information from unauthorized modification instead of disclosure. It is also possible that integrity is compromised by authorized users' mistakes.

- **Availability:** It ensures the accessibility of information and the continuousness of system functionalities.

- **Non-repudiation:** It ensures that the sender cannot deny he sent the information and the receiver cannot deny the receipt of the information by assuring the identity of both the originator and recipient of transmitted information. An example of security mechanisms for it is digital signature.

- **Security Management:** It provides users with certain roles the ability to customize the use of security mechanisms in a security product. The management can be switch on/off or customize a security function, or management security attributes of users or roles. This security objective is not highly related with protection on system or information, hence is quite distinctive with others.

- **Privacy**: Privacy targets on user's identity or actions non-observable to others, even TSF. This security objective is specific because it sometimes conflicts with other security objectives such as accountability. Un observability makes user's action unaccountable.

- **Accountability:** It provides functionalities for generating records for system behaviour or user actions, which can be used for future review.

- **Intrusion Detection and Response:** It addresses the detection instead of prevention of certain intrusion. It also covers the potential response activities such as security alarms in case of detecting an intrusion.
- **Recoverability:** It covers two aspects: data recoverability and system function recoverability. Data recoverability includes data correction after unauthorized modifications. System function recoverability requires that system recovers to a secure state and/or is still able to provide the key functionalities after certain failure happens.

This step shows mapping of various threats identified above with security objectives.

S.No	Threat Name	Security Objective
1.	Change_Data	Access_control Authentication Integrity Recoverability
2.	Data_Theft	Access_control. Authentication. Accountability.
3.	Scavenging	Confidentiality. Accountability Privacy
4	Covert_ communication_ channel	Accountability Confidentiality Authentication Recoverability
5.	Denial_of_service	Authentication Access_control Resources
6.	Sabotage	Access_control Security management Authentication
7.	Natural_disaster	Recoverability Resources
8.	Unauthorized_access	Access_ control Authentication Integrity
9.	Disclose_data	Authentication

		Access_control Authorization
10.	Impersonate	Identification & Authentication Authenticated_Address Integrity
11.	Insider	Access_Control Identification & Authentication Accountability Confidentiality Non-repudiation
12.	Outsider	Access_Control Authentication Non-repudiation
13.	Privacy_voilated	Access_Control Authentication Privacy Security Management
14.	Repudiate_Receive	Access_Control Integrity Security Management (Revoke_Certainity)
15.	Repudiate_send	Access_Control Integrity Security Management
16.	Spoofing	Access_Control Indentification & Authentication
17.	Social_Engineer	Security Management Confidentiality Accountability

Table 6: Mapping threats to security objectives

3.1.5 Mapping security objectives to CC security functional requirements

Security requirements are identified and are mapped to the security objectives. Basically security requirements are classified in 11 classes, [3,41] according to common criteria these are:-

i. **Security audit (FAU)** – Involves recognizing, recording, storing and analyzing information related to security activities. Audit records are produced by these activities, and can be examined to determine their security relevance.

ii. **Communication (FCO)** – Provides two families concerned with the non repudiation by the originator and by the recipient data.

iii. **Cryptographic support (FCS)** – Used when the TOE implements cryptographic functions. These may be used, for example, to support communication, identification and authentication, or data separation.

iv. **User data protection (FDP)** – Specifying requirements related to the protection of user data within the TOE during import, export and storage, in addition to security attributes related to user data.

v. **Identification and authentication (FIA)** – Ensures the unambiguous identification of unauthorized users and the correct association of security attributes with users and subjects.

vi. **Security management (FMT)** – Specifies the management of security attributes data and functions.

vii. **Privacy (FPR)** – Provides the user with protection against discovery and misuse of his or her identity by other users.

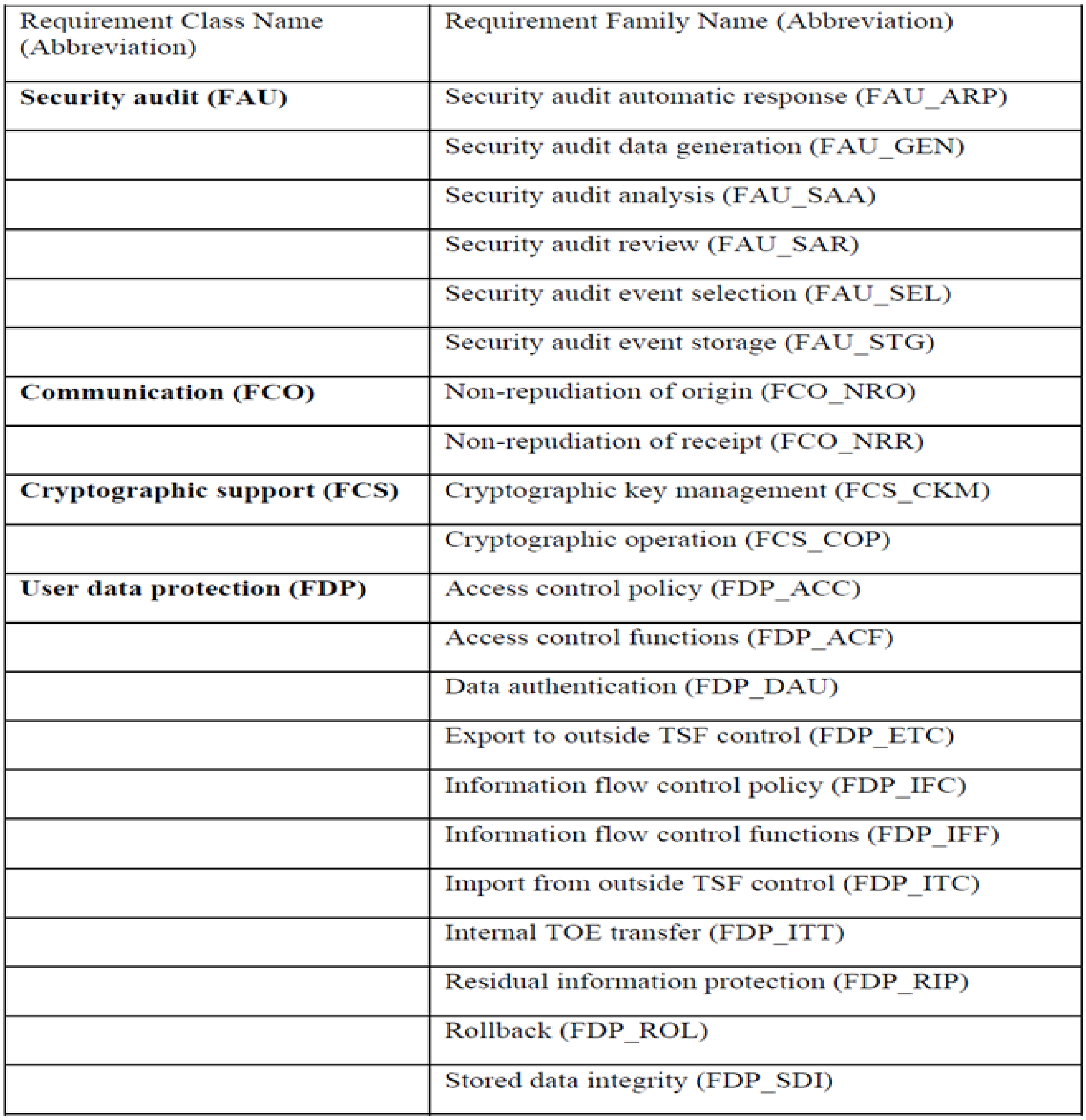
viii. **Protection of the TSF (FPT)** – Focused on the protection of TSF(TOE security functions) data, rather than of other data. The class relates to the integrity and other management of the TSF mechanism and data.

ix. **Resource utilization (FRU)** – supports the availability of required resources, such as processing capability and storage capacity. Include requirements for fault tolerance, priority of service and resource allocation.

x. **TOE access (FTA)** - Specifies the functional requirements in addition to those specified for identification and authentication requirements, for controlling the establishment of user session. The requirement of TOE section governs such things as limiting the number and scope of user sessions, displaying the access history and modification of access parameters.

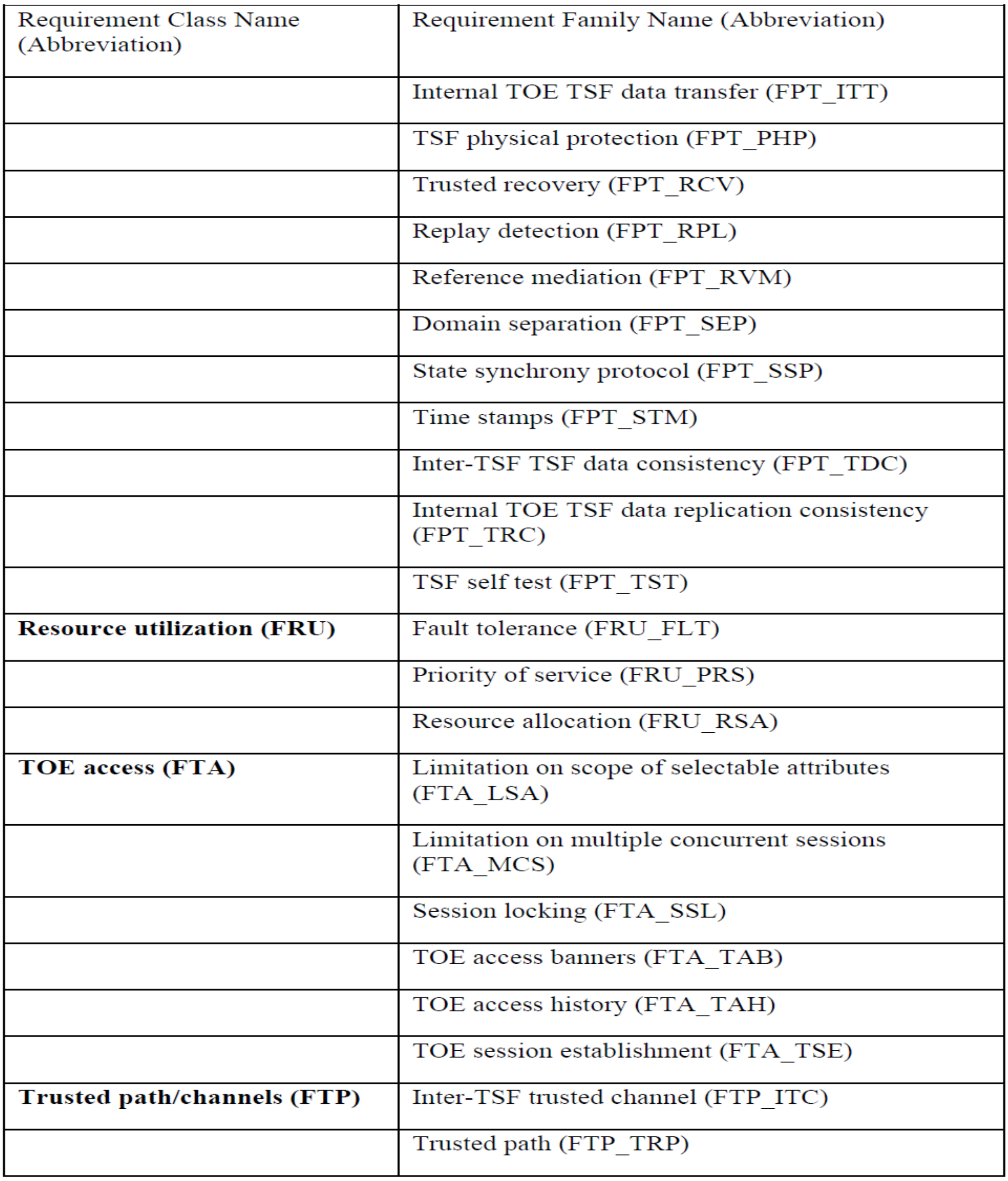
xi. **Trusted path/channels (FTP)** – concerned with trusted communications path between users and the TSF, and between TSFs.

These security classes shown above are further divided into subclasses as shown below[3]:



Requirement Class Name (Abbreviation)	Requirement Family Name (Abbreviation)
Security audit (FAU)	Security audit automatic response (FAU_ARP)
	Security audit data generation (FAU_GEN)
	Security audit analysis (FAU_SAA)
	Security audit review (FAU_SAR)
	Security audit event selection (FAU_SEL)
	Security audit event storage (FAU_STG)
Communication (FCO)	Non-repudiation of origin (FCO_NRO)
	Non-repudiation of receipt (FCO_NRR)
Cryptographic support (FCS)	Cryptographic key management (FCS_CKM)
	Cryptographic operation (FCS_COP)
User data protection (FDP)	Access control policy (FDP_ACC)
	Access control functions (FDP_ACF)
	Data authentication (FDP_DAU)
	Export to outside TSF control (FDP_ETC)
	Information flow control policy (FDP_IFC)
	Information flow control functions (FDP_IFF)
	Import from outside TSF control (FDP_ITC)
	Internal TOE transfer (FDP_ITT)
	Residual information protection (FDP_RIP)
	Rollback (FDP_ROL)
	Stored data integrity (FDP_SDI)

Requirement Class Name (Abbreviation)	Requirement Family Name (Abbreviation)
	Inter-TSF user data confidentiality transfer protection (FDP_UCT)
	Inter-TSF user data integrity transfer protection (FDP_UIT)
Identification and authentication (FIA)	Authentication failures (FIA_AFL)
	User attribute definition (FIA_ATD)
	Specification of secrets (FIA_SOS)
	User authentication (FIA_UAU)
	User identification (FIA_UID)
	User-subject binding (FIA_USB)
Security management (FMT)	Management of functions in TSF (FMT_MOF)
	Management of security attributes (FMT_MSA)
	Management of TSF data (FMT_MTD)
	Revocation (FMT_REV)
	Security attribute expiration (FMT_SAE)
	Security management roles (FMT_SMR)
FPR: Privacy	Anonymity (FPR_ANO)
	Pseudonymity (FPR_PSE)
	Unlinkability (FPR_UNL)
	Unobservability (FPR_UNO)
Protection of the TSF (FPT)	Underlying abstract machine test (FPT_AMT)
	Fail secure (FPT_FLS)
	Availability of exported TSF data (FPT_ITA)
	Confidentiality of exported TSF data (FPT_ITC)
	Integrity of exported TSF data (FPT_ITI)



Requirement Class Name (Abbreviation)	Requirement Family Name (Abbreviation)
	Internal TOE TSF data transfer (FPT_ITT)
	TSF physical protection (FPT_PHP)
	Trusted recovery (FPT_RCV)
	Replay detection (FPT_RPL)
	Reference mediation (FPT_RVM)
	Domain separation (FPT_SEP)
	State synchrony protocol (FPT_SSP)
	Time stamps (FPT_STM)
	Inter-TSF TSF data consistency (FPT_TDC)
	Internal TOE TSF data replication consistency (FPT_TRC)
	TSF self test (FPT_TST)
Resource utilization (FRU)	Fault tolerance (FRU_FLT)
	Priority of service (FRU_PRS)
	Resource allocation (FRU_RSA)
TOE access (FTA)	Limitation on scope of selectable attributes (FTA_LSA)
	Limitation on multiple concurrent sessions (FTA_MCS)
	Session locking (FTA_SSL)
	TOE access banners (FTA_TAB)
	TOE access history (FTA_TAH)
	TOE session establishment (FTA_TSE)
Trusted path/channels (FTP)	Inter-TSF trusted channel (FTP_ITC)
	Trusted path (FTP_TRP)

Table 7: Common criteria classification of security requirements

The mapping of these requirement classes and subclasses in the above table are mapped using common criteria to the security objectives defined in the step iv.

Mapping of security requirements can be done using the common criteria method.[41]

Security objective for ERP	CC functional security requirements
Access control	FDP_ACC (Access control policy) FDP_ACF (Access control function) FPT_SEP (Domain seperation) FMT_SMR (security management roles) FAU_SAR (Security Audit review) FMT_MSA(Managment of sec attribute) FPT_RVM (Reference Mediation) FPR_UNO (unobservability)

Identification & Authentication	FIA_AFL(Authentication failures)
	FIA_ATD(User attribute definition)
	FIA_SOS(Specification of secrets)
	FIA_UAU(User authentication)
	FIA_UID(User identification)
	FIA_USB(User-subject binding)
	FMT_MSA(Management of security attributes)
	FMT_REV(Revocation)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_RVM(Reference mediation)
	FPT_SEP(Domain separation)
	FPT_SSP(State synchrony protocol)
	FPT_TST(TSF self test)
	FTA_LSA(Limitation on scope of selectable attributes)
	FTA_TSE(TOE session establishment)
	FTP_ITC(Inter-TSF trusted channel)
	FTP_TRP(Trusted path)

Associated User Action	FAU_GEN(Security audit data generation) FIA_USB(User-subject binding)

Authenticated_Address	FCO_NRO(Non-repudiation of origin)
	FCO_NRR(Non-repudiation of receipt)
	FDP_ACF(Access control functions)
	FCS_CKM(Cryptographic key management)

Auditing	FAU_GEN(Security audit data generation) FAU_SEL(Security audit event selection) FMT_MOF(Management of functions in TSF) FAU_STG(Security audit event storage) FMT_MTD (Management of TSF data) FAU_SAR(Security audit review)

confidentiality	FCS_CKM(Cryptographic key management)
	FCS_COP(Cryptographic operation)
	FDP_ACC(Access control policy)

	FDP_ACF(Access control functions)
	FDP_ETC(Export to outside TSF control)
	FDP_IFC(Information flow control policy)
	FDP_IFF(Information flow control functions)
	FDP_ITC(Import from outside TSF control)
	FDP_ITT(Internal TOE transfer)
	FDP_RIP(Residual information protection)
	FDP_UCT(Inter-TSF user data confidentiality transfer protection)
	FMT_MSA(Management of security attributes)
	FMT_REV(Revocation)
	FMT_SMR(Security management roles)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_ITC(Confidentiality of exported TSF data)
	FPT_ITT(Internal TOE TSF data transfer)
	FPT_RVM(Reference mediation)
	FPT_SEP(Domain separation)

Integrity	FDP_SDI(Stored data integrity)
	FDP_UIT(Inter-TSF user data integrity transfer protection)
	FDP_ITT(Internal TOE transfer)
	FPT_ITI(Integrity of exported TSF data)

Availability	FMT_MSA(Management of security attributes)
	FMT_SMR(Security management roles)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_ITA(Availability of exported TSF data)
	FPT_RVM(Reference mediation)
	FPT_SEP(Domain separation)
	FPT_TST(TST self test)
	FRU_FLT(Fault tolerance)
	FRU_PRS(Priority of service)
	FRU_RSA(Resource allocation)
	FTA_MCS(Limitation on multiple concurrent sessions)

Non-repudiation	FCO_NRO(Non-repudiation of origin)
	FCO_NRR(Non-repudiation of receipt)
	FCS_CKM(Cryptographic key management)
	FCS_COP(Cryptographic operation)
	FIA_UID(User identification)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_TST(TSF self test)

Security Management	FMT_MOF(Management of functions in TSF) FMT_MSA(Management of security attributes)

	FMT_MTD(Management of TSF data)
	FMT_REV(Revocation)
	FMT_SAE(Security attribute expiration)
	FMT_SMR(Security management roles)
	FPT_AMT(Underlying abstract machine test)
	FPT_SLF(Fail secure)

privacy	FPR_ANO(Anonymity)
	FPR_PSE(pseudonymity)
	FPR_UNL(Unlinkability)
	FPR_UNO(Unobservability)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)

Accountability	FAU_GEN(Security audit data generation)
	FAU_SAR(Security audit review)
	FAU_SEL(Security audit event selection)
	FAU_STG(Security audit event storage)
	FIA_UID(User identification)
	FPR_UNO(Unobservability)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_ITI(Integrity of exported TSF data)
	FPT_RCV(Trusted Recoverability)
	FPT_RVM (Reference mediation)
	FPT_SEP (Domain separation)
	FPT_STM(Time stamps)
	FPT_TST(TSF self test)
	FTA_TAH(TOE access history)

Intrusion detection & response	FAU_ARP(Security audit automatic response)
	FAU_SAA(Security audit analysis)
	FPT_AMT(Underlying abstract machine test)
	FPT_FLS(Fail secure)
	FPT_PHP(TSF physical protection)
	FPT_RPL(Replay detection)
	FPT_RVM(Reference mediation)
	FPT_SEP(Domain separation)
	FPT_TST(TSF self test)
	FTA_SSL(Session locking)
	FTA_TSE(TOE session establishment)

Recoverability	FDP_UIT(Inter-TSF user data integrity transfer protection)
	FPT_FLS(Fail secure)
	FPT_ITI(Integrity of exported TSF data)
	FPT_RCV(Trusted Recoverability)

Table 8: Mapping between CC Security functional req and security objectives for ERP

3.2 Security elicitation in ERP Using secure tropos:-

Requirement elicitation through VOSREP for ERP is discussed in the above section. Here we present various step to find out the security features for ERP using secure tropos methodology.

The process which we will follow for security elicitation in tropos[20] is:

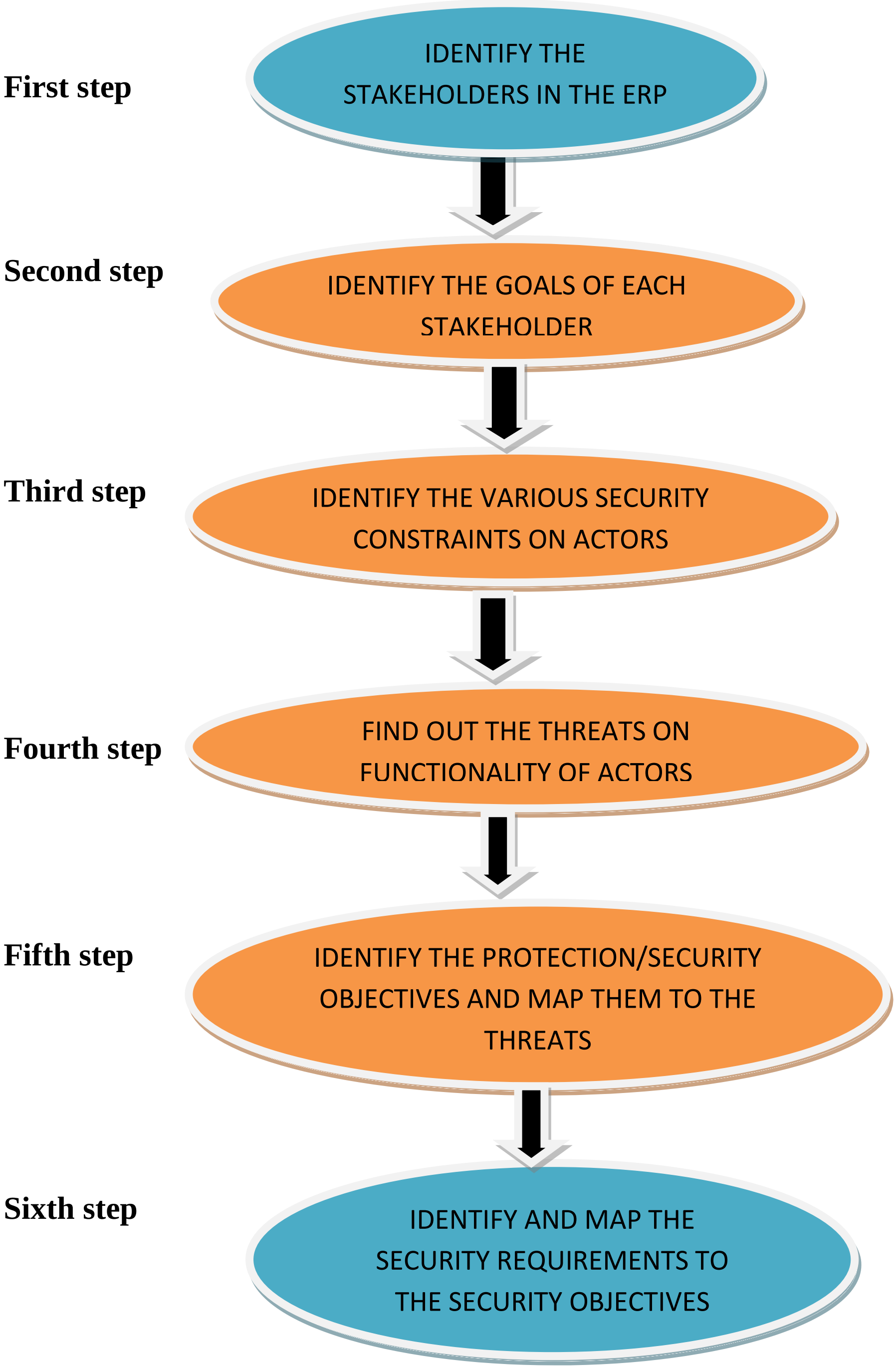

First step
IDENTIFY THE STAKEHOLDERS IN THE ERP
Second step
IDENTIFY THE GOALS OF EACH STAKEHOLDER
Third step
IDENTIFY THE VARIOUS SECURITY CONSTRAINTS ON ACTORS
Fourth step
FIND OUT THE THREATS ON FUNCTIONALITY OF ACTORS
Fifth step
IDENTIFY THE PROTECTION/SECURITY OBJECTIVES AND MAP THEM TO THE THREATS
Sixth step
IDENTIFY AND MAP THE SECURITY REQUIREMENTS TO THE SECURITY OBJECTIVES

Figure 14: Steps for Security Requirement Elicitation in tropos for ERP

3.2.1 Identify the stake holder in ERP system

Various actors and stakeholders are found in the ERP system are

- End Users
- Consultants – Functional
- Managers - Process owners
- Security administrator
- IT administrator
- Auditor

3.2.2 Identify the goals of each stake holders

The goals or the functionality of each of the stake holder is determined. The detailed functionality of each of the stake holder is shown in **Table 3** in the above section. **For example** goal of Consultant is to implement the system as required.

3.2.3 Identify various security constraints on actors

As discussed in section 2.4, security constraints are limitations (restrictions) that do not permit specific actions to be taken or prevent certain objectives from being achieved. Thus, constraints can represent a set of conditions; rules and restrictions imposed on a system, and the system must be operating in such a way that none of them will be violated. **For example** security constraint on actor "consultant" can be "access to authorized consultants only".

3.2.4 Find out the threats on functionality of actors

Potential threats on the system are identified if the security constraint is not applied in the system. Threats are described in the **Table 4** of the above section.

3.2.5 Determine the protection objectives to be applied to remove threats

Threats are then mapped to the protection objectives (security objectives) which are defined in the **Table 5.** Security/protection objectives are goals and constraints that affect the confidentiality, integrity, and availability of data and application. Security objectives can be classified as [3]:-

i. *Identification & Authentication*

ii. *Confidentiality*

iii. *Integrity*

iv. *Availability*

v. *Non-repudiation*

vi. *Security Management*

vii. *Privacy*

viii. *Accountability*

ix. *Intrusion Detection and Response*

x. *Recoverability*

3.2.6 Determine various security requirements for the security objectives

Various security requirements are defined in **Table 7.** These requirements are them mapped to the protection objectives/security objectives.

Basically the security requirements are classified in eleven main classes by CC. These are:-

i. **Security audit (FAU)** – Involves recognizing, recording, storing and analyzing information related to security activities. Audit records are produced by these activities, and can be examined to determine their security relevance.

ii. **Communication (FCO)** – Provides two families concerned with the non repudiation by the originator and by the recipient data.

iii. **Cryptographic support (FCS)** – Used when the TOE implements cryptographic functions. These may be used, for example, to support communication, identification and authentication, or data separation.

iv. **User data protection (FDP)** – Specifying requirements related to the protection of user data within the TOE during import, export and storage, in addition to security attributes related to user data.

v. **Identification and authentication (FIA)** – Ensures the unambiguous identification of unauthorized users and the correct association of security attributes with users and subjects.

vi. **Security management (FMT)** – Specifies the management of security attributes data and functions.

vii. **Privacy (FPR)** – Provides the user with protection against discovery and misuse of his or her identity by other users.

viii. **Protection of the TSF (FPT)** – Focused on the protection of TSF(TOE security functions) data, rather than of other data. The class relates to the integrity and other management of the TSF mechanism and data.

ix. **Resource utilization (FRU)** – supports the availability of required resources, such as processing capability and storage capacity. Include requirements for fault tolerance, priority of service and resource allocation.

x. **TOE access (FTA)** - Specifies the functional requirements in addition to those specified for identification and authentication requirements, for controlling the establishment of user session. The requirement of TOE section governs such things as limiting the number and scope of user sessions, displaying the access history and modification of access parameters.

xi. **Trusted path/channels (FTP)** – concerned with trusted communications path between users and the TSF, and between TSFs.

According to the above classification the mapping of protection objectives(security objectives is done.

Actors	**Goals/functionality**	**Security constraints on goals**	**Threats on goals**	**Protection objective for threats**	**Security Requirements**
Consultants	Design the functionality of organization in ERP according to the process information obtained	Access to authorized consultants only	Change_Data Data_Theft Sabotage Unauthorized_ access Disclose_data	Access control, Information flow, Accountability	FIA FCS FPR FDP FCO
Information owners/ managers	Describes the process to the consultants	Important docs to be encrypted	Privacy violated, Change data	Security management, Access_control, Authentication, Recoverability,	FMT FIA FTA FTP

Security administrators	Checks the security of system	Keep data private and safe	Outsider, Unauthorized access	Access_Control Authentication Non-repudiation Integrity	FIA FPR FTA FCS FCO
IT administrator	Assigns roles to the ERP users	Limited authorization	Privacy violated, Data theft	Access_Control, Authentication, Accountability, Intursion detection & response,	FIA FPR FAU FDP
Auditors	Examines and verifies the organization finances, assets and accounting records	Keep data private	Change data Data theft	Access_Control Authentication Recoverability Accountability	FAU FCS FIA FMT
End users	Test the functionality and enters data in the system	Limited authorization Obtain consent via mail	Unauthorized access Insider Disclosure of data	Access_ control Authentication Integrity Authorization	FIA FTA FMT FRU

Table 9: Mapping of entities for ERP extending secure tropos

Thus the above table shows the elicitation of security requirements for ERP by extending the secure tropos methodology.

Chapter 4

CASE STUDY

4.1 Case study of ERP implementation in college using secure tropos

In this section we will go through various steps described in above section of VOSREP (view point oriented security requirement elicitation process) for an ERP system using a case study of an ERP implementation in a college.

Step 1. Identify various actors/stake holders –

The direct actors for the ERP system for college according to the view point diagram for stakeholders shown is section 3.1 are the End users such as the students(who wants to check updated information regarding any issue) and department heads(who can edit and update the information) and Consultants who moulds the system according to the user requirements and have the authorities to configure the functionalities in the system.

Other Indirect and domain actors in the ERP system for college can be process owners(managers) , Security Administrators, IT department, Auditors etc.

We will describe the view point method for elicitating security requirements for ERP implemented in college by using the actor as direct actor only so as to clarify the idea of elicitation of security requirement in ERP.

Step 2 . Identify functionalities of the actors/stakeholders.

Functionality of different stake holders are:-

Functionality of students

- log in(only authorized students)
- Check the assignments
- Check for the marks details
- Checks the attendance
- Checks for the fees details and can pay the fees online
- Checks for library books name and can issue and reissue the book.

Functionality of department heads/professors

- Updates the system or software
- Mark the attendance
- Upload the marks and other data related to fees
- Edit the records
- Each department people can upload and edit their data.

Functionality of consultants

- Gathers the requirements from the end-users i.e. students and other department heads
- Give training to the end users
- Configure the system ERP
- Understands the process from process owners
- Set various roles for the users and other actors

Step- 3 Identify the threats which are associated with each of the functional requirements of the actors/stakeholders.

Stakeholders profile has seven fields consisting of name, functionality, type (as according to view point), Physical location (local or Remote), use case association(read, write, store, update etc.) and weather or not the use case involves exchanging private
and secret information.

Example student :

Stakeholder	Student
Functionality	Checks the assignments and marks etc
Type	Direct
Location	Local/remote
Private exchange	True
Secret exchange	False
Association	Read

Table 10: Case study for Student profile

Association = read(for students)	Association = write(for consultants and department heads)
Impersonate	change_data
If private exchange = true	If private exchange = true
privacy_voilated	privacy_voilated
If location =remote	If location = local
Outsider	insider

Table 11: Threats evaluation for stake holders for college system

Viewpoints	Services	Non-functional requirements	Threats	Security requirements
Students	1 Log in 1 Search information regarding library, assignments, fees payment 3. issue the books 4. download assignments 5. check attendance	1. correctness, reliable 2. Fast response time. 3. execution is correct, correctness.	Impersonate Denial of service Sabotage Disclose_data spoofing flooding Repudiate_receive unauthorized_access	1. Identification & authorization req. 2. Privacy req. 3. Non-repudiation req 4. Access_control_policies 5. Access_control_functions 6. Data_authentication 7. Stored_data_integrity
Department heads/ professors	1. Updates the system or software 2. Mark the attendance 3. Upload the marks and other data related to fees 4. Edit the records 5. Each department people can	1. Scalable 2. Robustness 3. Correctness 4. Minimize response time 5. Efficient 6. Scalable 7. Modifiable 8. Accuracy 9. Usablility	1. Chang_data 2. Data_theft 3. Disclose_data 4. Privacy_voilated 5. insider 6. Denial of service 7. Sabotage 8. repudiate	1. Non-repudiation 2. Privacy req. 3. Integrity req. 4. Authorization req 5. Authentication and identification req 6. Management of security

	upload and edit their data.			attributes 7. Security management roles 8. Fault tolerance 9. Priority of service 10. Resource allocation

Table 12: Example of ERP implemented in college by considering direct actors only.

4.2 Case study of ERP implementation in college using secure tropos

In this section we will go through the various steps of secure tropos for finding out the security features of ERP implemented in college.

Step 1. Identify various actors/stake holders –

Various actors and stakeholders are found in the ERP system for college.

Consider following actors for ERP in college are –

- Students
- Department heads
- Consultants
- IT administrator
- Security Administrators

Step 2. Goals of these actors are identified

In this step goals of the actors are found and described. Goals are the functionalities provided by the stakeholders in the system.

Example: -

Student Goals – login to their user ID, can access library account for re -issuing books,

Department head Goals – Access student details, library details, teacher details etc.

Consultant Goals – To implement the system effectively and as per told by the users.

IT administrator – To maintain the database.

Security administrator – To prevent the system from the viruses and the attackers.

Step 3. Security Constraint

Security constraint is evaluated on each of the actors of the system.

Example :-

Security constraint of "student" as actor is "access to authorized students only". i.e. no other student outside the college can access the system.

Step 4. Find out threats on functionality of actors

Threats on actors functionalities are chosen from **Table 4.**

Example :-

Spoofing, viruses, outsiders etc

Step 5. Determine the protection objectives to be applied to remove threats

Example: -

Identification & Authentication, Confidentiality

Step 6. Determine various security requirements for the security objectives

Example:-

Security Audit, Communication

Actors	**Goals/ functionality**	**Security constraints on goals**	**Threats on goals**	**Protection objective for threats**	**Security Requirements**
Consultants	Design the functionality of organization in ERP according to the process information obtained	Access to authorized consultants only	Change_Data Data_Theft Sabotage Unauthorized_access Disclose_data	Access control, Information flow, Accountability	FIA FCS FPR FDP FCO
Department Head	Describes the process to the consultants Checks the functionality of the	Important docs to be encrypted	Privacy violated, Change data	Security management, Access_control, Authentication,	FMT FIA FTA FTP

	students and keeps check on it.			Recoverability,	
Security administrators	Checks the security of system	Keep data private and safe	Outsider, Unauthorized access	Access_Control Authentication Non-repudiation Integrity	FIA FPR FTA FCS FCO
IT administrator	Assigns roles to the ERP users	Limited authorization	Privacy violated, Data theft	Access_Control, Authentication, Accountability, Intursion detection & response.	FIA FPR FAU FDP
Student	Check there record and status of library, class attendance, assignments etc	Keep data private	Change data Data theft	Access_Control Authentication Recoverability Accountability	FAU FCS FIA FMT
End users	Test the functionality and enters data in the system	Limited authorization Obtain consent via mail	Unauthorized access Insider Disclosure of data	Access_ control Authentication Integrity Authorization	FIA FTA FMT FRU

Table 13: Mapping of college actors with their functionalities & security constraints

Chapter 5

IMPLEMENTATION

5.1 Tools Used

We used the following Microsoft language and database for our project

Microsoft visual studio

- Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop console and graphical user interface applications along with Windows Forms applications, web sites, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework and Microsoft Silverlight.
- Visual Studio provides tools and other utilities that help to develop, execute, debug, and document programs written in the Microsoft visual studio programming language. It can be downloaded from Microsoft site.

SQL Server

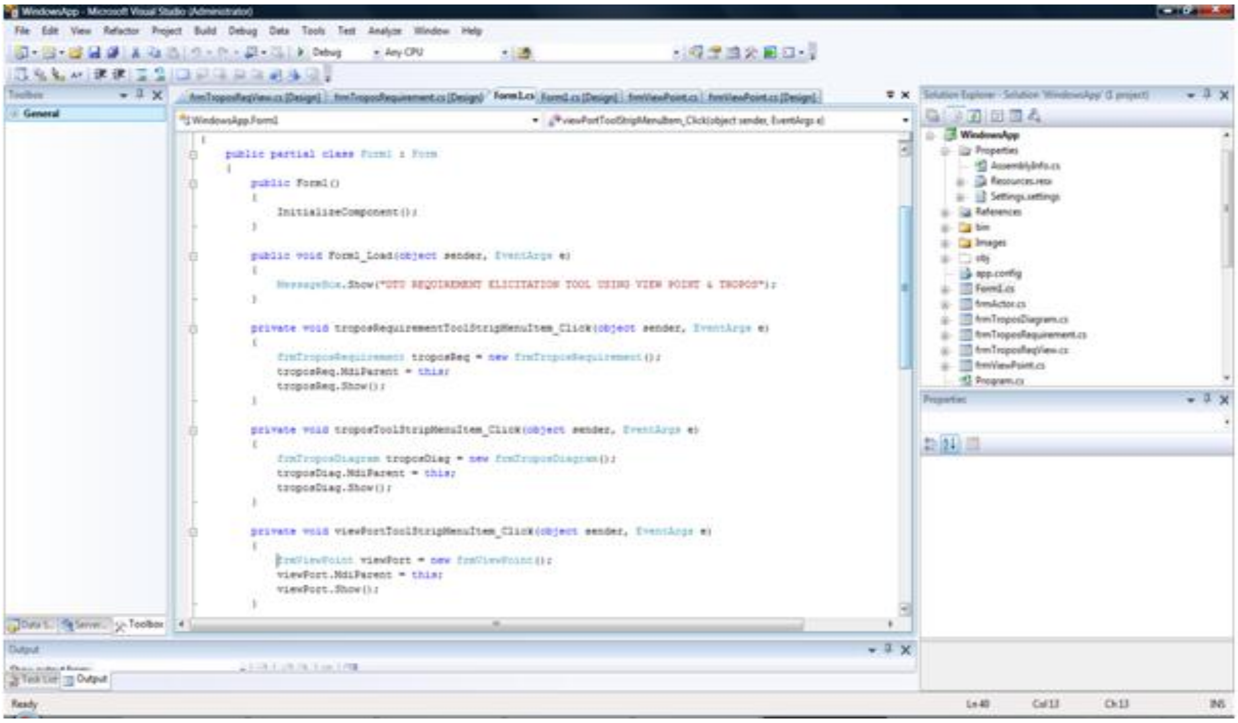
- Microsoft SQL Server is a full-featured relational database management system (RDBMS) that offers a variety of administrative tools to ease the burdens of database development, maintenance and administration.
- SQL has been used to make relations for our development tool. It offers a variety of functionalities to ease the burdens of database development, maintenance and administration.
- Enterprise Manager is the main administrative console for SQL Server installations. It provides you with a graphical "birds-eye" view of all of the SQL Server installations in network.

5.2 Files and relations used

The code consists of following windows:

- Main Window
- Viewpoint window
- Tropos Requirement window

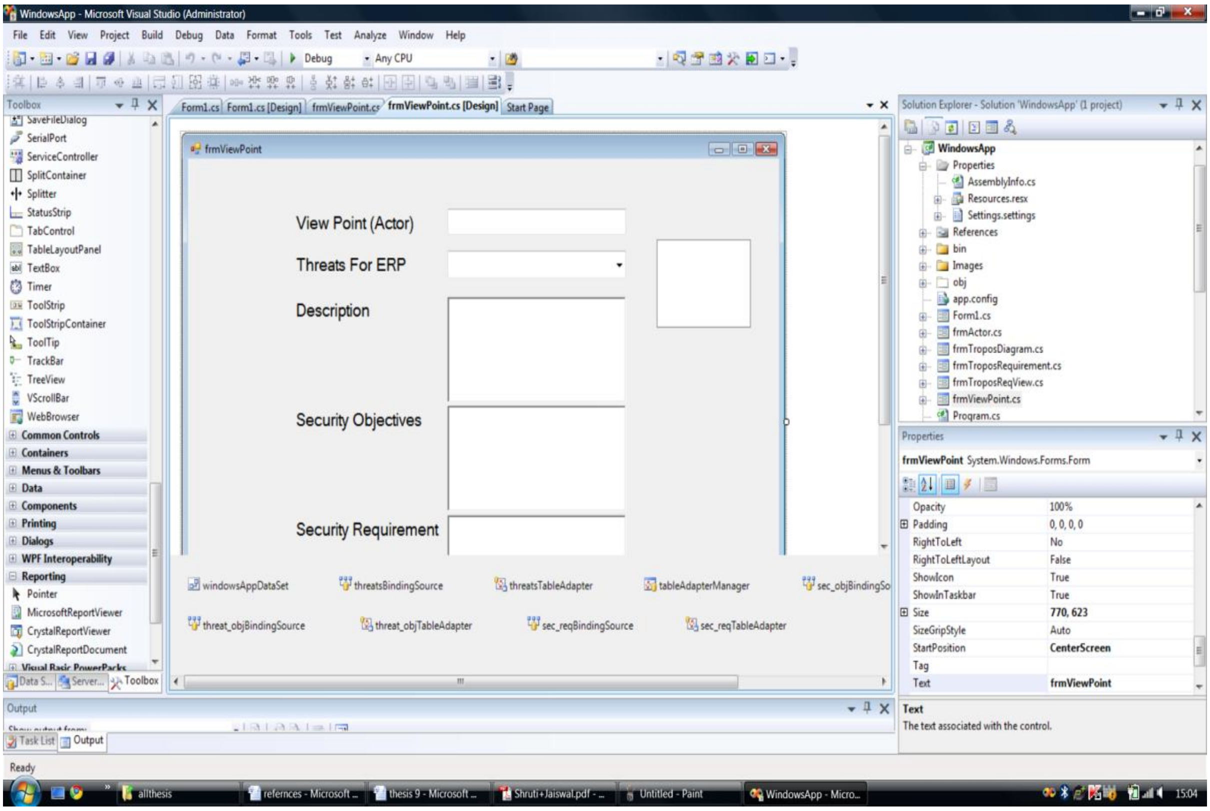
Main Window– It is the class that provides the main window from where the user can choose to open the desired project from the list of project given. When the user will select project of his choice then the options will be called to start the project.



```
public partial class Form1 : Form
{
    public Form1()
    {
        InitializeComponent();
    }

    public void Form1_Load(object sender, EventArgs e)
    {
        MessageBox.Show("STS REQUIREMENT ELICITATION TOOL USING VIEW POINT & TROPOS");
    }

    private void troposRequirementToolStripMenuItem_Click(object sender, EventArgs e)
    {
        frmTroposRequirement troposReq = new frmTropisRequirement();
        troposReq.MdiParent = this;
        troposReq.Show();
    }

    private void troposToolStripMenuItem_Click(object sender, EventArgs e)
    {
        frmTroposDiagram troposDiag = new frmTroposDiagram();
        troposDiag.MdiParent = this;
        troposDiag.Show();
    }

    private void viewPortToolStripMenuItem_Click(object sender, EventArgs e)
    {
        frmViewPoint viewPort = new frmViewPoint();
        viewPort.MdiParent = this;
        viewPort.Show();
    }
```

Figure 15: Showing the Main window code

Viewpoint Window – View point window helps in displaying the security requirements using viewpoint. Table viewpoint is called when this window opens and displays the five fields as described earlier.

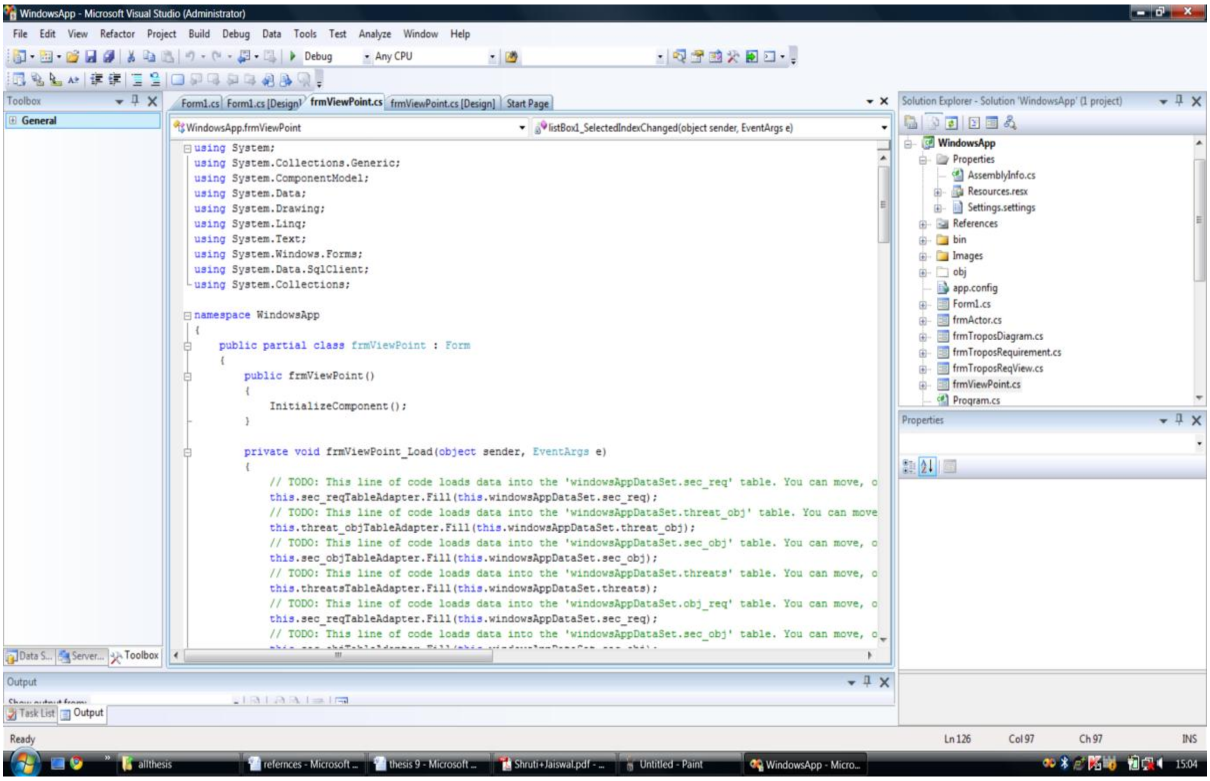


frmViewPoint System.Windows.Forms.Form

Opacity	100%
Padding	0, 0, 0, 0
RightToLeft	No
RightToLeftLayout	False
ShowIcon	True
ShowInTaskbar	True
Size	770, 623
SizeGripStyle	Auto
StartPosition	CenterScreen
Tag	
Text	frmViewPoint

Text
The text associated with the control.

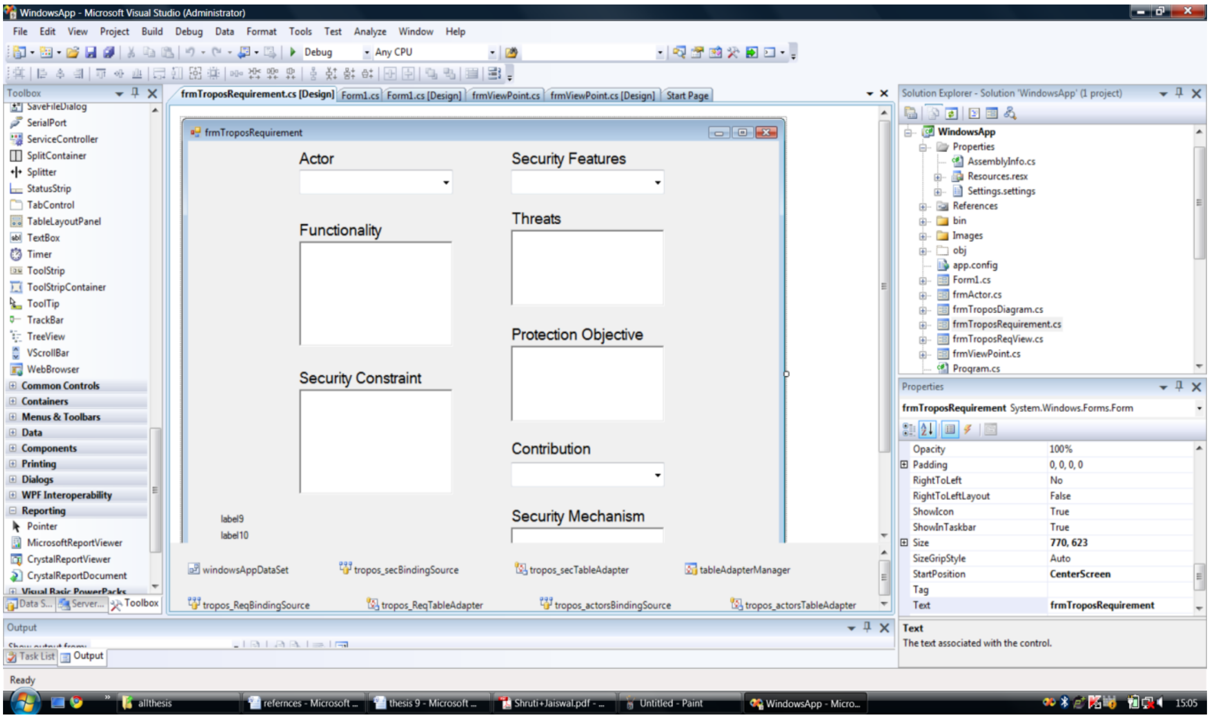
Figure 16: Showing the viewpoint window design



```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Data.SqlClient;
using System.Collections;

namespace WindowsApp
{
    public partial class frmViewPoint : Form
    {
        public frmViewPoint()
        {
            InitializeComponent();
        }

        private void frmViewPoint_Load(object sender, EventArgs e)
        {
            // TODO: This line of code loads data into the 'windowsAppDataSet.sec_req' table. You can move, o
            this.sec_reqTableAdapter.Fill(this.windowsAppDataSet.sec_req);
            // TODO: This line of code loads data into the 'windowsAppDataSet.threat_obj' table. You can move
            this.threat_objTableAdapter.Fill(this.windowsAppDataSet.threat_obj);
            // TODO: This line of code loads data into the 'windowsAppDataSet.sec_obj' table. You can move, o
            this.sec_objTableAdapter.Fill(this.windowsAppDataSet.sec_obj);
            // TODO: This line of code loads data into the 'windowsAppDataSet.threats' table. You can move, o
            this.threatsTableAdapter.Fill(this.windowsAppDataSet.threats);
            // TODO: This line of code loads data into the 'windowsAppDataSet.obj_req' table. You can move, o
            this.sec_reqTableAdapter.Fill(this.windowsAppDataSet.sec_req);
            // TODO: This line of code loads data into the 'windowsAppDataSet.sec_obj' table. You can move, o
```

Figure 17: Showing the viewpoint window code

Tropos requirement Window – Tropos requirement window helps in displaying the security requirements using viewpoint. Table tropos requirement is called when this window opens and displays the seven fields as described earlier.

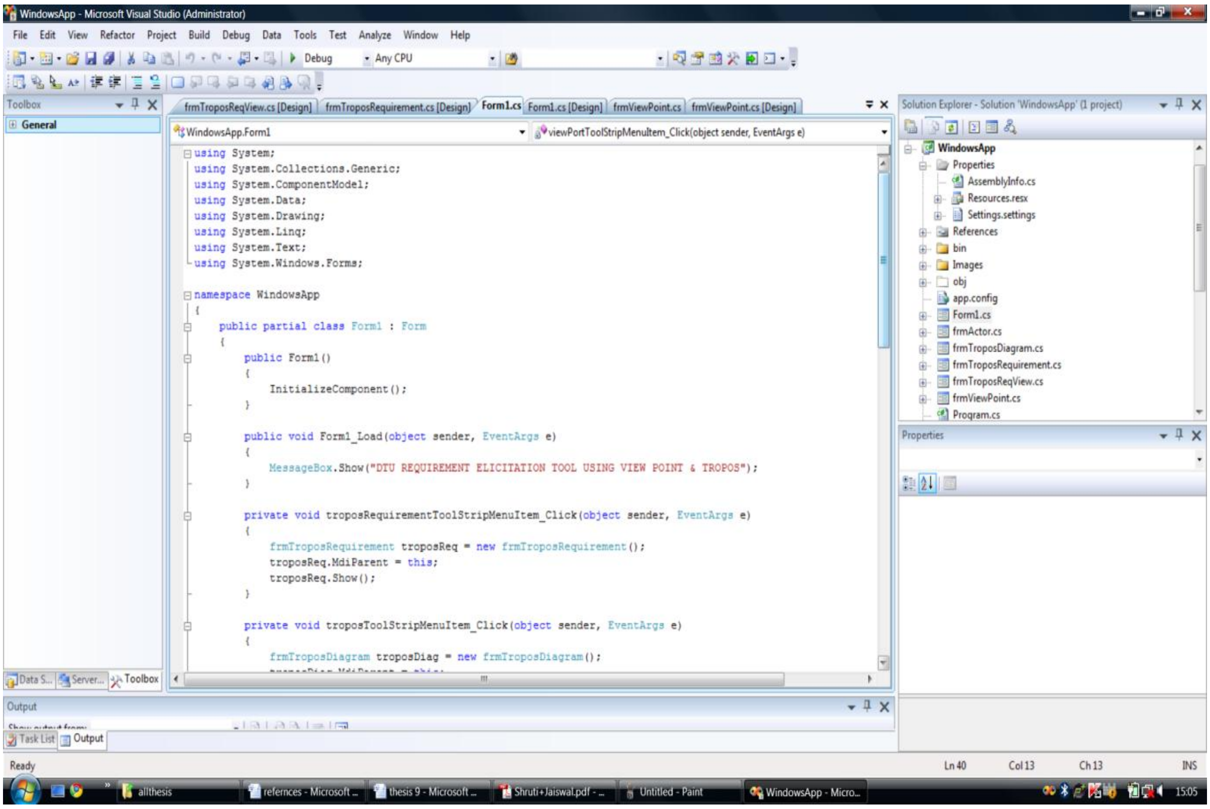


frmTroposRequirement System.Windows.Forms.Form

Opacity	100%
Padding	0, 0, 0, 0
RightToLeft	No
RightToLeftLayout	False
ShowIcon	True
ShowInTaskbar	True
Size	770, 623
SizeGripStyle	Auto
StartPosition	CenterScreen
Tag	
Text	frmTroposRequirement

Text
The text associated with the control.

Figure 18: Showing the tropos requirement window design



```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace WindowsApp
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }

        public void Form1_Load(object sender, EventArgs e)
        {
            MessageBox.Show("DTU REQUIREMENT ELICITATION TOOL USING VIEW POINT & TROPOS");
        }

        private void troposRequirementToolStripMenuItem_Click(object sender, EventArgs e)
        {
            frmTroposRequirement troposReq = new frmTroposRequirement();
            troposReq.MdiParent = this;
            troposReq.Show();
        }

        private void troposToolStripMenuItem_Click(object sender, EventArgs e)
        {
            frmTroposDiagram troposDiag = new frmTroposDiagram();
```

Figure 19: Showing the tropos requirement window project code

5.3 Running the code

First of all you need to run SQL Management studio and make a login. After login a database is created of the same name with which the project is saved. Once it is done all sql tables are embedded in it.

Then go to the Microsoft visual studio and open the project saved. It will pick the database tables from SQL server. Then debug the project and the project will run.

5.4 Snapshots

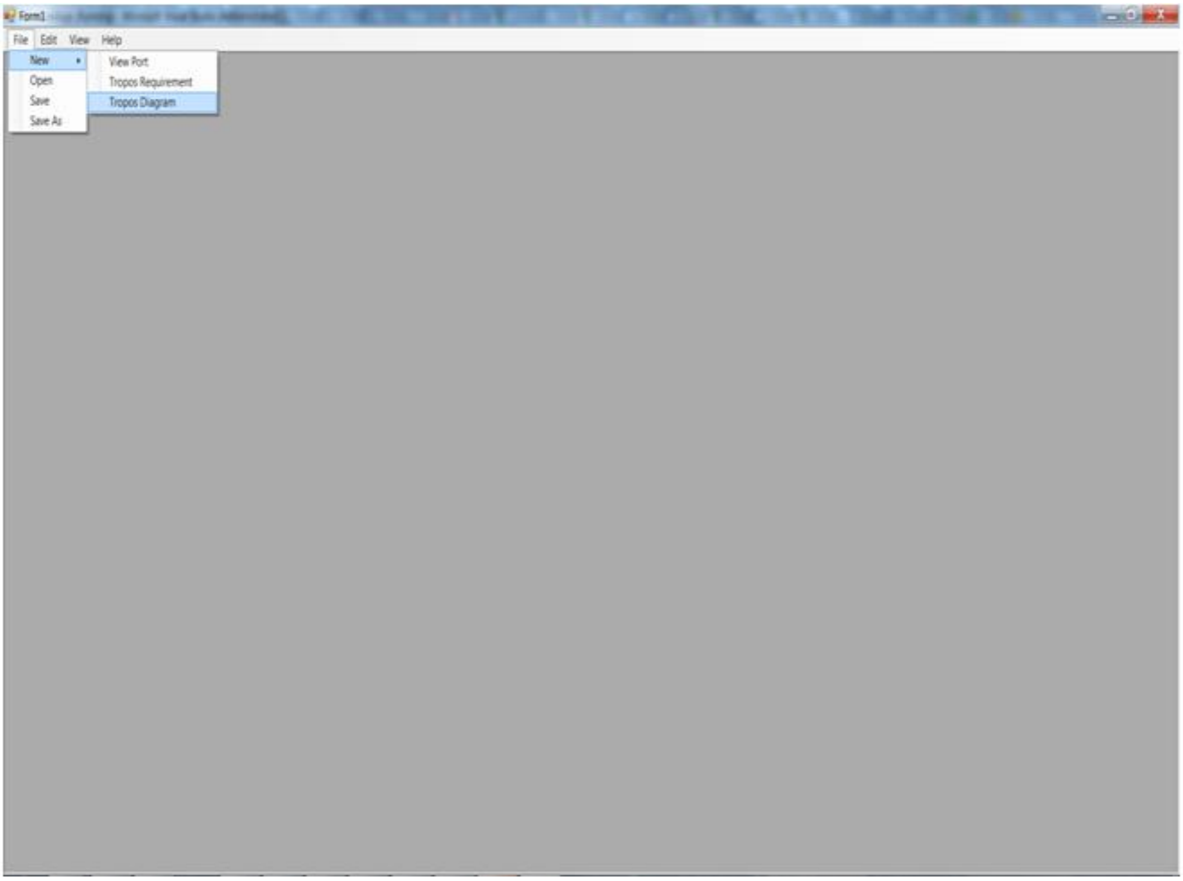
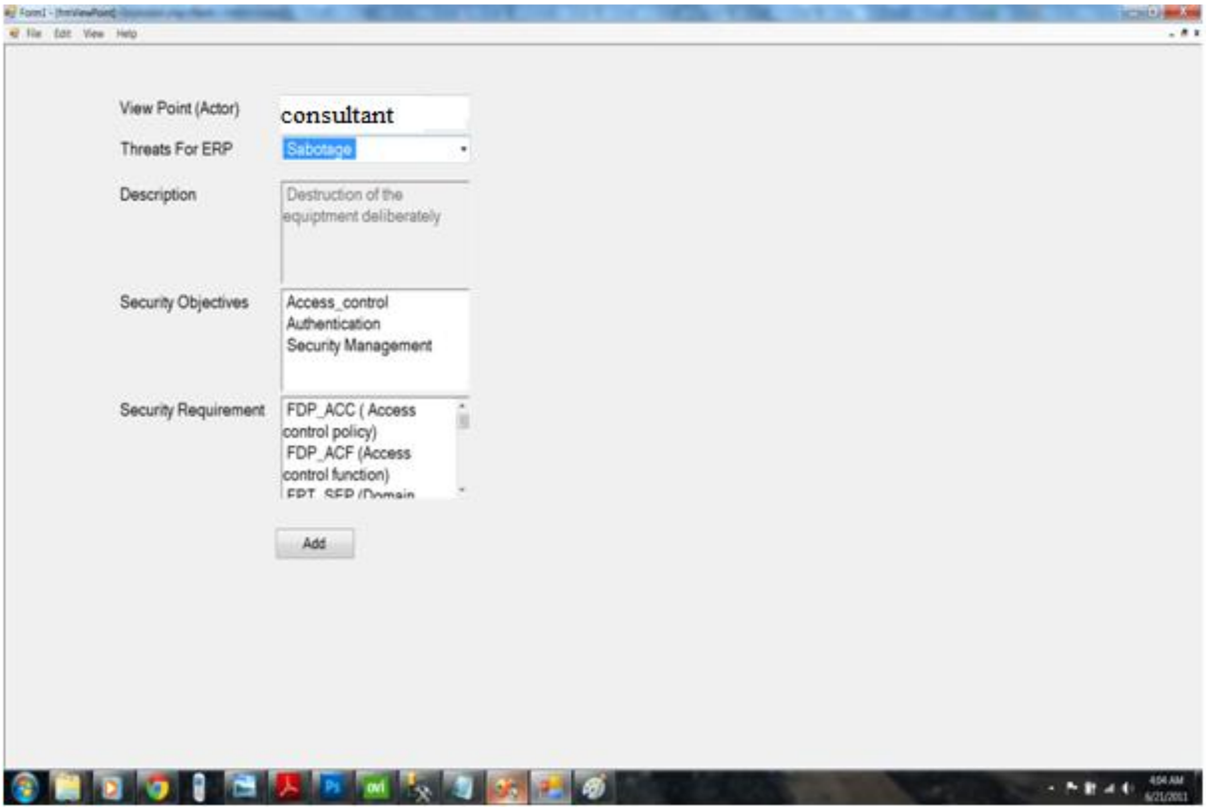


Figure 20: Displaying the main page.



View Point (Actor): consultant

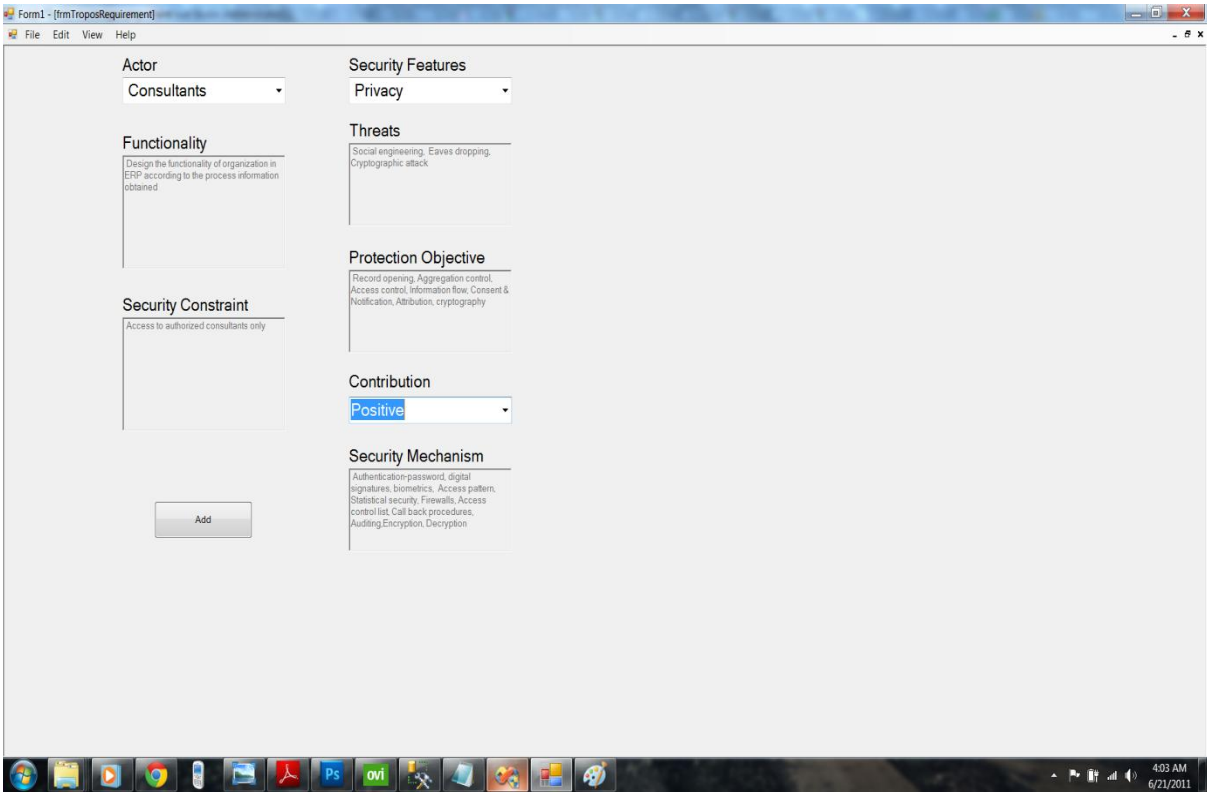
Threats For ERP: Sabotage

Description: Destruction of the equiptment deliberately

Security Objectives: Access_control
Authentication
Security Management

Security Requirement: FDP_ACC (Access control policy)
FDP_ACF (Access control function)
FPT_SEP (Domain

Figure 21: security requirement Using viewpoint



Actor: Consultants

Functionality: Design the functionality of organization in ERP according to the process information obtained

Security Constraint: Access to authorized consultants only

Security Features: Privacy

Threats: Social engineering, Eaves dropping, Cryptographic attack

Protection Objective: Record opening, Aggregation control, Access control, Information flow, Consent & Notification, Attribution, cryptography

Contribution: Positive

Security Mechanism: Authentication-password, digital signatures, biometrics, Access pattern, Statistical security, Firewalls, Access control list, Call back procedures, Auditing,Encryption, Decryption

Figure 22: Security requirements using tropos

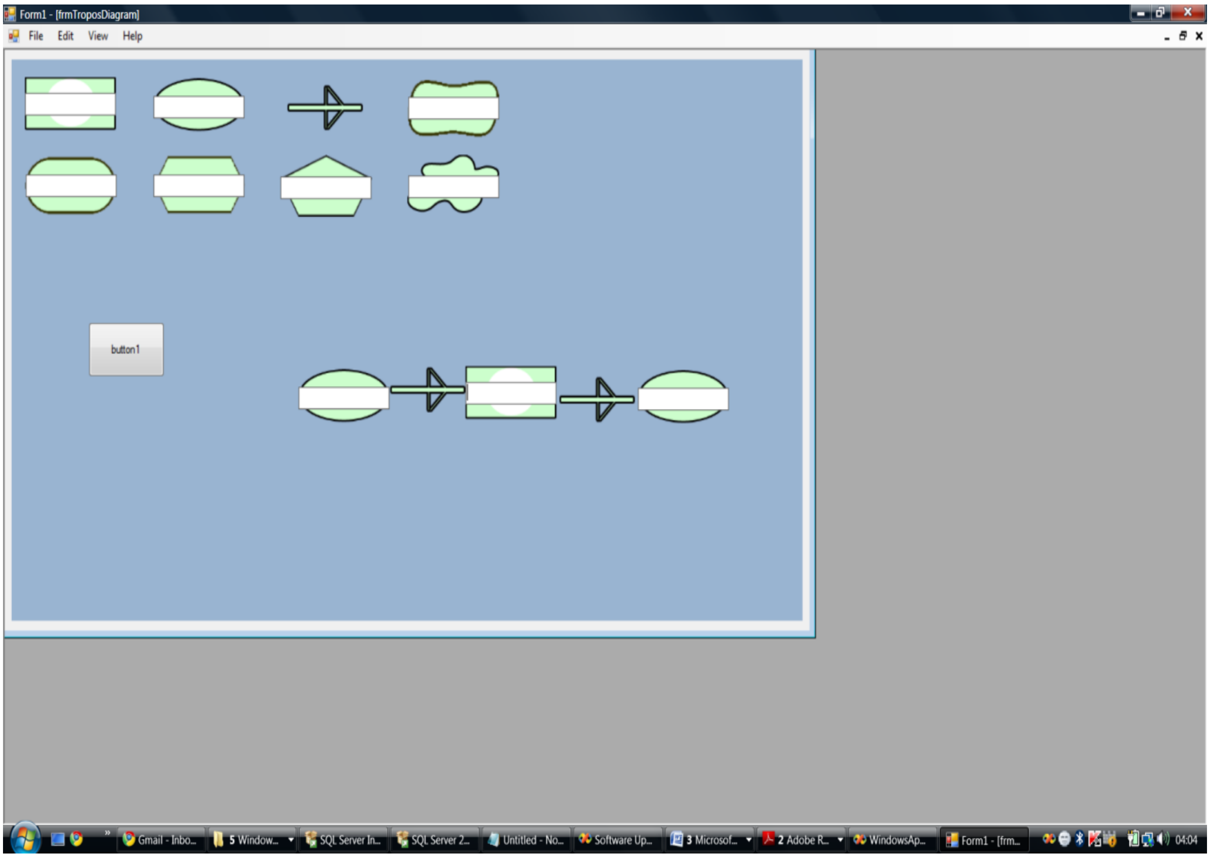


Figure 23: Security diagram using tropos

Chapter 6

CONCLUSION

Security Requirement elicitation plays a crucial role in determining the security features, threats and requirements of the system during the early phases of the SDLC in order to make the system error free and less vulnerable.

In our thesis we have described how security can be elicitated in the ERP organization using the security elicitation process of view point oriented approach and tropos approach. Main focus on the thesis is kept on ERP security requirement elicitation using view point and tropos methodology.

Viewpoint approach is different from the already existing approaches like Common criteria and misuse cases, since view point uses both functional and non-functional requirements to find out the security requirements.

Apart for security elicitation, it even analyze, prioritize and manage the security requirements. No other methodology involves all these steps in a single process thus making the view point oriented methodology unique. It is less complex as compared to the tropos methodology.

Tropos for security elicitation is a new approach developed in 2009, it uses the concept of security constraints, security features, protection objectives, security mechanism, threat. Thought this methodology grills the security requirements in depth as applied for ERP, but it is quite complex because of the diagrams and many notations included.

Chapter 7

REFERENCES

[1] **Alexander IF,** "*Modelling the interplay of conflicting goals with use and misuse cases"* Proceedings of the 8th international workshop on requirements engineering: foundation for software quality Essen, Germany, 2002.

[2] **Alexander IF**, *"Misuse cases, use cases with hostile intent"*. IEEE Software, 2003

[3] Common criteria for information technology security evaluation. Technical report CCIMB 99–031, CC Implementation Board, 1999.

[4] **John Mc Dermott, Chris Fox,** *"Using abuse case models for security requirements analysis."* Department of Computer Science, James Madison University, 1999.

[5] European Computer Manufacturers Association International, ECMA protection profile: ECOFC public business class. Technical report, TR/78, Geneva- Switzerland, 1999.

[6] **Robert J Ellison,** *"Attack Trees"* Software Engineering Institute, Carnegie Mellon University, 2005.

[7] **Donald G. Firesmith,** *"Engineering Security Requirements"*, Journal of object technology,2003, Vol2, no.1, pages 53-68.

[8] (www.techopedia.com/definition/24821/computer-security-compusec)

[9] **M Hertenberger, Prof. S.H. von solms**, " *A case for information ownership in ERP Systems"*, Kluwer Publishing, 2004

[10] http://www.mariosalexandrou.com/definition/erp.asp

[11] **Musaji** *"ERP system implementation overview"/*2002, pages 1-16

[12] **Manfred Paul Hertenberger,** *"A REFERENCE FRAMEWORK FOR SECURITY IN ENTERPRISE RESOURCE PLANNING (ERP) SYSTEMS"* 2005

[13] http://www.seradex.com/FAQS/ERP_Technology_FAQ.php#h

[14] **van de Riet, R.; Janssen, W.;** "*Security moving from database systems to ERP systems"* de Gruijter, P.; Database and Expert Systems Applications, 1998. Proceedings, Ninth International Workshop on Digital Object Identifier: 10.1109, 1998

[15] **S H von solms and M. P. Hertenberger,**springer,2005 *"ERPSEC - A Reference Framework to Enhance Security in ERP Systems"*

[16] **Juntao Gao1, Man Yuan1, Gan Huang1, Zhiyao Wang2,** *"ERP Software Requirement Elicitation with Reference Models"* IEEE , june 2010, 1School of Computer and Information Technology, Daqing Petroleum Institute, China

[17] **Donald G. Firesmith,** *"Engineering Security Requirements",* Journal of object technology, 2003, vol 2, no.1, pages 53-68.

[18**] Donald G. Firesmith,** *"Security Use cases",* Journal of object technology, 2003, vol 2, no.3, pages 53-64.

[19] **Gupta D. and Prakash N**., *"Engineering Methods from their Requirement specification",* Requirements Engineering Journal 2006, 3, pages 133 – 160.

[20**] P Bresciani, Giorgini, Giunchiglia, Mylopoulos, and A. Perini.** *"Tropos: An Agent-Oriented Software Development Methodology"* Autonomous Agents and Multi-Agent Systems, 8(3):203_236, 2004.

[21]**Haralambos Mouratidis1, Paolo Giorgini2, Gordon Manson1, Ian *Philp3*** *"A Natural Extension of Tropos Methodology for Modelling Security"* , IEEE, 2010

[22]**M. Morandini, D. C. Nguyen, A. Perini, A. Siena, and A. Susi.** "*Tool supported Development with Tropos: The Conference Management System Case Study",* In Proceeding of 8th International Workshop on Agent Oriented Software Engineering, 2007.

[23] **Luning Liu; Yuqiang Feng; Qing Hu; Xiaojian Huang;** *"Understanding Organizational Level ERP Assimilation: A Multi-Case Study"***,** System Sciences (HICSS), 2010 43rd Hawaii International Conference on Digital Object Identifier: 10.1109/HICSS.2010.419 , Publication Year: 2010 , Page(s): 1 – 10

[24] **Sengupta, A.R.** *"Enterprise information system with ERP — Pitfalls and way to overcome: A case study",*Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on,Digital Object Identifier: 10.1109/ICIME.2010.5477623 ,Publication Year: 2010 , Page(s): 35 – 37

[25] **Yan Jingdong; Shi Yinping; Lv Liping;** *"Study on Risks and Precautions of Enterprises",* Management and Service Science (MASS), 2010 International Conference on Digital Object Identifier: 10.1109/ICMSS.2010.5576902, Publication Year: 2010 ,Page(s):1,4

[26] **Zhensen Zhang; Ping Han;** *"Systems thinking of the both sides in ERP project implementation"* Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Volume: 1 Digital Object Identifier: 10.1109/ICCSIT.2010.5563742, Publication Year: 2010 , Page(s): 351 – 354

[27] **Camara, M.S.; Kermad, L.; El Mhamedi,** *"Risk Prediction in ERP Projects: Classification of Reengineered Business Processes".;* Computational Intelligence for Modelling, Control and Automation, 2006 and International Conference on Intelligent Agents, Web technologies and Internet Commerce, International Conference on Digital Object Identifier: 10.1109/CIMCA.2006.190, Publication Year: 2006 , Page(s): 213 - 213

[28] **Salinesi, C.; Bouzid, M.R.; Elfassy, E.;** *"An Experience of Reuse Based Requirements Engineering in ERP Implementation Projects"* Enterprise Distributed Object Computing Conference, 2007. EDOC 2007. 11th IEEE International, Digital Object Identifier: 10.1109/EDOC.2007.46, Publication Year: 2007 , Page(s): 379 – 379

[29] **Jiangao Deng; Yijie Bian** ,*"Constructing a Risk Management Mechanism Model of ERP Project Implementation"* Information Management, Innovation Management and Industrial Engineering, 2008. ICIII '08. International Conference on Volume: 2 Digital Object Identifier: 10.1109/ICIII.2008.79, Publication Year: 2008 , Page(s): 72 – 77

[30] **Lee, K.K.F.;** *"The five disciplines of ERP software implementation"* Management of Innovation and Technology, 2000. ICMIT 2000. Proceedings of the 2000 IEEE International Conference on Volume: 2 Digital Object Identifier: 10.1109/ICMIT.2000.916743 Publication Year: 2000 , Page(s): 514 – 519

[31] **Jing-Song Cui; Da Zhang;** *"The research and application of security requirements analysis methodology of information systems"* Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on Digital Object Identifier: 10.1109/IWASID.2008.4688352 Publication Year: 2008 , Page(s): 30 - 36 "Security [32]

[32]**Agarwal, A.; Gupta, D.;** "*Requirements Elicitation Using View Points for Online System" Emerging Trends in Engineering and Technology,"* 2008. ICETET '08. First International Conference on Digital Object Identifier: 10.1109/ICETET.2008.91, Publication Year: 2008 , Page(s): 1238 - 1243

[33] **van de Riet, R.; Janssen, W.;** *"Security moving from database systems to ERP systems"* 1998. Proceedings Ninth International Workshop on Digital Object Identifier: 10.1109/DEXA.1998.707413, Publication Year: 1998 , Page(s): 273 – 280

[34] **Tianshe Yang; Jung Choi; Zheng Xi; Yanhong Sun; Chengsu Ouyang; Yongxuan Huang;** *"Research of Enterprise Resource Planning in a Specific Enterprise",* Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on Volume: 1 , Digital Object Identifier: 10.1109/ICSMC.2006.384418, Publication Year: 2006 , Page(s): 418 – 422

[35] **Kuo-En Fu;** "*Development of a generic procedure model for the enterprise resource planning implementation in small and medium enterprises"* SICE Annual Conference 2010, Proceedings of Publication Year: 2010 , Page(s): 3523 - 3528

[36] **Fitzgerald, A.;** *"Enterprise resource planning (ERP)-breakthrough or buzzword?"* Factory 2000,1992. 'Competitive Performance Through Advanced Technology'., Third International Conference on (Conf. Publ. No. 359),Publication Year: 1992 , Page(s): 291, 297

[37] **Pozgaj, Z.;** *"Information collected in the biometric identification process should be used in enterprise resource planning"* Information Technology Interfaces, 2003. ITI 2003. Proceedings of the 25th International Conference on Digital Object Identifier: 10.1109/ITI.2003.1225365, Publication Year: 2003 , Page(s): 327 - 332

[38] **Chen, S.G.; Lin, Y.K.;** *"Performance analysis for Enterprise Resource Planning systems"* Industrial Engineering and Engineering Management, 2008. IEEM 2008. IEEE International Conference on Digital Object Identifier: 10.1109/IEEM.2008.4737833 Publication Year: 2008 , Page(s): 63 – 67

[39] **Szitas, Z ;** "*A simplified object-oriented model of enterprise resource planning systems."* Electronics Technology: Meeting the Challenges of Electronics Technology Progress, 2005. 28th International Spring Seminar on Digital Object Identifier: 10.1109/ISSE.2005.1491045 Publication Year: 2005 , Page(s): 302 – 307

[40] ***chatterjee,Asok De, Daya Gupta,*** *"software Implementation of Curve based Cryptography for Constrained Devices",* International Journal of Computer Applications, 2011 by IJCA Journal, Number 5 - Article 8, Year of Publi cation: 2011,*Kakali*

[41]**M. Ware, J. Bowles, C. Eastman,** "*Using the common criteria to Elicit security Requirements with use cases",* 2006 IEEE Computer Society.

[42] **Alberts, Christopher and Dorofee, Audrey**. *OCTAVE Method Implementation Guide* v2.0. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.cert.org/octave

[43] The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures available at www.cramm.com

[44] **A. van Lamsweerde**, *Elaborating security requirements by construction of intentional anti-models*, in: Proceedings of the 26th International Conference on software engineering (ICSE'04), IEEE Computer Society, Washington, DC USA,2004, pp. 148-157.