Master Thesis
Electrical Engineering
May, 2014

Evaluation of Multi Criteria Decision Making Methods for Potential Use in Application Security

Praveen Kumar Gade
Manjit Osuri

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Authors:

Praveen Kumar Gade
Email: praveeng47@gmail.com

Manjit Osuri
Email: manjit534@gmail.com

University advisor:
Charlott Lorentzen
School of Computing, BTH

University examiner:
Dr. Patrik Arlos
School of Computing, BTH

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

Internet : www.bth.se/com
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ACKNOWLEDGEMENT

We would like to thank our supervisor Charlott Lorentzen for her support and guidance throughout our thesis work. We are grateful to her for the valuable suggestions shared with us. We would like to thank our thesis examiner Dr. Patrick Arlos for his advices during every stage of thesis.

We are thankful to our parents, beloved friends and mentors who constantly encouraged us in shaping our career.

Best Regards
Praveen Kumar Gade
Manjit Osuri

ABSTRACT

With an upsurge in number of available smart phones, tablet PCs etc. most users find it easy to access Internet services using mobile applications. It has been a challenging task for mobile application developers to choose suitable security types (types of authentication, authorization, security protocols, cryptographic algorithms etc.) for mobile applications. Choosing an inappropriate security type for a mobile application may lead to performance degradation and vulnerable issues in applications. The choice of the security type can be done by decision making. Decision making is a challenging task for humans. When choosing a single alternative among a set of alternatives with multiple criteria, it is hard to know which one is the better decision. Mobile application developers need to incorporate Multi-Criteria Decision Making (MCDM) Models to choose a suitable security type for mobile application. A decision model for application security enhances decision making for mobile application developers to decide and set the required security types for the application. In this thesis, we discuss different types of MCDM models that have been applied in an IT security area and scope of applying MCDM models in application security area. Literature review and evaluation of the selected decision models gives a detailed overview on how to use them to provide application security.

Keywords: Multi-Criteria Decision Making, Mobile Application Security.

CONTENTS

ACRONYMS

ABS – Always Best Security

AHP – Analytical Hierarchy Process

ANN – Analytical Neural Networks

ANP – Analytical Network Process

ELECTRE - ELimination and Choice Expressing REality

IBA – Image Based Authentication

MAUT – Multi Attribute Utility Theory

MADM – Multi Attribute Decision Making

MCDA – Multi-criteria Decision Analysis

MCDM – Multi Criteria Decision Making

MODM – Multi Objective Decision Making

PROMETHEE – Preference Ranking Organization Method for Enrichment Evaluation

QOE – Quality of Experience

SMART – Simple Multi Attribute Rating Technique

FIGURES

TABLES

CHAPTER I - INTRODUCTION

INTRODUCTION

Nowadays, from mobile web browsing to mobile video conferencing, internet services have become requisite in our lives. With the increase of numerous mobile applications, users are being attracted to the internet services using mobile applications. Mobile application security is considered to be one of the important issues in the present scenario. With the possible loop holes and vulnerabilities it has become easy way for hackers to access the sensitive information of the user [26]. Application developers need to protect the information from the client side by using security techniques such as cryptographic algorithms, secure tunnels, authentication and authorization etc.

The security and performance of mobile applications varies from application to application depending on the content and type of application such as Mobile banking, Facebook, Skype etc. Even proper security measures are being taken by the application developers the attackers are still breaching the security and cracking into mobile application due to the poor selection of security type for applications. An adequate level of security and performance of mobile application leads to better Quality of Experience (QoE) [5]. Decision models can be used to provide a unique path for application developers to choose the security types of the mobile applications to make security decisions.

Decision making models are classified into two types, namely single criteria and multi criteria methods. Application developers need to consider these security decision models while developing the mobile applications to meet the security requirements of the operating system. If the security decision model could act as a prerequisite for mobile application to work on platforms such as Android, IOS etc, then the application could be safe from the detrimental attacks (brute force attack, dictionary attacks, credential theft). So far in the field of information technology, decision models have been applied for Information Security, network security, computer security purpose, but there has been no work done on decision models applied to application security. There exists a wide variety of decision making models, but a selection of single method or combination of methods is a challenging task which mainly depends on type of decision problem [7]. In this thesis work, we define our decision problem as choice of appropriate security type (authentication type) for mobile application in ideal case which needs user authentication. So to solve this decision problem, an extensive literature study was carried out with the research on available decision models in IT security and the feasible decision models were selected for application security. Then decision models were evaluated to choose the security types of the mobile applications and are

necessary for application developers to regulate the security types of the mobile applications which prevents from the attacks.

In an initial phase, extensive literature study was carried out and MCDM models that have been used in IT security area are presented. In a second phase, MCDM models that are suitable for mobile application security were identified. In a third phase, identified MCDM models are evaluated. In final phase, based on the analysis of the results and our views this paper suggests a suitable MCDM model for application security.

1.1 Motivation

The motivation behind initiating this research is to provide QoE with the aid of decision models in mobile application environment. Performance and security are the two most important parameters that need to be considered when dealing with mobile applications. It is often more common to append the strongest security to applications due to the increasing threats [14]. A broad range of security mechanisms has been developed to secure mobile applications. Too little attention is given to the actual process of making a decision about the required security type of mobile applications with respect to a set of predefined OS security requirements. It is very important for the application developers to let the users access the mobile applications in a secure and efficient way of maintaining a trade-off between performance and security.

1.2 Aims and Objectives

The aim of the thesis is to suggest an appropriate security decision model for mobile application developers.

Objectives:

1. To make a detailed study on decision models that has been used for IT security purposes.
2. To find out if there are any decision models used for application security.
3. To analyze and compare decision models based on desirable security criteria and alternatives.
4. To suggest the most suitable decision model for application security.

1.3 Research Questions

1. Are there any decision models that have been used for IT security purpose?

2. Are there any decision models that are suitable for application security that was not yet used?
3. How can these decision models be used for application security?
4. Which decision model is most suitable for application security?

1.4 Related work

In [4], authors introduced Analytic Network Process (ANP) into computer network safety assessment field and compared the evaluation weight matrix based on ANP with the matrix based on Analytic Hierarchy Process (AHP). The results are similar for both models. The authors found that the ANP model has corrected some remarkable errors of the AHP model and they concluded that the assessment based on ANP is more scientific than the assessment based on AHP.

In [5] author has evaluated different decision making methods for their fitness to decision making in the security area. Three decision making models are chosen to select an adequate network security level. A practical decision making model for adaptive selection of suitable security levels has been developed and evaluated experimentally on a mobile device using limited resources.

The authors in [17] proposed information security risk management methods to rank security controls quantitatively with the aid of the PROMETHEE and GAIA module. A proposed control ranking model based on multi criteria analysis for a security plan control is set out to be the main contribution of the paper.

In [18], authors provided tentative guidelines to help in choosing an appropriate MCDA method. They also suggested a comparative study of different MCDA methods that helps to identify under different circumstances a particular method is suitable. The authors presented the process of modeling and structuring plays an important role of any decision aid methodology.

In [7], author developed a practical decision model on AHP which formalizes quantitative and qualitative considerations of a defined criterion with regard to Quality of Service. The primary motive of the thesis is on adjustable and lightweight authentication protocols for network access control. The author also presented the concept of Always Best Security (ABS).

1.5 Contribution

The main contribution of this thesis is to suggest suitable decision models for mobile application developers. This paper provides a detailed view on how to choose appropriate authentication methods for application security with the aid of decision models to provide better security. In addition, this paper presents a detailed list of decision models that have been used in IT security so far.

1.6 Outline of thesis

The first chapter introduces the thesis work. The second chapter presents the background of decision making models, their process, and the classification of decision making models. The third chapter presents the research methodology we have used in different phases which aims to answer the research questions. The fourth chapter gives a detailed literature study of how decision models can be used in application security. The fifth chapter evaluates selected decision models. The sixth chapter concludes the thesis and presents future work.

CHAPTER II – BACKGROUND

BACKGROUND

This chapter describes the definitions, fundamentals and concepts of decision making, decision making model, decision making process, classification of decision making methods, Multi-criteria decision making methods.

2.1 Decision Making

Definition 1: Decision making is a process of identifying and choosing alternatives based on the values and references of the decision maker [10].

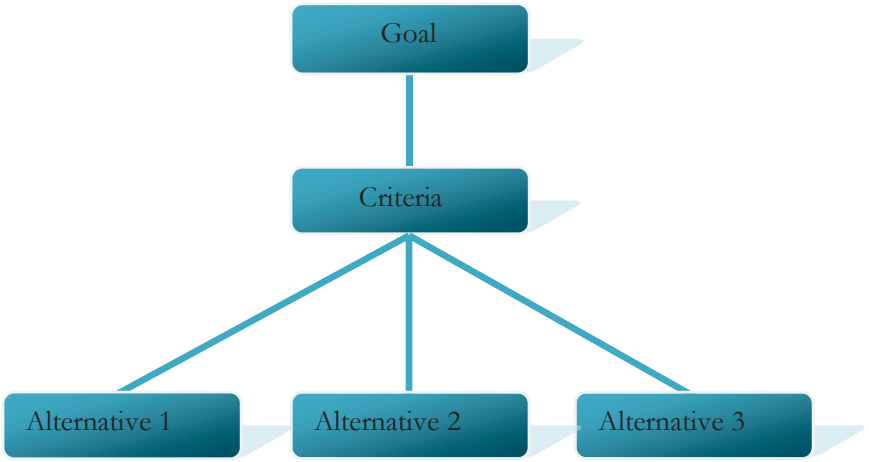


Figure1: Basic block diagram of Decision Making

Definition 2: Decision making is the process of sufficiently reducing uncertainty and doubt about the alternatives to allow a reasonable choice to be made from among them [27].

2.2 Decision Making Model

Decision making model involves a decision making process to generate a single alternative or a set of alternatives. From Figure 2 it is evident that a decision making method takes subjective inputs from the decision problem and produces suitable alternative as output.

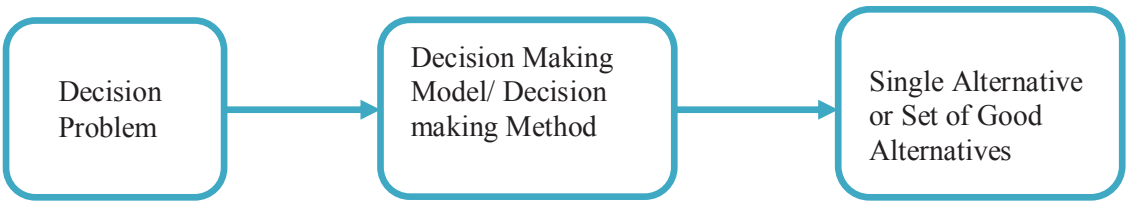


Figure2: Involvement of Decision making model in the Decision making process.

Decision making models are classified into two types namely single criteria and multi criteria decision making methods.

2.2.1 Single Criterion Decision Making Models

In this type, while choosing the alternative, the overall goal is entirely dependent on the single criteria.

E.g. In figure 3, if the decision maker needs to choose security levels for the mobile application then the output is entirely dependent on the single criteria 'Resources'.

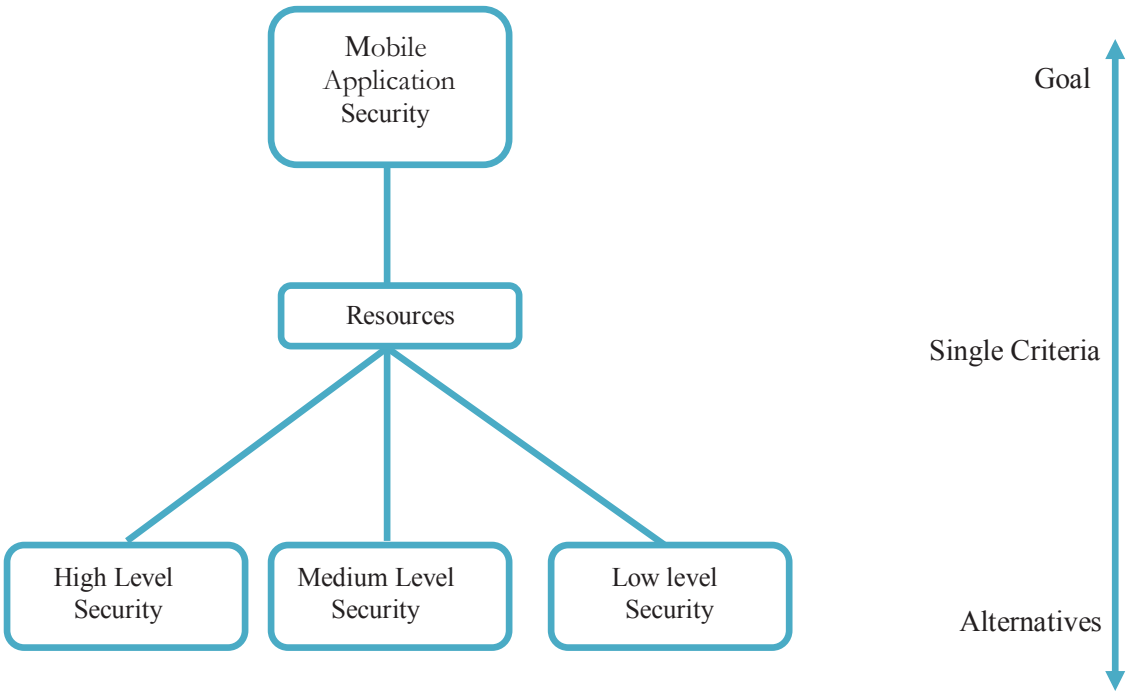


Figure3: Example showing single criteria decision making

2.2.2 Multi Criteria Decision Making Models

In this type, while choosing an alternative, the overall goal depends on two or more criteria.

E.g. In figure 4, if the decision maker needs to choose security levels for the mobile application then the output is dependent on the multiple criteria namely resources, Threat level. In figure 4, output is not only dependent on single criteria but also on the second one. The selection of alternative is mainly dependent on how the importance is given criteria.

In this thesis, we only dealt with the concepts and methods related to MCDM. No single criterion methods or concepts are used in the entire thesis.

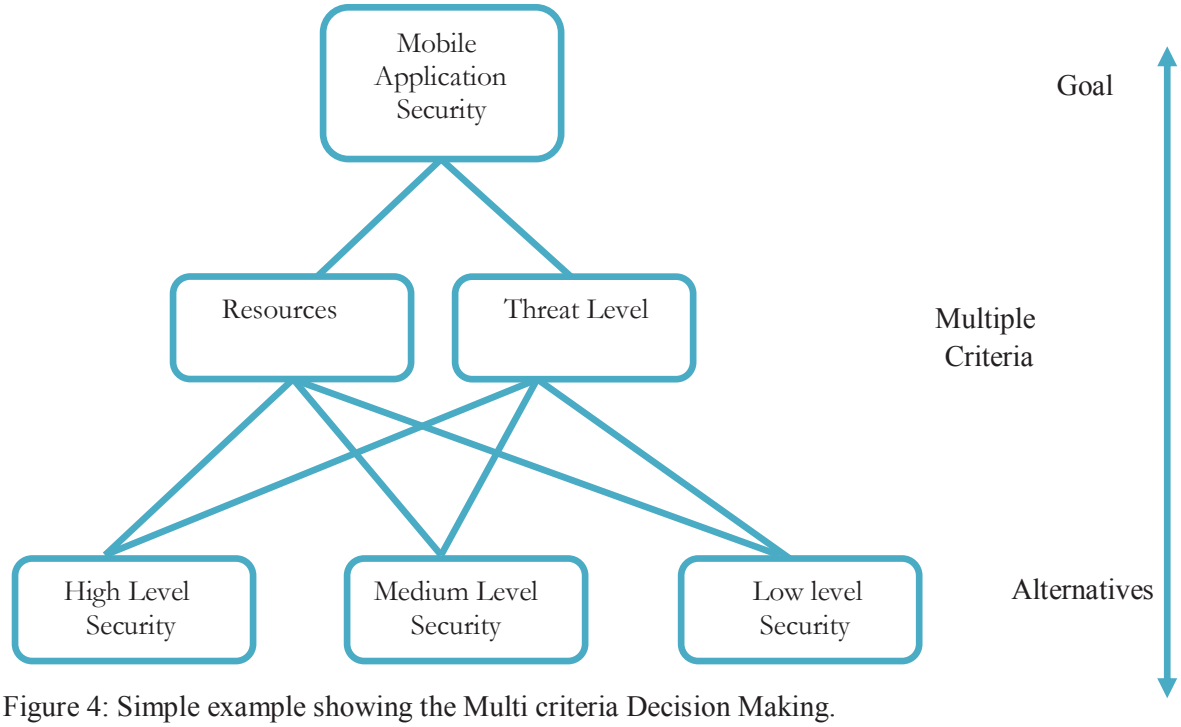


Figure 4: Simple example showing the Multi criteria Decision Making.

2.3 Decision Making Process

Decision making is a process of selecting a single alternative from a set of alternatives in a systematic and logical way. The basic step by step process involved in decision making is called a decision making process [10].

1. Define the decision problem
2. Identify the criteria
3. Identify Alternatives
4. Allocate importance weights to each criteria
5. Score the criteria for each of the alternative
6. Apply the decision rules
7. Evaluate alternatives against criteria
8. Identify the best alternative

1. **Define the decision problem**: Decision makers must be completely be aware of the decision problem. It is important to identify, understand and define the problem before making a decision. This process must be able to identify the root causes by carefully

limiting assumptions.

2. **Identify the criteria**: Identifying and defining criteria which will discriminate among alternatives must be based on goals [10]. A decision problem which contains a large number of criteria is particularly helpful to yield better alternatives. An ideal set of criteria should be operational, meaningful and non-redundant.

3. **Identify alternatives**: A major part of decision making involves the analysis of a finite set of alternatives. All the available alternatives are compared with the chosen aspects and then any alternatives that fail to meet the aspects are eliminated until there remains only one alternative thus achieving the desired goal.

4. **Allocate importance weights to each criterion**: The weights to the criteria are assigned accordingly and implement pairwise comparison.

5. **Score the criteria for each of the alternative**: A matrix is formed by scoring the criteria for each of the alternative and this matrix is applied to the decision rules.

6. **Apply the decision rules**: Based on the input from criteria weights and scores of criteria from each alternative decision rules must be applied to determine the potential and suitable alternative

7. **Evaluate alternatives against criteria**: After the evaluations, the decision making tool can be applied to rank the alternatives or allowing choosing a more promising alternative from a set of defined alternatives.

8. **Identify the best alternative:** The suitable alternative if identified in the last phase of the decision model with the help of evaluation and thus the goal is achieved.

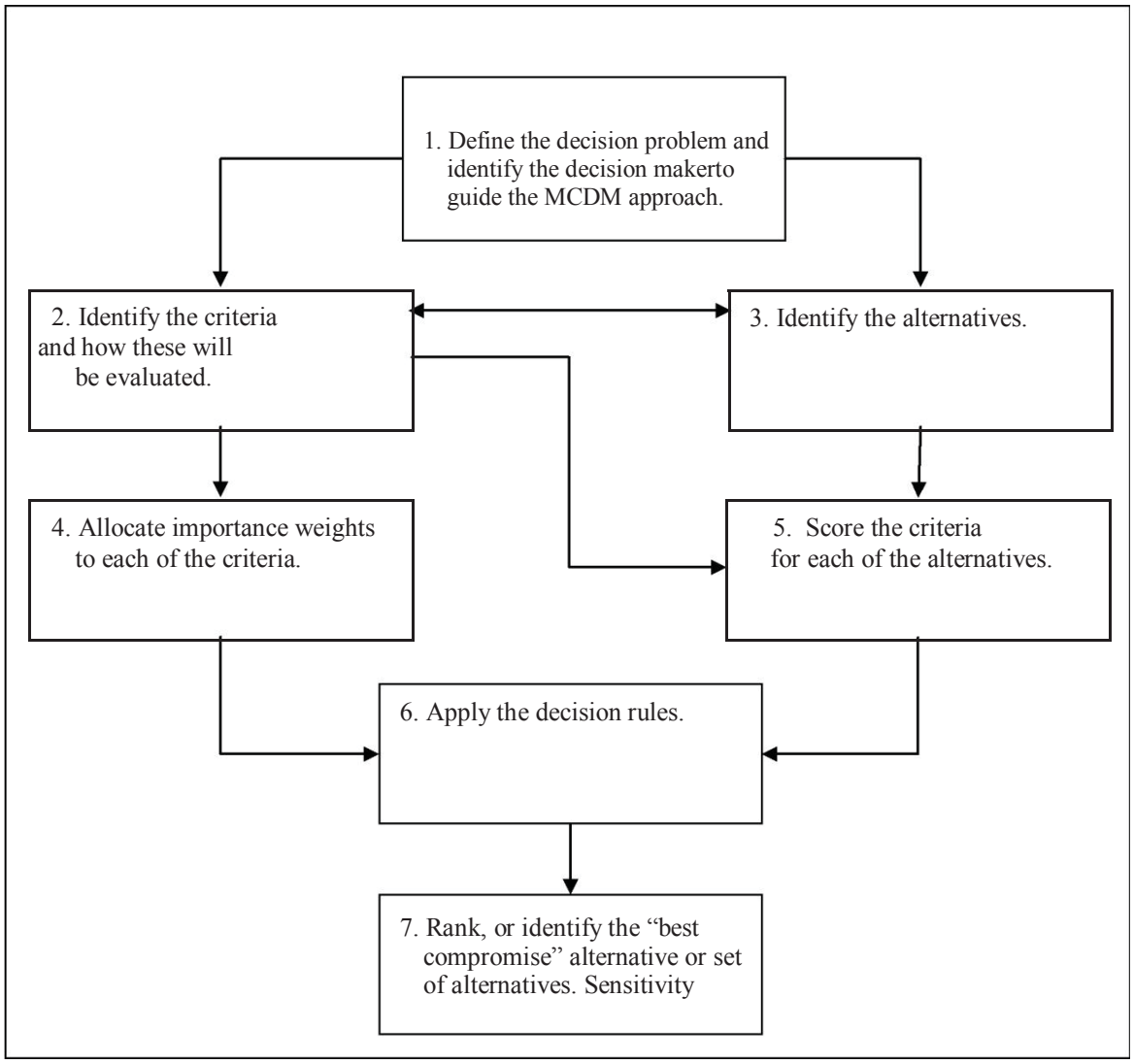


Figure 5: Step by Step Process involved in Decision Making Model

2.4 Classification of Decision Making Models

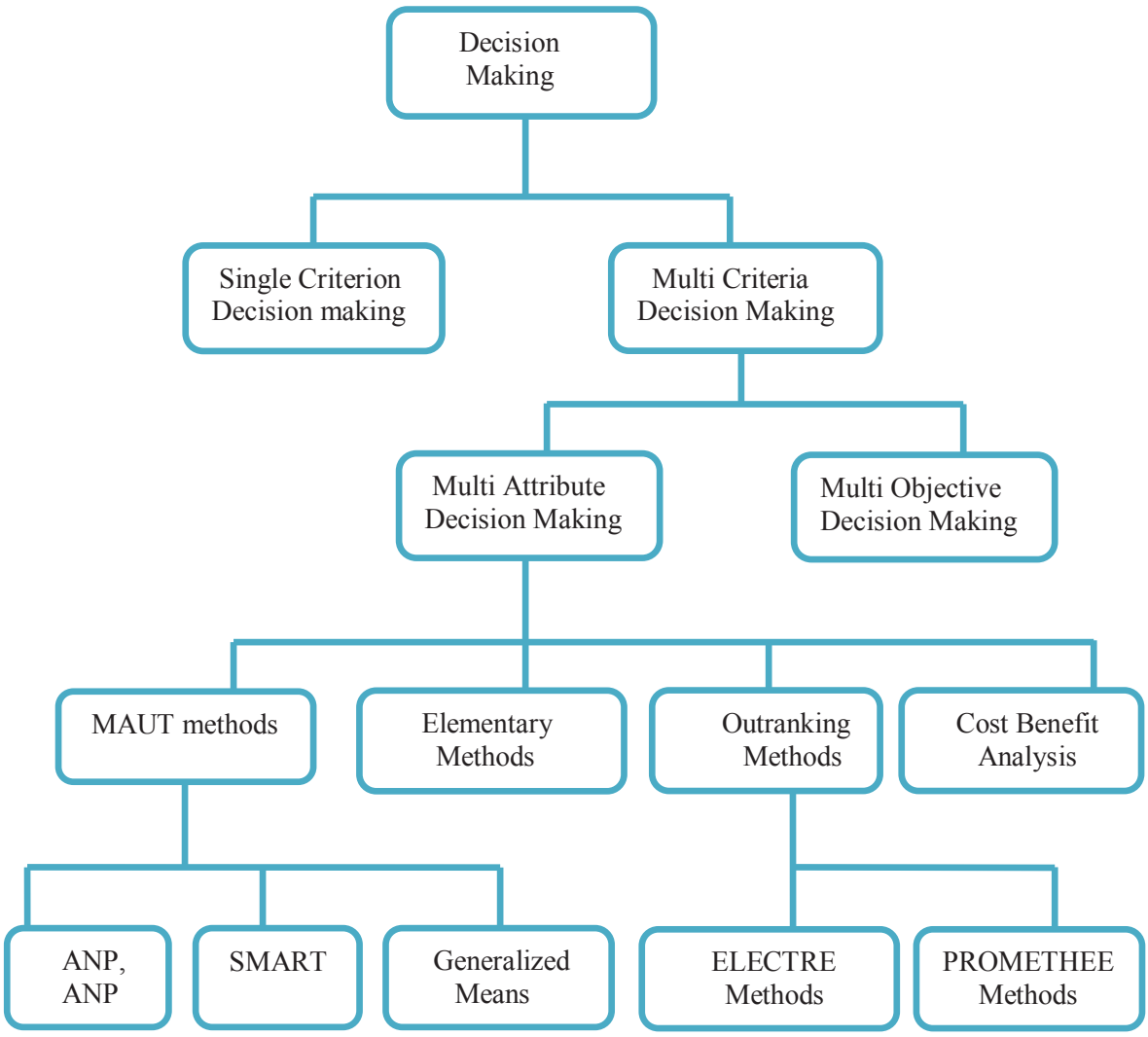


Figure 6: Classification of Decision Models according to application security.

Based on type of decision problem, decision making is divided into two types of single criterion and multi criteria decision making. Based on the number of criteria, MCDM classified into two types namely Multi Attribute Decision Making (MADM) and Multi Objective Decision Making (MODM). MADM techniques partially or completely rank the alternatives: a single most preferred alternative can be identified or a short list of limited number of alternatives can be selected [10]. As we can see from Figure 6, ANP and SMART both use the Multi Attribute Utility Theory (MAUT).

2.5 Multi Criteria Decision Making Model

Multiple-criteria decision making (MCDM) model concerns the structuring and solving decision problems and planning problems which involves multiple criteria. The main purpose is to support decision makers facing such problems. There does not exist a unique solution for such problems and it should be necessary to differentiate between solutions.

Basically, MCDM problems can be interpreted by solving in different ways as follows

1. Choosing "best" alternative from a set of available alternatives.
2. Choosing "A small set of good alternatives" or "grouping alternatives into different preference sets".
3. An extreme interpretation could be "find all efficient" or "nondominated" alternatives.

Our study in this thesis paper corresponds with choosing the "best" alternative from a set of available alternatives.

2.6 Introduction to Mobile Application Security

Security features and measures vary from application to application in mobile applications such as authentication provided to banking application is different from Email application. In general, there are two types of applications in mobile environment namely native applications and web applications each has its own architecture in designing.

Native application must be downloaded from the app store to the mobile device to be used. These types of applications are developed using Development tools, SDKs. Web application generally run in web browser in the mobile device and can run in any type of mobile platforms such as Android, Iphone, and Windows etc.

In this thesis we considered mobile application under ideal case and assumed a decision problem as a choice of authentication method. We assumed this as our decision problem and evaluated the decision models.

2.7 Decision Models in Application Security

Based on the types of the detrimental attacks, decision models can be applied in different stages of Mobile application security.

Authentication is a process involved in confirming identify of a person or a software program. Mobile application needs user authentication to access the information provided by the service provider. So while developing mobile applications, application developers should choose the suitable authentication according to the user needs and to secure from the attacks. General types of attacks during authentication are Brute force attacks, cookie replay, dictionary attacks, credential thefts. Decision models can be used in choosing authentication methods, authentication protocols.

Authorization is a process involved in act of granting or denying rights to application resources. This process will be done after the authentication of a person or software. General types of attacks during authorization of application are luring attacks, data tampering, Elevation of privilege, disclosure of confidential data.

General types of threats and attacks in the process of cryptography are poor key generation, poor key management, and weak or custom encryption mechanisms.

CHAPTER III- RESEARCH METHODOLOGY

RESEARCH METHODOLOGY

The research methodology that we have used in this study in different phases aims to answer the research questions fulfilling the objectives of this research. The initial phase comprises a detailed literature study on the various decision making methods that have been used for IT security purposes. The second phase takes up the part of identifying MCDM techniques, which confines the scope of applying decision models in application security by analyzing and comparison based on desirable security criteria and alternatives. The first and second research questions can be answered from the above phases. Evaluation of the chosen decision models answers the third research question. Evaluation of decision models is carried out with the help of mathematical procedures which mainly includes matrix equations and matrices. Based on the evaluated results, suggesting the suitable decision model for application security answers the fourth research question. The established research is based on data collection that has been logically organized moving from question to answers.

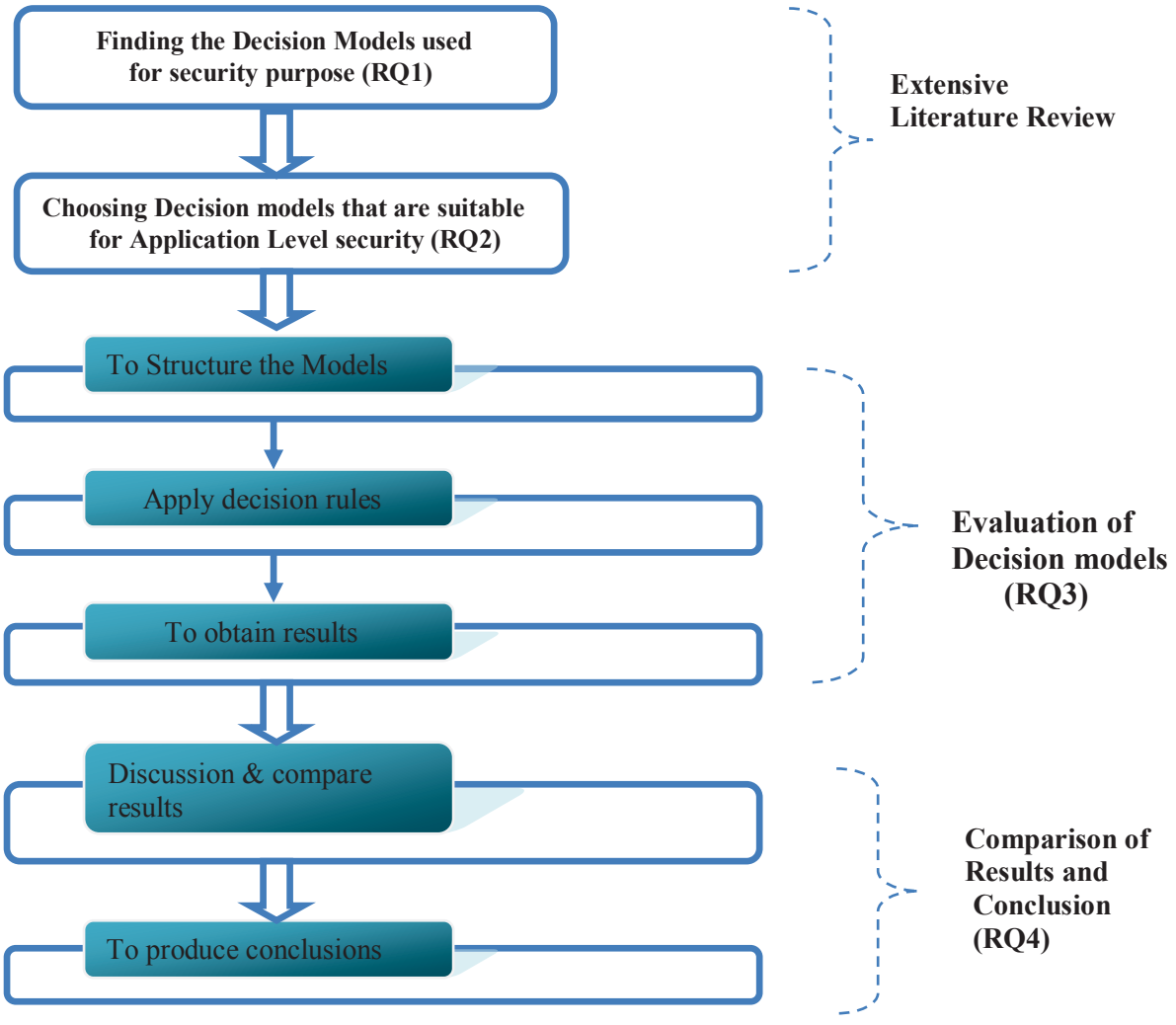


Figure 7: Flow of Research Methodology

Evaluation Method: The evaluation part plays an important role in this thesis. The main reason to choose the evaluation is, it is the only possible way to study the practical behavior of the decision model by assuming initial input values and priorities from decision maker (In this thesis authors are decision makers) [7][8]. In the evaluation method first phase is to structure the model with the help of goal, criteria and alternative as discussed in chapter II. The second phase is to apply the decision rules, this is entirely dependent on the type of the decision model we are evaluating, for e.g. decision rules followed by ANP are different from SMART model, chapter V describes more about decision rules of corresponding decision models. The results from evaluation method help in choosing the suitable method for application security.

3.1 Literature Review:

A literature review consists of critical points of current knowledge which includes substantive findings, theoretical and methodological contributions to a particular topic. Based on [5], [7] and research problem we consider literature review as the primary research methodology in our thesis work because, we need to follow a mathematical approach to find a solution to our research problem. So, in order to explore the suitable decision model which has the following traits such as less time consumption, less complexity, excludes complex calculations, we have chosen literature review as our research methodology. We have used this methodology to find current research work and previous work which helps to enhance the significance of applying decision models in application security area. With the help of literature review we find the current decision models that have been used in IT security and which further has the scope of applying to application security.

We have studied behavior of existing decision models and their recent application in various fields using the available resources from various databases namely IEEE (Institute of Electrical and Electronics Engineer), Journals, ACM (Association of Computer Machinery), Google scholar, Science Direct etc.. These resources are collected from our university library database. Based on the resources from the databases, we find two decision models and applied in application security area which provides answers to our research questions. Later, we discussed some theoretical assumptions to our mathematical approach. The decision model is then evaluated, and results are observed. We discussed about the real time application of decision models in application security which helps for the security experts.

CHAPTER IV- EXTENSIVE LITERATURE REVIEW

EXTENSIVE LITERATURE REVIEW

This chapter presents the literature study of decision models that are previously used in various research papers in the areas of IT security i.e., network security, computing security, date security and information security. A detailed description of these decision models along with the research gap in the field of application security is plotted in table 1. This chapter also covers the list of MCDM selection approaches for the evaluation of decision models. MCDM models that have been used in IT security area so far are

1. AHP
2. ANP
3. SMART
4. ELECTRE
5. PROMETHEE

Analytical Hierarchy Process (AHP) is one of the more widely applied multi attribute decision making methods (10). AHP allows its users to decompose their decision problem into a hierarchy of sub problems which can then be analyzed independently. Its methodology is based on pair wise comparisons of the defined criteria which are used to establish the weight to assess the performance scores for alternatives.
From the table 1 of the literature review, AHP decision model has been used in network security area, computing security as well as in the fields of data security and information security. The research gap has been found in the field of application security.

Analytic Network Process (ANP) is a Multi-criteria decision making method that can be applied in various management and technical related decision problems. ANP is more generalized form of AHP [8]. One can easily understand ANP when it is compared with AHP. The step by step process of ANP is as follows.

Step1. **Structure the problem**: This step involves in stating the problem clearly and decomposing the problem into a network like structure.

Step2. **Pairwise comparisons**: Decision elements at each cluster are compared pairwise with respect to their importance towards their control criteria. Also, interdependencies among criteria of a cluster are examined pairwise, the influence of each element on other elements is represented by an eigenvector. The relative importance values are determined with Saaty's scale[20].

Step3. **Super matrix formation**: To obtain global priorities in a system with interdependent influences, the local priority vectors are entered in the appropriate columns of a matrix. A super matrix is a partitioned matrix, where each matrix segment represents a relationship between two clusters in a system.

Step4. **Synthesis of the criteria and alternatives' priorities and selection of the best alternatives**: The priority weights of the criteria and alternatives can be obtained from the normalized super matrix.

ANP decision model has been found to be used in Network security areas and Information security.

Simple Multi Attribute Rating Technique (SMART) is the simplest form of Multi-attribute utility theory methods. SMART was initially proposed by Edwards [21], since then it has been widely used in business and management fields, social sciences. This method is based on linear additive or simple multiplicative models for aggregating single criterion evaluation. They are most suitable for the analysis of discrete alternatives [5]. The SMART method shows good performance and requires less computation power, making the method appropriate for IT security area. The main advantage of this approach is its simplicity in comparison with the other decision making methods.

The **ELECTRE** method is used to establish a partial ranking and choose a set of alternatives by eliminating less favorable ones while encountering few criteria with large number of alternatives in a decision making problem. The electre method begins with pair wise comparisons of alternatives under each criterion. Its basic concept is to deal with outranking relations using pair wise comparisons among alternatives under each one of the criteria separately[23]. Electre method has been evidently found to be used in the information security field.

The **PROMETHEE** method is one of the most frequently used methods of multi criteria decisions based on mutual comparison of each alternative pair with respect to each of the selected criteria. These methods require very clear additional information that is easily obtained and understood by both decision makers and analysts [24]. Promethee methods had been widely used in various others fields including the Information Security for its mathematical properties and friendless of use.

	IT Security / Decision Models	Network Security	Computing Security	Data Security	Information Security	Application Security
MAUT Methods	AHP	✓ [7][8][17]	✓ [25]	✓ [23]	✓ [11]	?
	ANP	✓ [4]	×	×	✓	?
	SMART	✓ [5]	×	×	×	?
	Generalized means	×	×	×	×	?
Out-Ranking Methods	ELECTRE methods	×	×	×	✓ [16][23]	?
	PROMETHEE methods	×	×	×	✓ [17]	?

Table 1: Decision models applied in IT security area

The primary output of the extensive literature review is Table 1. In an IT firm, IT security is categorized as Network Security, Computing Security, Data Security, Information Security and Application Security. All the decision models except generalized means listed in Table 1 have been applied in all categories of IT security except application security. According to our literature review no decision models have been applied in application security.

Below are the symbols which clarify the above Table 1:

✓ - Decision models that have been applied in IT security.

× - Decision models that have not been applied in IT security (except application security).

? - Indicates no decision models have been applied in application security forms a research gap.

4.1 Choice of MCDM Techniques

Choosing a specific MCDM method for evaluation is an important and challenging task which includes systematic and logical analysis. Below is a list of MCDM selection approaches [3].

1. Laaribi's approach
2. Hanne's approach
3. Ulengin et al.'s approach
4. Salinesi and Kornyshova's approach
5. Vincke's approach
6. Felix's approach
7. Ozernoy's approach
8. Olson et al.'s approach
9. Ballestero and Romero's approach

Among all the approaches listed above Hanne's approach is suitable for our decision problem because of the following reasons. The other approaches follow complex procedures for selection and are not relevant for IT security.

1. Ease of Use
2. General application domain
3. User- friendliness

Selection of a single or multiple MCDM models is a challenging task. There exist many factors that need to be considered while choosing a method to apply for application security. Some of them are in [3]

- Consistency
- Robustness
- Ease of use
- Time required
- Implementation of the method

Following are the set of rules that need to be embraced from application developer point of view while choosing a decision model to apply into application security.

1. In general, application developers do not have good understanding in decision models. So decision making process becomes complicated if the decision maker chooses complex decision making methods. So developer needs to choose the decision model which should not include complex calculations and which consumes less time for decision making process.
2. The outcome of the decision making process should be reliable.
3. Decision making process requires less human intervention.
4. Decision models should be applicable for the sensitive analysis.

Based on the above findings we have considered two decision models namely ANP and SMART.

The strength of the ANP lies in its use of ratio scales to capture all kinds ofinteractions, formulate accurate predictions, and make decisions [20]. ANP method is considered to be the effective decision making model compared with AHP [20]. There exists online tools to solve the decision problem using ANP, but we have done theoretically to clarify the readers with detailed evaluation procedure and how they can be used for application security. These theoretical models can be applicable for combination of two or more decision models.

SMART has been chosen for its less computational efforts compared with outranking methods for its less complexity compared with AHP [5]. The SMART model is most appropriate for an analysis where identified alternatives are distinct.

A multi-criteria decision model consists of a goal, criteria and alternatives. In this thesis paper, our aim is to find the appropriate authentication method for mobile application. The alternatives are user Id and password authentication, image based authentication [19] and we identified resources, threat level and user preferences as criteria.

Criteria:

- Resources: Resource allocation plays an important role when the security and performance factors are taken into consideration. The application developer needs to consider the amount of utilization of resources such as operating memory, connectivity speed depending on the security type.

- Threat level: Threat level is identified to indicate the type of attacks during the authentication process.

- User Preferences: This criterion has been chosen to help the user experience according to their preferences. Some users would like to authenticate with a stronger security protocol while others with simple and light weight security mechanism.

Alternatives: The decision making model has two alternatives defined.

- Image-based Authentication (IBA): This type of authentication is carried out by identifying the pictures of the users by matching with the previously chosen ones. This type of authentication is used for stronger security purposes while consuming more resources.
- Username and password: This type of authentication requires users to enter the username and password credentials to grant the access. This type of authentication is more vulnerable and is preferred when there is a low risk of attacks.

CHAPTER V- EVALUATION OF DECISION MODELS

EVALUATION OF DECISION MODELS

Purpose of Evaluation: This chapter is based on theoretical assumptions and mathematical procedures with an aim to provide the insight of how efficiently the decision model works. The main purpose of the evaluation is to extract the overall weights of the alternatives for each decision model and based on these weights, decision maker (in this thesis authors are decision makers) chooses the suitable alternative. In this chapter two decision models Analytical Network Process and Simple Multi-attribute Rating Technique are evaluated mathematically with a step a step procedure. Each decision model has its own nature and set of rules for the evaluation process.

Finally, corresponding results from both decision models were taken and compared. Based on the comparison the suitable decision model is suggested for application security.

Prerequisites for evaluating MCDM:

- ✓ Decision maker should provide the input values (rating among criteria) and priorities among alternatives.
- ✓ Check whether the decision model has suitable scope for applying into our subject area (In this thesis application security is our subject area) which was done in chapter IV.

One should consider the goal, criterion and alternatives prior to evaluation of both decision models

- ✓ **Goal** of the decision model is 'To choose suitable authentication method for application security'
- ✓ **Criterion** is Resources, User preferences and Threat level
- ✓ **Alternatives** are 'Username and Password based Authentication method' and 'Image based Authentication"

5.1 Analytic Network Process (ANP):

ANP is a network like structure and all the elements in network model are considered to be as nodes. Figure 9 depicts the ANP decision making model which shows the choice of authentication method as a goal.

Step 1: We have considered decision problem as choice of appropriate authentication method for application security. This step involves decomposition of decision problem into network model.

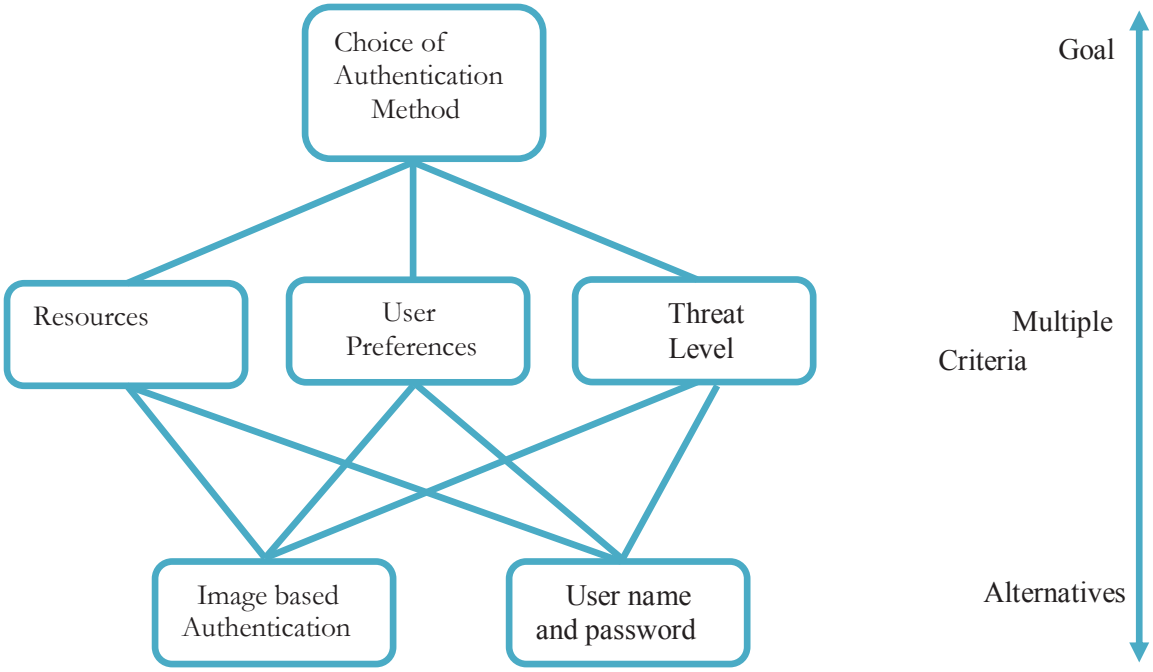
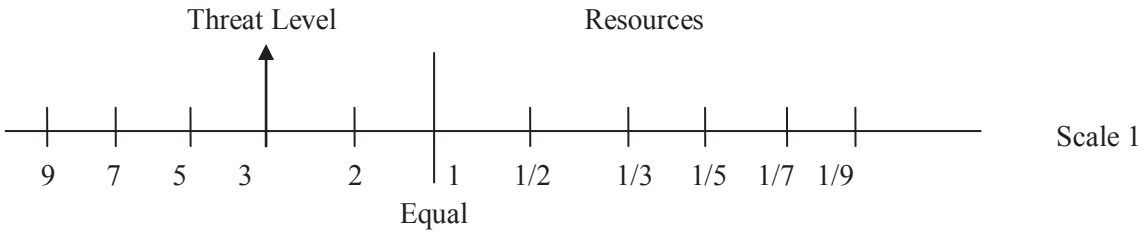


Figure 8: Showing the ANP Decision Making Method.

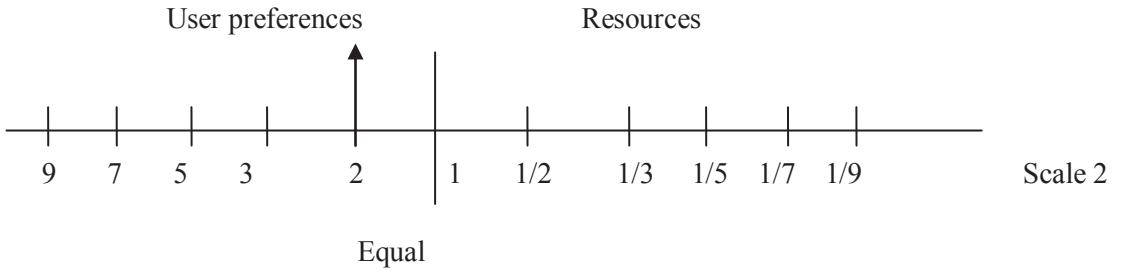
Step 2: **Pair wise comparisons**

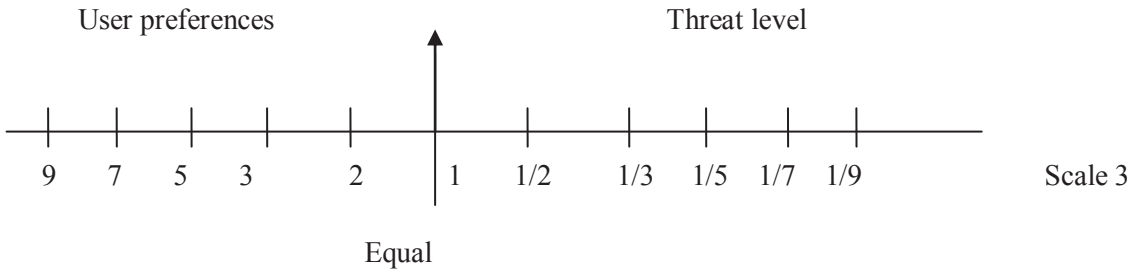
Pair wise comparison is the process of comparing criteria to each other in pairs to judge which of each criteria is preferred. As our criteria are Resources, Threat level and User Preferences, we need to do pairwise comparison for these three alternatives. So we compare it based on the preference scale as shown below



Decision maker has to choose the importance of the criteria with respect to alternatives. As the author of this thesis is the decision maker, he has to choose the importance of criteria. In the above scale Threat level is given 3 times more important than resources. The up arrow in the scale indicates that the importance of one criteria against the other.

In the similar way, following are the two scales for comparison of User preferences and resources, User preferences and Threat level. Comparison of two similar criteria results to 1 as they have same importance to each other.





		Criteria		
		Resources	Threat level	User Preferences
Criteria	Resources	1	$1/3$	$1/2$
	Threat level	3	1	1
	User Preferences	2	1	1

Table 2: Pair wise comparison of criteria

Now from the obtained values in Table 2, we need to form Eigen vector of the matrix and further need to normalize it. Following is the Eigen vector of Matrix

Eigen Vector of the Matrix:

Matrix N for n (=3) Criteria

$$\mathbf{N} = \begin{pmatrix} 1 & A_{12} & A_{13} \\ A_{12}^{-1} & 1 & A_{23} \\ A_{13}^{-1} & A_{23}^{-1} & 1 \end{pmatrix} \text{ ---------- (1)}$$

$$N = \begin{pmatrix} 1 & 1/3 & 1/2 \\ 3 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix} \quad \text{---------- (2)}$$

- ✓ To normalize the matrix N, divide each element by sum of its own column
- ✓ Sum of elements in first column, second column and third column are S_{c1}, S_{c2}, S_{c3} in Eq 3

Normalize and calculate First normalized principal Eigen Vector X1

$$|N| = \begin{pmatrix} 1/S_{c1} & a_{12}/S_{c2} & a_{13}/S_{c3} \\ a_{12}^{-1}/S_{c1} & 1/S_{c2} & a_{23}/S_{c3} \\ a_{13}^{-1}/S_{c1} & a_{23}^{-1}/S_{c2} & 1/S_{c3} \end{pmatrix} \quad \text{----------} \quad (3)$$

$$X_1 = \begin{pmatrix} \sum row_1/n \\ \sum row_2/n \\ \sum row_3/n \end{pmatrix} \quad \text{---------- (4)}$$

Square normalized matrix |N| and calculate next iteration of Eigen vector until difference $X_k+1 - X_k$ is negligible $X_2 \rightarrow |N|^2$

Step 3: **Super matrix formation**: After obtaining weights of criteria and alternatives, these are to be filled in a super matrix to find the suitable alternative based on the weights [20]

			Criteria			Alternatives	
		Choice of authentication method	Resources	User Preferences	Threat level	User Id Password Authentication	Image based Authentication
	Choiceof authentication method						
Criteria	Resources						
	User Preferences						
	Threat Level						
Alternatives	User Id and password authentication						
	Image based authentication						

Table 3: Structure of Supermatrix:

Super matrix: A super matrix is a two dimensional matrix of elements by elements. The priority vectors obtained in pairwise comparisons appear in the appropriate column of supermatrix. **Table 3** shows basic structure of supermatrix. This supermatrix came into picture only in the process of evaluating ANP decision model. In ANP model, we first structure unweighted supermatrix which includes the weights of the criteria w.r.t alternatives and weights of alternatives w.r.t criteria, this is due to the feedback, loop nature of ANP process, whereas in AHP we only find out the weightsof the criteria w.r.t to alternatives. So, the result of the both decision models varies accordingly.

			Criteria			Alternatives	
		Choice of authentication method	Resources	User Preferences	Threat level	User Id and Password authentication	Image Based Authentication
	Choiceof authentication method						
Criteria	Resources	17					
	User Preferences	43					
	Threat Level	40					
Alternatives	User Id and Password authentication		50	20	33		
	Image based authentication		50	80	67		

Table 4: Unweighted Supermatrix in hierarchal model

Table 4 shows unweighted supermatrix in controlled hierarchal model in which the weights of the criteria w.r.t alternatives are entered in matrix. Until this process we follow the same procedure as in AHP. From now we move on to the core of ANP process where the importance of alternative w.r.t criteria needs to be weighted. ANP is feedback like structure so the overall goal not only dependent on the importance of criteria against each alternative but also on the importance of alternative against each criteria.

			Criteria			Alternatives	
		Choice of authenticati on method	Resources	User Preferences	Threat level	User Id and Password authentication	Image Based Authentication
	Choice of authentication method						
Criteria	Resources	17				13	13
	User Preferences	43				13	75
	Threat Level	40				75	13
Alternatives	User Id and Password authentication		50	20	33		
	Image based authentication		50	80	67		

Table 5: Unweighted Supermatrix in Network model

After all comparisons are done we get 'unweighted supermatrix'. This matrix is then normalized i.e., the sum of all columns is scaled to 1.

Normalize a matrix: Add all the corresponding elements in the column and divide each element by sum of its own column. After normalizing the unweighted super matrix the result is weighted super matrix shown in Table 6.

Step4: Synthesis of the criteria and alternatives' priorities and selection of the best Alternatives:

			Criteria			Alternatives	
		Choice of authentication method	Resources	User Preferences	Threat level	User Id and Password authentication	Image Based Authentication
	Choiceof authentication method						
Criteria	Resources	0.17				0.74	0.12
	User Preferences	0.43				0.12	0.74
	Threat Level	0.4				0.12	0.12
Alternatives	User Id and Password authentication		0.5	0.2	0.33		
	Image based authentication		0.5	0.8	0.67		

Table 6: Normalized Weighted Supermatrix in Network model

The whole model is synthesized by calculating the Limit Matrix shown in Table 7. Limit matrix is weighted super matrix taken to the power of k+1, where k is an arbitrary number.

Let's say the weighted supermatrix is X then it should be taken to the power of k+1 i.e. X^{k+1}. We have to multiply until the difference of X^{k+1} and X^{k} is negligible.

			Criteria			Alternatives	
		Choice of authentication method	Resources	User Preferences	Threat level	User Id and Password authentication	Image Based Authentication
	Choiceof authentication method						
Criteria	Resources		18	18	18		
	User Preferences		26	26	26		
	Threat Level		6	6	6		
Alternatives	User Id and Password authentication	36					
	Image based authentication	64					

Table 7: Limit Matrix showing the overall weights of the two alternatives

From the above evaluation method, the priority of alternatives resulted in Image based authentication. Image based authentication has highest weight compared to Id password based authentication hence preferred. The red color figures indicates the overall weights of the alternatives.

5.2 Simple Multi Attribute rating Technique (SMART):

Step by step process of evaluating SMART decision model is as follows

1. Identify the Decision problem.

   In this thesis, decision problem is choice of authentication method.

2. Identify the alternatives to be evaluated.

For evaluating this decision making model, we have identified two alternatives

- User Id and Password authentication (Low security)
- Image based authentication (High security)

3. Identify the criteria to evaluate alternatives.
   We have chosen three criteria namely
   - Resources
   - Threat level
   - User preferences

4. Need to assign criteria scores for each identified criterion to measure the performance of the alternatives onthat criterion.
   - To assign the scores to the criteria we considered the verbal statements which correspond to the particular scores (Table 8 and Table 9)

5. Calculate weight of each criterion.
   - We used the direct rating method to calculate the weights for criteria. Threat level attribute has the highest importance and result in the highest weight (Table 10). Resource attribute has the lowestpriority. The choice of the weights was based on our assumption that the threat level attributes are the most important for users of the system under consideration.

6. Normalize the weights and weighted average
   - For normalization formula 1 was used and for weighted average formula 2 was used.

Verbal statement:	Scores
High	100
Medium	50
Low	10

Table 8: Verbal Scores
Assigned scores based on verbal statement

Criteria / Alternatives	User Preferences	Threat level	Resources
User Id & Password Authentication	Medium	High	Low
Image based Authentication	High	Low	Medium

Table 9: Importance to the criteria based on direct rating method

Threat level attribute has the highest importance and higher weight.

- ✓ The following formula can be used for normalization:

$$u_{ij} = a_{ij} / \sum a_{ij} \qquad (5)$$

where
a_{ij} - scores assigned to criteria

Weights / Criteria	weights	Normalized Weights
User preferences	50	0.29
Threat level	90	0.52
Resources	30	0.17

Table 10: Normalized weights of Criteria

- ✓ To find out the weighted averages

$$u_i = \sum_j w_j \qquad (6)$$

$$\sum_j w_j = 1 \qquad (7)$$

Where

U_i is aggregate utility for the i_{th} alternative

W_j– is normalized weight of the j_{th} criterion

U_{ij}– is normalized scores of the i_{th} alternative on j_{th} criterion

Weighted average for User Id & password Auth = 50*0.29+100*0.52+ 10*0.17 = 68.2

Weighted average for Image based authentication = 100*0.29 + 10*0.52+ 50*0.17 = 42.7

It is evident from the results that image based authentication has lowest weighting average and hence it is preferable for authentication.

CHAPTER VI – DISCUSSION OF EVALUATION

DISCUSSION OF EVALUATION

This chapter discusses about the results obtained from two evaluated decision models and results are compared.

ANP is a network like structure, in this method all the elements i.e. goal, criteria and alternatives are considered as nodes. The overall goal is not only dependent on importance of alternatives but also on importance of criteria. The weights obtained from the limit matrix are 36 for user id & password, 64 for image based authentication. In ANP we look into each alternative w.r.t criteria independent from one another. Now we can see user preferences of Image based authentication (75+43) is slightly more than threat level in user id & password based authentication (75+40) as shown in Table 6. Hence the result was in the favor of image based authentication.

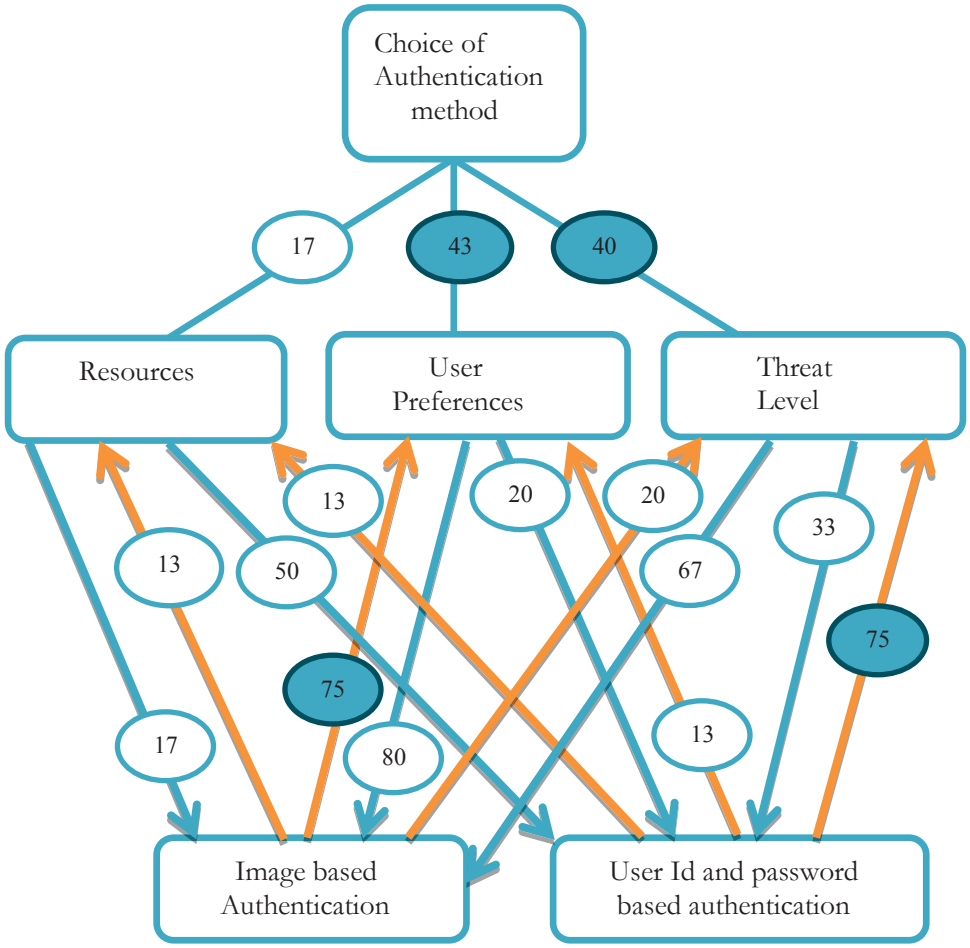


Figure 9: Structure of ANP showing the resulted weights in feedback loops

SMART doesn't use pairwise comparisons as used in ANP, instead it follows multi-attribute utility theory which requires less computation. Scores are assigned to criteria based on verbal statement and importance of criteria is determined by using direct rating method. From the weighted average

obtained in evaluation image based authentication is preferred as it has the lowest weighted average of 42.7

In ANP and SMART we have considered similar metrics as criteria namely Resources, User preferences and threat level for the evaluation. In this thesis we assumed the decision problem as choice of authentication for a application security under Ideal case which needs user authentication. We have applied same decision problem for two decision models and evaluated the models. Even though two decision models follow its own procedures based on their nature, the result from both of these is the same.

CHAPTER VII-CONCLUSION AND FUTURE WORK

CONCLUSION AND FUTURE WORK

6.1 This research work addresses the challenges in selection of decision model for a particular decision problem. In addition this paper shows the scope of applying Multi criteria decision making (MCDM) methods in application security area. Two decision methods namely Analytical Network Process (ANP), Simple Multi-Attribute Rating Technique (SMART) are evaluated and results are analyzed. Based on the literature review and evaluation process of MCDM methods, this paper suggests SMART decision making method for application developers whose security decisions involves higher number of alternatives. If ANP is used in case of higher number of alternatives it brings complexity to the decision making process. ANP is an effective decision making method in case of less number of alternatives. It is finally concluded that in the evaluation of two decision models, image based authentication proved to be best for security of applications.

Research Question 1: Are there any decision models that have been used for IT security purpose?
Answer: Yes. AHP, ANP, SMART, Fuzzy reasoning, ANN are the decision models that have been used in IT security purpose.

Research Question 2: Are there any decision models that are suitable for application security that was not yet used?
Answer: Yes. AHP, ANP and SMART decision models can be used for Application security based on their nature and ease of use.

Research Question 3: How can these decision models be used for application security?
Answer: Decision models can be used in different stages of application security such as authentication, authorization, cryptography, advanced security algorithms. In this report we have chosen authentication as goal for security decision.

Research Question 4: Which decision model is most suitable for application security?
Answer: No decision model is 100 % suitable for a decision problem. Let's consider in this thesis paper, we have chosen ANP and SMART decision models for security decisions but one cannot say that these would produce 100% solution to the decision problem. There might be other decision models or combination of decision models that could result better than ANP and SMART.

6.2 Future Work:

Security decision models could practically be applicable in real time environment for E.g. while developing a mobile app, native apps. Combination of two or more decision models is suggested for better security decisions.

REFERENCES:

[1] F.A. Lootsma, H. Schuijt, "The Multiplicative AHP, SMART and ELECTRE in a Common Context", *Journal of Multi-Criteria Decision Analysis*, vol. 6, pp.185-196, 1997.

[2] Decision Making: A Computer-Science and Information-Technology Viewpoint http://indecs.eu/2009/indecs2009-pp22-37.pdf

[3] E. Kornyshova, C. Salinesi, "MCDM Techniques Selection Approaches: State of the art", Conference Proceedings, Honolulu, HI, 2007, pp. 22 – 29.

[4] J. N. Yi, W. D. Meng, W. M. Ma, J. J. Du, "Assess Model of Network Security based on Analytic Network Process", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics,Guangzhou, China, pp. 27 – 32, 2005.

[5] S. Smirnov, "Decision Making for Finding an Adequate Security Level", Master's thesis, Dept. Interaction and System Design, Blekinge Institute of Technology, Ronneby, Sweden, 2007.

[6] Tzeng, Gwo-Hshing, "A VIKOR-based Multiple Criteria Decision Method for Improving Information Security Risk", *International Journal of Information Technology & Decision Making*, Vol. 8, No. 2, pp. 267-287, 2009.

[7] Henric Johnson, "Toward Adjustable Lightweight Authentication for Network Access Control", Ph.D. Dissertation, Dept. Telecommunication Systems, Blekinge Institute of Technology, Karlskrona, Sweden, 2005.

[8] Q. Dong-mei, F. Chun-shu, "Study on Network Security Assessment Based on Analytical Hierarchy Process", International Conference on Electronics, Communications and Control, Tianjin, 2011, pp.2320 – 2323.

[9] L. O. Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", *Proceedings of IEEE*, NJ, pp. 2021-2041.

[10] János Fülöp. Introduction to Decision Making Methods. [Online]. Available: http://academic.evergreen.edu/projects/bdei/documents/decisionmakingmethods.pdf

[11] I. Syamsuddin, J. Hwang, "The Application of AHP to Evaluate Information Security Policy Decision Making", *Journal of Simulation*, Systems, Science and Technology,2009, 10(5), 33-37.

[12] Rolander, Nathan, A. Ceci, and M. Berdugo. "A framework for MCDM method selection." Georgia Institute of Technology report, 2003.

[13] "Mobile Application Security." [Online]. Available: http://www.cio.ca.gov/OIS/Government/events/documents/Mobile_Application_Security.pdf/. [Accessed: 01 - April - 2013].

[14] Designing Secure Mobile Apps, [Online], Available: http://www.slideshare.net/denimgroup/designing-secure-mobile-apps/. [08 April 2013].

[15] Y. Fengshe, "Research on the Evaluation of Computer Security Based on the Fuzzy Analytic Hierarchy Process", Proceedings of the International Conference on Education Technology and Management Engineering, 2012, China, Vol.16-17.

[16] J. Van der Meer, T. T. EUR, A. Meulstee, Y. Z. EUR,"Multi-criteria decision model inference and application in information security risk classification", 2012.

[17] L. Jun-Jie, W. Yuan-Zhuo, "A Ranking Method for Information Security Risk Management based on AHP and PROMETHEE", Proceedings of the International Conference on Management and Service Science, 2010, China, pp. 1-4.

[18] A. Guitouni, J.M. Martel, "Tentative guidelines to help choosing an appropriate MCDA method", *European Journal of Operational Research*, 109(2), 1998, pp501-521.

[19] Image based Authentication, [Online], Available: http://confidenttechnologies.com/mobile_authentication/mobile_application_security [05 May2013].

[20] Thomas L. Saaty. Fundamentals of Analytic Network Process. ISAHP, Kobe, Japan (1999).

[21] W. Edwards, Social Utilities, Engineering Economist, Summer Symposium Series 6, 1971

[22] Promethee methods, [Online], Available: http://www.inf.unideb.hu/valseg/dolgozok/anett.racz/docs/DSS/Promethee.pdf [25Aug2013].

[23] Jeroen van der Meer, "Multi-criteria decision model inference and application in information security risk classification", Master Thesis, Dept. Economics, Erasmus University Rotterdam,2012.

[24] S. Zhaoxu, H. Min,"Multi-criteria decision making based on PROMETHEE method", International Conference on Computing, 2010, Beijing, pp.416 – 418.

[25] D. Zhao, J.F.Ma, Y.S. Wang,"Model of fuzzy risk assessment of the information system",*Journal-Chine Institute of Communications*, 28.4 (2007): 51.

[26] Mobile Applications Risks, Hacking Prevention Hot Topics at Recent RSA Security Gathering, [Online], Available: http://www.notebookreview.com/default.asp?newsID=6411[25 Jan2013].

[27] Introduction to Decision Making, Part 1 [Online], Available: http://www.virtualsalt.com/crebook5.htm[25 June 2013].